

## STUDY

on voluntary collaboration practices in  
addressing online infringements of trade mark  
rights, design rights, copyright and rights  
related to copyright



This study has been commissioned to Deloitte SLU by the EUIPO through the European Observatory on Infringements of IP Rights

Main authors:

**Prof. Dr. Thomas Hoeren, ITM, University Of Münster (Germany)**

**Prof. Dr. Guido Westkamp, Chair in Intellectual Property and Comparative Law, Co-Director, Queen Mary Intellectual Property Institute (United Kingdom)**

**Deloitte team members: María Vidal, Susana Rodriguez Ballano, Paula Iun, Ana De Lluc Compte, Jaime Pascual, Andrea Sánchez Guarido, Julia Torres.**

## Index

<b>Foreword by the Executive Director</b>	8
<b>Introduction and summary of the results: Glossary of terms</b>	11
<b>1. Executive summary</b>	<b>14</b>
<b>3. Introduction</b>	16
3.1. <i>Context</i>	16
3.2. <i>Purpose of the study</i>	16
3.3. <i>Scope</i>	17
3.4. <i>Methodology</i>	17
<b>3. General characteristics of the selected VCPs</b>	19
3.1. <i>Summary of the VCPs analysed</i>	19
3.2. <i>Comparative table</i>	25
3.3. <i>Horizontal comparison</i>	35
<b>4. Legal issues</b>	38
4.1. <i>VCPs of Member States of the European Union</i>	38
4.2. <i>U.S. VCP</i>	43
4.3. <i>CJEU Case Law</i>	43
4.4. <i>The legal framework: fundamental aspects for VCPs</i>	44
Chapter 1: Glossary of terms	48
Chapter 1: Structure and content	50
1. Introduction	51
<b>2. Signatories to the Charter and third parties</b>	53
2.1. <i>Role of rightholders</i>	53
2.2. <i>Role of public authorities</i>	53
2.3. <i>Role of platforms</i>	54
2.4. <i>Role of civil society</i>	55
<b>3. Duties and procedures</b>	56
3.1. <i>Becoming a signatory</i>	57
3.2. <i>Preventive measures aimed at platforms before offers are submitted by sellers</i>	57
3.3. <i>Proactive measures aimed at platforms after offers have been submitted by sellers</i>	59
3.4. <i>Sanctions</i>	62
<b>4. Coexistence of the measures set out in the VCP with European Union and French legal frameworks and related case law</b>	65
4.1. <i>Charter of Fundamental Rights</i>	65
4.2. <i>European Union Directives</i>	65
4.3. <i>Constitutional prerequisites and fundamental rights in France</i>	66
4.4. <i>French Regulations</i>	67
4.5. <i>Analysis of the VCP in relation to the European Union and French legal frameworks and case law</i>	68
<b>5. Technologies</b>	80
<b>6. Costs</b>	81
<b>7. Education</b>	82
<b>8. Effectiveness</b>	83
<b>Chapter 1: Annex 1</b>	85
<i>Charter for the Fight Against the Sale of Counterfeit Goods on the Internet between Intellectual Property Rightholders and e-Commerce Platforms</i>	85

<b>Chapter 1: Annex 2</b>	91
<i>Signatories that joined the Charter in December 2009</i>	91
<b>Chapter 1: Annex 3</b>	93
<i>Signatories that joined the Charter in February 2012</i>	93
<b>Chapter 1: Annex 4</b>	94
<i>European Union legal framework</i>	94
<b>Chapter 1: Annex 5</b>	96
<i>CJEU Case Law</i>	96
<b>Chapter 1: Annex 6</b>	100
<i>French legal framework</i>	100
<b>Chapter 2: Glossary of terms</b>	103
<b>Chapter 2: Structure and content</b>	105
<b>1. Introduction</b>	106
<b>2. Stakeholders and third parties</b>	108
2.1. Role of the Werberat	108
2.2. Role of associations	109
2.3. Role of Advertisers/Agencies	110
2.4. Role of public authorities	110
2.5. Role of civil society	110
<b>3. Duties and procedures</b>	111
3.1. Scope of application of the VCP	111
3.2. Definition of Advertising Environments Breaching Copyright	111
3.3. Complaint procedure before the Werberat	112
<b>4. Coexistence of the measures set forth under the VCP with European Union and Austrian legal frameworks and related case law</b>	117
4.1. Charter of Fundamental Rights	117
4.2. European Union Directives	117
4.3. Constitutional prerequisites and fundamental rights in Austria	118
4.4. Austrian Regulations	119
4.5. Analysis of the VCP in relation to the European Union and Austrian legal frameworks and case law	120
<b>5. Technologies</b>	126
<b>6. Costs</b>	127
<b>7. Education</b>	128
<b>8. Effectiveness</b>	129
<b>Chapter 2: Annex 1</b>	130
<i>Interviewed stakeholders</i>	130
<b>Chapter 2: Annex 2</b>	131
<i>Article 1.7 of the Ethics Code (Unlawful Advertising Environments)</i>	131
<b>Chapter 2: Annex 3</b>	132
<i>Rules of Procedure of the Werberat</i>	132
<b>Chapter 2: Annex 4</b>	137
<i>European Union legal framework</i>	137
<b>Chapter 2: Annex 5</b>	138
<i>Austrian legal framework</i>	138
<b>Chapter 2: Annex 6</b>	141
<i>CJEU Case Law</i>	141
<b>Chapter 3: Glossary of terms</b>	147
<b>Chapter 3: Structure and content</b>	149
<b>1. Introduction</b>	150
<b>2. Stakeholders and third parties</b>	152
2.1. Role of JICWEBS and DTSG	152

2.2. <i>Role of signatories</i>	153
2.3. <i>Role of Verification Providers</i>	154
2.4. <i>Role of rightholders</i>	155
2.5. <i>Role of public authorities</i>	155
2.6. <i>Role of civil society</i>	155
<b>3. Duties and procedures</b>	157
3.1. <i>Scope of application of the GPPs</i>	157
3.2. <i>Definition of Likely Infringing Websites</i>	157
3.3. <i>The GPPs</i>	159
<b>4. Coexistence of the measures set forth under the GPPs with European Union and the UK legal frameworks and related case law</b>	165
4.1. <i>Charter of Fundamental Rights</i>	165
4.2. <i>European Union Directives</i>	166
4.3. <i>Fundamental rights in the UK</i>	167
4.4. <i>UK Regulations</i>	169
4.5. <i>Analysis of the GPPs in relation to the European Union and the UK legal frameworks and case law</i>	170
<b>5. Technologies</b>	176
<b>6. Costs</b>	177
<b>7. Education</b>	178
<b>8. Effectiveness</b>	180
<b>Chapter 3: Annex 1</b>	181
1. <i>GPPs (June 2015)</i>	181
1.1. <i>Introduction</i>	181
2. <i>Compliance and Enforcement</i>	182
2.1. <i>Selection of Verification Provider</i>	182
2.2. <i>Independent Policy Verification Process</i>	183
2.3. <i>Reporting</i>	183
2.4. <i>Timing</i>	184
<b>Chapter 3: Annex 2</b>	186
<i>Signatories</i>	186
<b>Chapter 3: Annex 3</b>	188
<i>Evolution of the trading of Display Advertising</i>	188
<b>Chapter 3: Annex 4</b>	190
<b>Chapter 3: Annex 5</b>	192
<i>European Union legal framework</i>	192
<b>Chapter 3: Annex 6</b>	194
<i>UK legal framework</i>	194
<b>Chapter 3: Annex 7</b>	199
<i>CJEU case law</i>	199
<b>Chapter 4: Glossary of terms</b>	205
<b>Chapter 4: Structure and content</b>	208
<b>1 Introduction</b>	209
<b>2. Signatories of the Code and third parties</b>	210
2.1. <i>Role of BREIN</i>	210
2.2. <i>Role of the ECP</i>	210
2.3. <i>Role of Intermediaries</i>	211
2.4. <i>Role of civil society</i>	212
<b>3. Duties and procedures</b>	213
3.1. <i>Scope of application of the VCP</i>	213
3.2. <i>Procedure</i>	213
3.3. <i>Penalties and sanctions</i>	217

<b>3.4. NTD procedure flowchart</b>	218
<b>3.5. NTD in the Netherlands</b>	219
<b>4. Coexistence of the measures set forth under the VCP with European Union and Dutch legal frameworks and related case law</b>	222
4.1. Fundamental rights	222
4.2. European Union Directives	223
4.3. Constitutional prerequisites and fundamental rights in the Netherlands	224
4.4. Dutch Regulations	224
4.5. Analysis of the VCP in relation to the European Union and Dutch legal frameworks and case law	225
<b>5. Technologies</b>	235
<b>6. Costs</b>	236
<b>7. Education</b>	237
<b>8. Effectiveness</b>	238
<i>Future actions</i>	239
<b>Chapter 4: Annex 1</b>	240
<i>BREIN's members</i>	240
<b>Chapter 4: Annex 2</b>	241
<i>Notice-and-take-down Code of Conduct</i>	241
<b>Chapter 4: Annex 3</b>	248
<i>European Union legal framework</i>	248
<b>Chapter 4: Annex 4</b>	252
<i>Dutch legal system</i>	252
<i>The Dutch Civil Code</i>	252
<b>Chapter 4: Annex 5</b>	254
<i>International legal framework</i>	254
<b>Chapter 4: Annex 6</b>	260
<i>Case law</i>	260
<i>Dutch case law</i>	260
<i>CJEU case law</i>	265
<b>Chapter 5: Glossary of terms</b>	269
Chapter 5: Structure and content	272
<b>1. Introduction</b>	273
<b>2. Signatories of the Code of Conduct and third parties</b>	275
2.1. Role of the <i>RettighedsAlliancen</i>	275
2.2. Role of the <i>Danish Ministry of Culture (Kulturministeriet)</i>	275
2.3. Role of intermediaries	276
2.4. Role of civil society	276
<b>3. Duties and procedures</b>	277
3.1. Scope of application of the VCP	277
3.2. Procedure	277
<b>4. Coexistence of the measures set forth under the VCP with the European Union, Danish legal frameworks and related case law</b>	283
4.1. Fundamental rights	283
4.2. European Union Directives and Regulations	284
4.3. Constitutional prerequisites and fundamental rights in Denmark	285
4.4. Danish regulations	285
4.5. Analysis of the VCP in relation to the European Union and Danish legal frameworks and case law	287
4.6. Summary of findings relating to the coexistence of the Code of Conduct with the European Union, Danish legal frameworks and case law	294
<b>5. Technologies</b>	296
<b>6. Costs</b>	297

<b>7. Education</b>	298
7.1. SWC: objectives and target groups	298
7.2. Future actions	300
7.3. Further voluntary collaboration practices derived from the Copyright Package	300
<b>8. Effectiveness</b>	302
<b>Chapter 5: Annex 1</b>	304
<i>The Danish Telecommunications Industry, TI: Code of Conduct for Management of Rulings on Blockings Related to Infringements of Rights</i>	304
<b>Chapter 5: Annex 2</b>	305
<i>Copyright Package</i>	305
<b>Chapter 5: Annex 3</b>	308
<i>Project description</i>	308
<b>Chapter 5: Annex 4</b>	311
<i>List of Teleindustrien members</i>	311
<b>Chapter 5 : Annex 5</b>	312
<i>European Union legal framework</i>	312
<b>Chapter 5: Annex 6</b>	319
<i>Danish legal framework</i>	319
<b>Chapter 5: Annex 7</b>	322
<i>CJEU and Danish case law</i>	322
<b>Chapter 6: Glossary of terms</b>	330
<b>Chapter 6: Structure and content</b>	333
<b>1. Introduction</b>	334
<b>2. RogueBlock participants and third parties</b>	337
2.1. Role of rightholders	337
2.2. Role of public authorities (IPR Center)	337
2.3. Role of the IACC and payment processors	338
2.4. Role of civil society	339
3. Duties and procedures	340
3.1. Scope of application of the VCP	340
3.2. RogueBlock procedure	340
3.3. Other payment processor approaches	346
<b>4. Coexistence of the measures set forth under the RogueBlock with the U.S. legal framework</b>	348
4.1. Fundamental rights in the U.S.	348
4.2. U.S. statutes	348
4.3. Online intermediary liability	350
4.4. Analysis of the VCP in relation to the U.S. legal framework	351
4.5. Summary of findings relating to the coexistence of the RogueBlock with the U.S. legal framework	354
<b>5. Technologies</b>	355
<b>6. Costs</b>	356
<b>7. Education</b>	357
<b>8. Effectiveness</b>	358
8.1. Numbers and statistics	358
8.2. Challenges	358
<b>Chapter 6: Annex 1</b>	359
<b>Chapter 6: Annex 2</b>	360
<i>Fundamental rights in the U.S.A.</i>	360
<i>U.S.A. legal system</i>	360

## Foreword by the Executive Director

The success and growing value of Intellectual Property Rights (IPR) of all kinds has inevitably been accompanied by an increase in activity by those seeking to profit from the misuse of these rights.

Other studies by the EUIPO, through the European Observatory on Infringements of Intellectual Property Rights, have clearly demonstrated the economic value of IPR, the huge cost of infringements to legitimate businesses, and the sometimes ambivalent attitude to these rights by citizens.

In particular, a previous report showed the growth in illicit online business models, where IPR infringements are often built on the misuse of domain names and other digital identifiers.

At the same time, consumers and citizens in the digital world more and more want access to all online information and creative works immediately. The internet has allowed this and many now think that anything available there is, or should be, free and can therefore be reused.

This has created tension between the legitimate rights of the creators and owners and the expectations of many citizens. It has also resulted in a very difficult enforcement environment in which the legal rules that exist have sometimes failed to catch up with the speed of change of technologies and practice.

Since enforcement authorities cannot be expected to be on top of every infringement they have sought other solutions. In the present report, voluntary collaboration practices (VCPs) drawn from five EU Member States and the United States are examined in an independent study in collaboration with top academic experts.

These voluntary practices are intended to respect both the law and the fundamental rights of citizens, while combating online infringements of trade mark rights, design rights, copyright and rights related to copyright. They include codes of conduct and practices for taking down infringing sites, as well as for controlling advertising and the access to online payment systems.

This study casts light on the role of the parties involved, their coexistence with legal frameworks, the role of technology, the costs involved and the role of educational activities.

Inevitably, within such a complex legal and cultural landscape, many differences in approach were found. The study also had to cope with challenges as regards access to data and gaps in the data about the effectiveness of the VCPs examined.

The present study forms part of the ongoing work of the EUIPO, through the Observatory, aimed at both understanding the scale of the problem of IPR infringements and the variety of responses for combating misuse of IPR rights from both the public and the private sectors. It also complements the work on VCPs being carried out in parallel by the European Commission.

Since e-commerce is an increasingly strong force in modern business, representing 17% of all EU business turnover in 2014, tackling the growth in infringements must be seen as an area of major concern for both EU policymakers and businesses alike.



This research, and the evidence that changes in internet practices may often outstrip the ability of legal systems to adapt, underlines the need for efforts to prevent infringements to be smarter, more targeted and more efficient. At the same time, fundamental rights, privacy rights and data protection need to be respected by any VCPs created.

As such, this study deserves careful study by all stakeholders in order to ensure that both the public debate and the policymaking environment are as well informed as possible on this important issue.



**António Campinos**  
Executive Director, EUIPO

## INTRODUCTION AND SUMMARY OF THE RESULTS



## Introduction and summary of the results: Glossary of terms

For the purposes of this introductory chapter:

- **Austrian Copyright Law**: the Austrian Federal Law No 111/1936 of 9 April 1936 on Copyright in Literary Works, Works of Art and Related Rights ('Bundesgesetz über das Urheberrecht an Werken der Literatur und der Kunst und über verwandte Schutzrechte')<sup>1</sup>.
- **Austrian Data Protection Law**: the Austrian Federal Law No 165/1999 on the Protection of Personal Data ('Bundesgesetz über den Schutz personenbezogener Daten')<sup>2</sup>.
- **Austrian VCP**: the Article 1.7 of the ethics code of the Austrian advertising industry and related articles on the rules of procedure of the Werberat.
- **BEUC**: 'Bureau Européen des Unions de Consommateurs', the European consumer organisation.
- **Bonnier CJEU Ruling**: the ruling issued on 13 April 2012 by the CJEU under case C—461/10, *Bonnier v Perfect Communications*.
- **BREIN**: 'Bescherming Rechten Entertainment Industrie Nederland', the Protection Rights Entertainment Industry Netherlands (the BREIN foundation)<sup>3</sup>.
- **Charter of Fundamental Rights**: the Charter of Fundamental Rights of the European Union<sup>4</sup>.
- **CNAC**: the French National Anti-Counterfeiting Committee<sup>5</sup> ('Comité National Anti-Contrefaçon').
- **Danish VCP**: the Danish code of conduct for internet service providers regarding the management of court DNS blocking orders relating to IP infringements.
- **Data Protection Directive**: the Directive of 24 October 1995 on Data Protection<sup>6</sup>. At the moment of the drafting of this Study, the Data Protection Directive was in force. This Directive **has been repealed** by the General Data Protection Regulation on May 2016.
- **Deloitte**: Deloitte Asesores Tributarios, S.L.U.<sup>7</sup>
- **DHPA**: the Dutch Hosting Providers Association<sup>8</sup>.
- **DTSG**: the Digital Trading Standards Group, the standards group within JICWEBS aimed at protecting brand safety and preventing advertising misplacement.
- **Dutch VCP**: the Dutch notice-and-take-down code of conduct directed to internet service providers that provide a public telecommunications service in the Netherlands, which have to deal with reports regarding unlawful content on the internet. The Dutch VCP defines intermediary as a 'provider of a (telecommunications) service on the internet'<sup>9</sup>. The explanatory notes to the code's articles specify that intermediaries can be either a person or an organisation that provides online services for the storage, transmission or provision of information.
- **eBay CJEU Ruling**: the ruling issued on 12 July 2011 by the CJEU under case C-324/09, *L'Oréal vs Ebay*<sup>10</sup>.
- **CJEU**: the Court of Justice of the European Union.
- **E-Commerce Directive**: the Directive of 8 June 2000 on Electronic Commerce<sup>11</sup>.

<sup>1</sup> <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001848>.

<sup>2</sup> <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597>.

<sup>3</sup> <http://www.anti-piracy.nl/english.php>. See complete list of Brein's participants in Annex 1 of Chapter 4 of this study.

<sup>4</sup> Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, pp 391–407.

<sup>5</sup> <http://www.cnac-contrefacon.fr/cnac/>.

<sup>6</sup> Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23/11/1995 pp 0031 – 0050.

<sup>7</sup> Team members: María Vidal, Susana Rodríguez Ballano, Paula Iun, Ana De Lluc Compte, Jaime Pascual, Andrea Sánchez Guarido, Julia Torres.

<sup>8</sup> <https://www.dhpa.nl/>.

<sup>9</sup> Article 1, section b. of the Dutch VCP.

<sup>10</sup> <http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=324/09&td=ALL>.

- **ECIP**: the Dutch Electronic Commerce Platform ('Platform voor de InformatieSamenleving') an independent foundation which is now in charge of the administration and the development of the Dutch VCP.
- **Enforcement Directive**: the Directive of 29 April 2004 on the Enforcement of Intellectual Property Rights<sup>12</sup>.
- **EUIPO**: the European Union Intellectual Property Office (formerly named the Office for Harmonization in the Internal Market (Trade Marks and Designs))<sup>13</sup>.
- **EU Regulation 386/2012**: the Regulation of 19 April 2012 entrusting the EUIPO with tasks related to the enforcement of intellectual property rights<sup>14</sup>.
- **French Data Protection Law**: the French Law No 78-17, of 6 January 1978, regarding IT, Databases and Liberties<sup>15</sup> ('Loi No 78-17 relative à l'informatique, aux fichiers et aux libertés').
- **French E-Commerce Law**: the French Law No 2004-575, of 21 June 2004, regarding Confidence in the Digital Economy<sup>16</sup> ('Loi No 2004-575 pour la confiance dans l'économie numérique').
- **French Enforcement Law**: the French Law No 2007-1544, of 29 October 2007, regarding the Fight against Counterfeiting<sup>17</sup> ('Loi No 2007-1544 de Lutte contre la Contrefaçon').
- **French VCP**: the French charter for the fight against the sale of counterfeit goods on the internet between intellectual property rightholders and e-commerce platforms.
- **IACC**: the International AntiCounterfeiting Coalition.
- **IAB UK**: the Internet Advertising Bureau UK, a trade association related to online advertising<sup>18</sup>.
- **InfoSoc Directive**: the Directive of 22 May 2001 on the Information Society<sup>19</sup>.
- **INPI**: the French National Industrial Property Institute<sup>20</sup> ('L'Institut National de la Propriété Industrielle').
- **ISP Connect**: a Dutch ISP Association<sup>21</sup>.
- **IPEC**: the Intellectual Property Enforcement Coordinator, a government office belonging to the Office of Management and Budget of the U.S.<sup>22</sup>.
- **IPR Center**: the National Intellectual Property Rights Coordinator Center overseen by the U.S. Immigration and Customs Enforcement, which is part of the U.S. Department of Homeland Security Investigations.
- **JICWEBS**: the Joint Industry Committee for Web Standards, an organisation created by the UK media industry<sup>23</sup>.
- **Kino.to CJEU Ruling**: the ruling issued on 27 March 2014 by the CJEU in Case C-314/12, *UPC Telekabel/Constantin Film & Wega Filmproduktionsgesellschaft*<sup>24</sup>.

<sup>11</sup> Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ L 178, 17/07/2000 pp 0001 – 0016.

<sup>12</sup> Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, OJ L 157 of 30 April 2004.

<sup>13</sup> <https://euiipo.europa.eu/ohimportal/es/>.

<sup>14</sup> Regulation (EU) No 386/2012 of the European Parliament and of the Council of 19 April 2012 on entrusting the Office for Harmonisation in the Internal Market (Trade Marks and Designs) with tasks related to the enforcement of intellectual property rights, including the assembling of public and private-sector representatives as a European Observatory on Infringements of Intellectual Property Rights.

<sup>15</sup> <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460>.

<sup>16</sup> <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164>.

<sup>17</sup> <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000279082>.

<sup>18</sup> <https://www.iabuk.net/>.

<sup>19</sup> Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167, 22/06/2001 pp 0010 – 0019.

<sup>20</sup> <http://www.inpi.fr/fr/accueil.html>.

<sup>21</sup> <http://ispconnect.nl/>.

<sup>22</sup> <https://www.whitehouse.gov/omb/intellectualproperty>.

<sup>23</sup> <http://www.jicwebs.org/>.

<sup>24</sup> <http://curia.europa.eu/juris/document/document.jsf?sessionId=9ea7d0f130d5682c6360d7a642ab82679809c8f7b53e.e34KaxilC3eQc40LaxgMbN4ObNmPe0?text=&docid=149924&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=141830>.

- **MOU**: the Memorandum of Understanding on the Sale of Counterfeit Goods<sup>25</sup> of 4 May 2011, concluded at a European Union level under the auspices of the European Commission. On 21 June 2016 a new MoU on the online sale of counterfeit goods was opened for signature.
- **Observatory**: the Observatory on Infringements of Intellectual Property Rights, entrusted to the EUIPO on 5 June 2012<sup>26</sup>.
- **Open Internet Access Regulation**<sup>27</sup>: the Regulation laying down measures concerning open internet access.
- **Promusicae CJEU Ruling**: the ruling issued on 29 January 2008 by the CJEU under case C-275/06, *Promusicae v Telefónica*<sup>28</sup>.
- **SWC**: 'Share with Care', a campaign result of the joint initiative between the Danish Internet Service Providers, Teleindustrien, the Danish Ministry of Culture and RettighedsAlliancen.
- **Teleindustrien**: the Danish telecom industry association<sup>29</sup>.
- **Svensson CJEU Ruling**: the ruling issued on 13 February 2014 by the CJEU under Case C-466/12, *Svensson vs Retriever Sverige*<sup>30</sup>.
- **UK**: the United Kingdom.
- **UK Copyright, Designs and Patents Act**: the Act of the Parliament of the UK of 1988 on Copyright, Designs and Patents<sup>31</sup>.
- **UK Data Protection Act**: the Act of the Parliament of the UK of 1998 on Data Protection<sup>32</sup>.
- **UK Registered Designs Act**: the Act of the Parliament of the UK of 1949 on Registered Designs<sup>33</sup>.
- **UK Trade Marks Act**: the Act of the Parliament of the UK of 1994 on Trade Marks<sup>34</sup>.
- **UK VCP**: the UK good practice principles for the trading of digital display advertising.
- **Umbrella Portal**: the master IACC portal where the complaints and the resolutions are uploaded by the stakeholders involved in the RogueBlock.
- **U.S.**: the United States.
- **U.S. VCP**: the U.S. IACC payment processor initiative & portal program, later named RogueBlock.
- **VCPs**: practices developed by industry, public bodies and/or third parties such as non-governmental organisations which are then adhered to by the respective industry in addressing infringements of trade mark rights, design rights, copyright and rights related to copyright over the internet.
- **Werberat**: the Austrian Advertising Council which is the executive body of the Austrian Society for Advertising Self-Regulation<sup>35</sup>.

<sup>25</sup> [http://ec.europa.eu/growth/industry/intellectual-property/enforcement/index\\_en.htm](http://ec.europa.eu/growth/industry/intellectual-property/enforcement/index_en.htm).

<sup>26</sup> <https://euiipo.europa.eu/ohimportal/en/web/observatory/about-us>.

<sup>27</sup> Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015, laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union. <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R2120&from=EN>.

<sup>28</sup> <http://curia.europa.eu/juris/liste.jsf?language=en&num=C-275/06>.

<sup>29</sup> <http://www.teleindustrien.dk/>.

<sup>30</sup> <http://curia.europa.eu/juris/liste.jsf?num=C-466/12>.

<sup>31</sup> <http://www.legislation.gov.uk/ukpga/1988/48/contents>.

<sup>32</sup> <http://www.legislation.gov.uk/ukpga/1998/29/contents>.

<sup>33</sup> <http://www.legislation.gov.uk/ukpga/Geo6/12-13-14/88/contents>.

<sup>34</sup> <http://www.legislation.gov.uk/ukpga/1994/26/contents>.

<sup>35</sup> <https://www.werberat.at/>.

## 1. Executive summary

This study consists of an analysis of the six following voluntary collaboration practices (VCPs) addressing online infringements of trade mark rights, design rights, copyright and rights related to copyright.

- Notice-and-take-down VCPs:
  - The French charter for the fight against the sale of counterfeit goods on the internet between intellectual property rightholders and e-commerce platforms.
  - The Dutch notice-and-take-down code of conduct directed to internet service providers that provide a public telecommunications service in the Netherlands.
  - The Danish code of conduct for internet service providers regarding the management of court DNS blocking orders relating to IP infringements.
- Advertising related VCPs:
  - Article 1.7 of the ethics code of the Austrian advertising industry and related articles on the rules of procedure of the Werberat.
  - The UK good practice principles for the trading of digital display advertising.
- Payment processor related VCP:
  - The U.S. IACC payment processor initiative & portal program, later named RogueBlock.

The study focusses on the following topics: The role of the parties involved in the VCPs; the duties and procedures envisaged by them; their coexistence with legal frameworks and related case law; the role of technologies used (if any); the costs assumed by parties to the VCPs; the role of educational activities; and the effectiveness of the VCPs.

When drafting the study, a number of difficulties were encountered. Certain categories of stakeholders could not provide input or did not wish to be interviewed (e.g., some national consumer associations, the IACC). Furthermore, in some cases, there is little factual data about the effectiveness of the VCP as it is sometimes not measured.

The VCPs examined share certain commonalities, e.g.:

- They are voluntary and therefore do not impose compulsory sanctions for not complying with the duties and procedures envisaged by them.
- They establish preventive and/or proactive measures in order to prohibit or to detect infringements of intellectual property rights.
- Almost none of the VCPs (except for the UK and the U.S. VCP) involve any costs or fees to stakeholders, though indirect costs may arise in some VCPs in relation to enforcement.

Differences among them have also been identified, e.g.:

- Origin. Initiated following the involvement of public authorities (e.g., French VCP and Danish VCP) vs. created by an industry (e.g., Austrian VCP, UK VCP, Dutch VCP, U.S. VCP).
- Intellectual property rights involved. Copyright and related rights + trade marks + design rights (e.g., UK VCP, Dutch VCP, Danish VCP, U.S. VCP) vs. only certain of such rights (e.g. French VCP and Austrian VCP).
- Structure. Industry Code of Conducts (Dutch VCP, Danish VCP, Austrian VCP, UK VCP) vs initiatives between stakeholders (French VCP, U.S. VCP).
- Costs assumed by parties. Annual adherence fee and costs for verification (UK and U.S. VCPs) vs general costs for detecting infringements (Dutch VCP, Danish VCP, Austrian VCP and French VCP).
- Territorial limit. Connection to the country where the VCP is based (e.g., Austrian VCP, UK VCP, Dutch VCP, Danish VCP) vs. no express territorial limit (e.g., French VCP and U.S. VCP).

- Education. Fewer educational activities (e.g., French VCP) vs. specific educational activities focusing on the VCP (e.g., Austrian VCP, UK VCP, Danish VCP) vs. general educational activities on IP infringements (e.g., Dutch VCP).
- Role of technologies. Use of technologies such as software to detect online infringements, or content verification tools (e.g., French VCP and UK VCP) vs. complaint forms or no role for specific technologies (e.g., Austrian VCP, Dutch VCP, Danish VCP, and U.S. VCP).

After having applied the relevant legal framework and related case law to the various VCPs examined, it has been generally concluded that, mostly, the duties and procedures envisaged by the VCPs do not raise problems with regard to the legal frameworks concerned. However, certain exceptions have been highlighted, namely:

- In France, the retention of personal data related to certain sellers during a five year period to prevent their re-registration in e-commerce platforms and the duty to store certain documents relating to other sellers after closure of their accounts for the same period of time might raise issues with regards to the right to the protection of personal data of the sellers concerned.
- In the Netherlands, intermediaries are in charge of the removal of any content considered 'unlawful' or 'undesirable'. Courts have not yet established any parameters that may be followed in order to perform an appropriate evaluation procedure for these considerations. Consequently, intermediaries could be subject to certain arguments that their action is in conflict with the freedom of expression of the content provider. Pursuant to the information obtained in the interviews carried out, intermediaries do not usually remove content which is not clearly illegal according to their evaluation process in order to avoid any risk. In such cases, they recommend following a judicial procedure for determining if the disputed content is illegal and ordering its removal
- Also, in the Netherlands the disclosure of the content provider's personal data by the intermediary to the notifier is subject to a balancing test and is allowed in situations where the balance undertaken implies that the interest of the notifier should prevail.

As regards the data available in relation to the effectiveness of the VCP, the following can be stated:

- The information that could be found stems either from an assessment of the application of the VCP by a public body (French VCP), a report or figures published by the organisation or industry body administering the VCP (U.S. VCP, UK VCP, Austrian VCP, Danish VCP) or figures mentioned by rightholder associations (Dutch VCP).
- The type of information available can include aspects such as the number of rightholder complaints and their outcome (Austrian VCP), the number of website blockings (Danish VCP, Dutch VCP), the number of merchant accounts closed (U.S. VCP) or the number of accounts suspended for the sale of counterfeit products (French VCP).

The study and the conclusions reached are based on information obtained both from an exhaustive desk research and from the feedback and supporting documentation provided by certain stakeholders and third parties involved in the VCPs that have agreed to participate in the study.

The study has been drafted following close collaboration between Deloitte and two experts in intellectual property law, Prof. Dr. Thomas Hoeren and Prof. Dr. Guido Westkamp, who supervised all of the work. In addition, local law firms have supported the analysis of the impact of applicable law on the VCPs.



## 3. Introduction

### 3.1. Context

EU Regulation 386/2012 entrusted the EUIPO with tasks aimed at facilitating and supporting the activities of national authorities, the private sector and the European Union institutions in their fight against the infringement of intellectual property rights. In carrying out these tasks the EUIPO, acting through the Observatory, is supporting the enforcement of intellectual property rights and helping combat the growing threat of intellectual property rights infringement.

Considering the mission and the range of activities defined in Regulation 386/2012, the EUIPO has set out main goals for the Observatory which include the provision of facts and evidence for use in the formulation of effective intellectual property policies by policymakers and the creation of resources to aid the fight against infringements of intellectual property rights. These goals will be achieved by implementing identified key initiatives, which are defined taking into account the input and feedback received from Member States, European Union institutions and the Observatory stakeholders. One of the key initiatives of the Observatory is contributing to the combatting of the infringement of intellectual property rights on the internet by providing data to support European Union and national authorities.

At international, European and national levels numerous legislative measures have been adopted to help protect and enforce intellectual property rights on the internet. At European Union level the Enforcement Directive harmonises civil enforcement measures and remedies that are applicable to intellectual property rights infringements in the European Union Member States and requires all Member States to apply effective, dissuasive and proportionate remedies against those engaged in infringements of intellectual property. The E-Commerce Directive defines limitations on the liability of internet service providers. Article 16 of the Electronic Commerce Directive indicates that Member States and the Commission shall encourage the drawing up of codes of conduct at Community level, by trade, professional and consumer associations or organisations, designed to contribute to the proper implementation of the Directive.

The regulatory approaches in the enforcement of intellectual property rights have been complemented by a range of non-legislative initiatives implemented within and outside the European Union. Article 17 of the Enforcement Directive encourages the development, by trade or professional associations or organisations, of codes of conduct at Community level aimed at contributing towards the enforcement of the intellectual property rights. At the European Union level, the European Commission has been conducting stakeholder dialogues which brought together a group of stakeholders to discuss specific problems in the field of intellectual property enforcement and explored possible methods of voluntary cooperation in compliance with the existing legal framework. In this framework the MOU was signed, which aims at enhancing the collaboration between signatories in the fight against the sale of counterfeit goods over the internet.

The Observatory is supporting the European Commission in the implementation of the existing MOU, as well as in the implementation of the European Union Action Plan on Enforcement of intellectual property rights which, inter alia, deals with stakeholder dialogues.

### 3.2. Purpose of the study

After identifying, with the assistance of its stakeholders, VCPs existing within the European Union as well as some VCPs from third countries, six of the identified practices were selected for an in-depth assessment. The EUIPO entrusted to Deloitte the drafting of a study, the main objective of which is to perform an analysis on the basis of defined criteria relating to these six VCPs addressing online infringements of trade mark rights, design rights, copyright and rights related to copyright.

In the context of this study, VCPs refer to practices developed by industry, public bodies and/or third parties such as non-governmental organisations which are then adhered to by the respective industry in addressing infringements of trade mark rights, design rights, copyright and rights related to copyright over the internet.



### 3.3. Scope

The following VCPs are analysed in the context of this study:

- French VCP: The French charter for the fight against the sale of counterfeit goods on the internet between intellectual property rightholders and e-commerce platforms.
- Austrian VCP: Article 1.7 of the ethics code of the Austrian advertising industry and related articles on the rules of procedure of the Werberat.
- UK VCP: The UK good practice principles for the trading of digital display advertising.
- Dutch VCP: The Dutch notice-and-take-down code of conduct directed to internet service providers that provide a public telecommunications service in the Netherlands.
- Danish VCP: The Danish code of conduct for internet service providers regarding the management of court DNS blocking orders relating to IP infringements
- U.S. VCP: The U.S. IACC payment processor initiative & portal program, later named RogueBlock.

The Observatory has selected the mentioned VCPs based on the following criteria:

- Wide variety of contexts in which voluntary collaboration takes place, i.e., collaboration with ISPs, practices involving market place operators/e-platforms, payment providers and advertisers.
- Practices coming primarily from EU Member States.
- The choice of VCPs was discussed and coordinated with the IP in the Digital World Working Group members.

This study analyses in depth the application of the selected VCPs by assessing the following elements:

- Role of the parties involved in the implementation of the VCPs.
- Analysis of the duties and procedures prescribed by the VCPs.
- Coexistence of the measures established under the VCPs with local legal frameworks and related case law and, where applicable with European Union legal framework. In this regard, the analysis of any potential impact of competition law on the VCPs is outside of the scope of the study.
- Role of technologies used in implementing the duties and procedures envisaged by the VCPs.
- Costs assumed by the parties involved in the implementation of the VCPs.
- Role of educational activities of the parties involved to promote the VCPs.
- Effectiveness of the measures established by the VCPs.

### 3.4. Methodology

#### 3.4.1. Phases

##### 3.4.1.1. First steps

In undertaking this study, an exhaustive preliminary desk research has been performed by Deloitte so as to identify the sources of information for each VCP. This desk research has been essential in order to determine the basis on which the further analysis of the selected VCPs should be conducted.

For each selected VCP, the two (2) following groups of sources of information have been identified as a result of the desk research performed:

- Primary sources: i.e., key stakeholders (rightholders, public authorities, intermediaries, civil society, etc.).
- Secondary sources: i.e., IP studies, articles from antipiracy organisations, reviews of stakeholders, news, landmark judgments, educational activities, legal frameworks.

### *3.4.1.2. Phase 2: Deep dive*

After having conducted the preliminary desk research and having established the relevant primary and secondary sources of information for each selected VCP, Deloitte has analysed in depth the mentioned VCPs as well as all related information and documentation.

A sampling of stakeholders related to each selected VCP has been contacted and some of them have consented to be interviewed for the purposes of this study, whilst others have declined the invitation to participate.

To conduct the interviews, customised questionnaires have been prepared for each selected VCP and each category of stakeholders. Stakeholders have been interviewed through conference calls in order to go through the questionnaires and gain as much information as possible about the selected VCPs and their background. After having interviewed the stakeholders, each selected VCP was mapped with all the information gathered and its duties and procedures were studied in depth.

Once all interviews had been carried out, after the mapping for each selected VCP, Deloitte re-contacted certain stakeholders in order to confirm and to clarify certain aspects.

### *3.4.1.3. Phase 3: Drafting process*

On the basis of the mapping and all the information gathered, Deloitte has drafted, for each selected VCP, a chapter covering the items mentioned under Section 2.3 ('Scope').

The statements contained in the study about the stakeholders' position regarding the VCPs and their day-to-day handling are based on the feedback and supporting documentation provided by the stakeholders that have agreed to participate in the study.

The drafting process has been performed through a close collaboration between Deloitte and two experts in intellectual property law, who have supervised all of the work: Professor Thomas Hoeren and Professor Guido Westkamp.

In addition, local law firms have assisted Deloitte in the analysis of the impact of applicable law on the VCPs. In particular, they have provided feedback on possible collisions between the VCPs and European law, where applicable, and national law and related case law as well as on the impact of fundamental rights and data protection rules on the VCPs.

## **3.4.2. Practical challenges**

The following difficulties were encountered while conducting this study:

- Several national consumer associations have been contacted in order to gather their opinions about the selected VCPs. Unfortunately, the majority of them could not or did not provide any input to this study and indicated that they were not interested in participating in it. Consumer associations that decided to participate in the study were not fully involved in the enforcement of intellectual property rights but they were willing to discuss the VCP after having analysed it.
- However, at the European level, BEUC has been very receptive to participate and to provide its comments. BEUC's considerations on the enforcement of Intellectual Property Rights through VCPs in light of consumers' rights have been taken into account (for details, the reader is referred to the in-depth analysis of the Dutch VCP).
- In relation to certain of the VCPs analysed, stakeholders have not measured the effectiveness of the VCPs. In these cases, little factual data about the effectiveness of the VCP has been provided by them. Therefore, it was difficult to assess the effectiveness of certain of the selected VCPs.
- Regarding the U.S. VCP, the IACC was contacted. However, while the IACC affirmed its belief in the effectiveness of voluntary cooperation practices, it did not wish to be interviewed for this study. Thus, in relation to the U.S. VCP and its procedure, the study is based on information publicly available and the statements provided by certain stakeholders.

## 4. General characteristics of the selected VCPs

Section 3.1 provides a summary of the main aspects of each of the VCPs examined. More detail on each practice can be found in the comparative table in section 3.2. The full analysis of each practice is set out in the respective chapter of this study dedicated to that particular VCP.

### 4.1. Summary of the VCPs analysed

#### 4.1.1. The French charter for the fight against the sale of counterfeit goods on the internet between intellectual property rightholders and e-commerce platforms (French VCP)

The French VCP was concluded in December 2009 after an initiative of the French Government and implemented in February 2012. It is aimed at protecting trade mark and design rights and provides preventive measures and reactive procedures in order to fight against the sale of counterfeit goods on the internet.

Signatories of the French VCP are mainly rightholders and e-commerce platforms. The application of the French VCP is not limited by territory. It is addressed to any rightholder or e-commerce platform in the world. It is the aim that the stakeholders work together under the French VCP. Rightholders give advice to the e-commerce platforms on how to distinguish original products from counterfeit products. E-commerce platforms commit themselves to establish preventive and technical measures to detect counterfeit goods being offered as well as measures to identify such sellers of counterfeit goods. Therefore, corresponding software might have to be installed. In addition to that, e-commerce platforms are obliged to establish notification procedures that are addressed to both, rightholders and consumers.

Two public bodies, the INPI and the CNAC, worked on the draft of the French VCP. INPI supervises in terms of debate and discussion with the rightholders and e-commerce platforms and is responsible for the provision of administrative and informative support when a new signatory wants to join the French VCP. In such cases, it informs the already existing signatories and requests their opinion.

Under the VCP, e-commerce platforms commit to taking both preventive and reactive measures. The French VCP binds e-commerce platforms to implement preventive measures before an offer of a counterfeit good is submitted and published by a seller. The effectiveness depends, inter alia, on the exchange of information between the two parties.

It also provides for proactive measures against the selling of counterfeit goods that are addressed to e-commerce platforms after an offer is submitted by the seller. E-commerce platforms can identify sellers and use automatic tools to detect the offers and sellers. Notification mechanisms can be made available to both, rightholders and consumers. Furthermore, documents that are proof of the authenticity of the offered product can be requested.

The selling of a counterfeit product can be sanctioned by the e-commerce platform by the take-down of the offer. The re-publication of the offer in relation to the counterfeit good has to be prevented and the seller can be suspended from the platform for a period of six months. In cases where there has been repetition, the seller can be banned for any re-registration from the e-commerce platform for a period of five years.

E-commerce platforms have to ask sellers that are likely to sell counterfeit products for documentation that can prove the authenticity of the products sold. Sellers that fail to do so can be suspended, their accounts can be closed and their re-registration can be prevented for a period of five years.

In cases where the sellers are from outside the European Economic Area or if the product sold is located anywhere outside the European Economic Area, e-commerce platforms have to request from sellers' documentation proving that they have received and hold an authorisation from the relevant rightholder to sell the product. In cases of sellers failing to do so, the offer can be withdrawn and the account of the seller can be closed without any time limitation if further offers are detected.

However, there are no consequences for the signatories for not complying with their aforementioned duties arising from the French VCP. Adherence to the French VCP is voluntary. Signatories are free to implement the measures for cooperation on a voluntary basis or to implement other measures that they consider appropriate.

No fees arise for signatories as a consequence of their adherence to the French VCP. The only costs that may arise for e-commerce platforms are personnel or software costs.

Signatories or the INPI are generally not undertaking educational activities.

In a review of the VCP in December 2009, signatories considered that the objectives of the French VCP had been broadly achieved. The two e-commerce platforms that had signed the French VCP at the time of review in 2009 reported that the selling of counterfeit goods via their platforms had decreased.

#### 4.1.2 The Article 1.7 of the ethics code of the Austrian advertising industry and related articles on the rules of procedure of the Werberat (Austrian VCP)

The Austrian VCP established in April 2014 is part of the self-regulatory Ethics Code of the Austrian Advertising Industry which aims to prevent the misuse of advertising and aims to ensure that the interests of consumers as well as those of the advertising industry are fairly represented. The Austrian advertising industry imposed the Ethics Code on its work voluntarily.

According to the Austrian VCP, it is contrary to general advertising principles to place an advertisement in unlawful advertising environments<sup>36</sup> (such as a website, a banner advertising or a spot on the internet). The Austrian VCP is directed at protecting copyright and related rights.

The territorial scope of application of the Austrian VCP is limited to advertisers that are based in Austria and to advertisements that are directed to an Austrian audience<sup>37</sup>. Furthermore, the Austrian VCP does not apply to political and election advertising, publications promoting the arts and culture alone, or the advertising of and for non-profit organisations.

The Werberat is the body that receives and deals with complaints that have been filed through its website from associations - namely mostly those that combat intellectual property rights infringement - regarding advertising they consider having been placed in environments breaching copyright. The Werberat also carries out the preliminary examination of the complaint. If the Werberat considers a complaint as justified (in German 'begründet'), it issues a request to the advertising agency or the advertiser, asking for their opinion within three working days. The requests of the Werberat are not legally binding for the advertiser. Although, the Werberat cannot sanction copyright infringements, most advertisers remove the criticised advertisement. In case the advertiser agrees to discontinue the campaign, no further actions are taken. However, if the advertiser considers the complaint unfounded and does not agree to discontinue the advertisement, the complaint and the grounds for the advertiser's disagreement are forwarded to the Small Senate which examines them. Advertisers that do not agree with the decision of the Small Senate can then file an appeal to the Ethics Senate.

No fees arise for signatories as a consequence of their adherence to the Austrian VCP. The only indirect costs that may arise are for signatories are personnel costs. News or information about the Austrian VCP as well as the decisions of the Werberat are available on the website of the Werberat. According to the Werberat, upon their request all contacted advertisers removed their advertising from the identified advertising environments.

#### 4.1.3. The UK good practice principles for the trading of digital display advertising (UK VCP)

The UK VCP was established in December 2013 with the intent to prevent abusive digital display advertising. It was drafted by the Digital Trading Standards Group (DTSG), which is part of the Joint Industry Committee for Web Standards (JICWEBS), whose aim is the protection of brand safety in the advertising context.

---

<sup>36</sup> European Digital Rights (EDRi), an association of civil and human rights organisations from across Europe, in commenting on a draft of this Chapter 3, stated 'the term advertising environment breaching copyright is not a legal term and, in all cases, it is used to refer to online resources that are either assumed or alleged to be involved in 'obvious' breaches of copyright. It is therefore inappropriate to use this term without using the word 'alleged', regardless of whether the bureaucratic procedure of the Werberat has been followed or not'.

<sup>37</sup> It may be extracted from CJEU rulings that the following criteria, inter alia, may determine that advertising is addressed to an Austrian audience: (i) use of German language; (ii) use of Austrian telephone numbers of contact purposes; or (iii) use of a '.at' domain name.

The practice is directed at protecting copyright and related rights as well as trade marks and design rights. The aim is to reduce the risk of digital display advertising misplacement by introducing transparency to the market.

The VCP is addressed to the following businesses from the advertising industry: sellers, buyers and facilitators. Sellers are commercial enterprises which sell goods directly or are responsible for the placing or display of an advertisement on digital media properties. Buyers are businesses that buy such display advertising from the seller. Facilitators are businesses that provide the technology platform with the aim of brokering the advertising placement with buyers and sellers. Another stakeholder is the verification provider, who, as an independent auditor, has the task of demonstrating that signatories comply with the standards of the UK VCP. IP rightholders are also stakeholders in the VCP.

The scope of the VCP is limited to businesses of the advertising industry with a UK presence, targeting UK audiences or users. It applies to any kind of misplacement.

The VCP sets out six principles:

1. Trading activities of the seller and the buyer are formalised and concluded under clear terms for their trading activities.
2. The seller and the buyer have to indicate and agree on where the advertisement should (not) appear. They also have to establish mechanisms to minimise any misplacement (special software might have to be installed to that effect).
3. The seller has to confirm whether the measures apply and has to inform the buyer about the provisions that they apply in order to avoid any misplacement of the advertisement.
4. The seller explains its specific provisions in order to minimise the misplacement or its statement of reasonable endeavours. Furthermore, the seller commits itself to inform the buyer about the process supporting the measures implemented.
5. If, however, those measures do fail and an advertisement has been misplaced, the seller and the buyer commit themselves to the contractual consequences that they have previously agreed on.
6. Signatories have to facilitate a procedure with the aim of reducing advertising misplacement approved by JICWEBS and verified by a verification provider.

The UK VCP involves some fees. Firstly, signatories have to pay an annual fee amounting to £943 for their adherence to the GPPs. Secondly, the verification process is subject to a fee which varies depending on the verification provider engaged. For example, one of the verification provider's fees start at £2,839.

In the UK, some activities for education have been carried out. There is educational information available both on the websites of JICWEBS and of IAB UK.

The UK VCP does not contain any sanctions that could be imposed on the signatories for not complying with their VCP duties.

According to the 'Progress Report' released by JICWEBS on 12 February 2015 concerning the effectiveness of the UK VCP, it was expected that by 2015 ninety per cent (90%) of the display advertising market would involve signatories of the UK VCP.

#### 4.1.4. The Dutch notice-and-take-down code of conduct directed to internet service providers that provide a public telecommunications service in the Netherlands (Dutch VCP)

The Dutch VCP was concluded in October 2008 by an initiative of the Dutch Minister of Economic Affairs and the Dutch Ministry of Justice and is the oldest of the six examined VCPs. It is addressed to internet service providers and supplies them with a procedure to deal with reports of unlawful and undesirable content on the internet. The Dutch VCP is directed at ensuring that a report is always dealt with and that unlawful or undesirable content that conflicts with the law of the Netherlands will be removed from the internet. Reports can involve not only intellectual property rights but can be based on any kind of content that is unlawful in the Netherlands.

The Dutch VCP applies to rightholders and intermediaries. Stakeholders of the Dutch VCP are rightholders, the BREIN, intermediaries, namely internet service providers, and the ECP. BREIN is a private rightholder association and deals with the majority of reports and claims in front of Dutch courts. The ECP is an independent foundation which acts as an open and independent platform and is in charge of the administration of the VCP. The intermediaries involved in the practice are the internet service providers.

The territorial scope of application is limited to intermediaries that provide telecommunication services on the internet in the Netherlands. Furthermore, the allegedly unlawful content has to be in conflict with the law of the Netherlands and has to be available to the public on the internet.

Intermediaries can subscribe to the Dutch VCP or draft their own notice-and-take-down code of conduct. The VCP does not require any special technology. Neither does the subscription to the Dutch VCP cause any costs or fees. The intermediaries provide information about the VCP to their members.

Under the Dutch VCP, the intermediary has to be notified through a report from a public prosecutor or a report from a notifier and has to decide whether to take the content down or not, if unlawful content has been detected on the internet. The Dutch VCP is voluntary and not mandatory. Therefore it does not contain any sanctions that could be imposed.

There are not any known educational activities directed towards consumers in the Netherlands.

As regards the effectiveness of the Dutch VCP, in light of the data published by one of the hosting providers, Leaseweb, and from BREIN, it is apparent that a high number of websites with illegal content have been removed since the establishment of the Dutch VCP in 2008.

#### 4.1.5. The Danish code of conduct for internet service providers regarding the management of court DNS blocking orders relating to IP infringements (Danish VCP)

The Danish VCP was concluded in September 2014. The Danish Ministry of Culture launched the 'Copyright Package' in 2012. The Copyright Package contained eight initiatives which have been implemented gradually, one of them being the aforementioned Danish VCP. The Danish VCP is aimed at establishing procedures to be followed by internet service providers and copyright owners in order to block access to illegal services on the internet and to simplify efficient implementation of decisions regarding DNS blocking through court orders. The Danish VCP applies to all types of intellectual property rights, especially copyright and trade marks, and their infringement. It only applies to DNS blocking.

Stakeholders of the Danish VCP are the RettinghedsAlliancen, intermediaries, namely internet service providers, the Danish Consumer Council and the Danish Ministry of Culture. The RettinghedsAlliancen is an alliance of Danish rightholders and is formed by different organisations belonging to the creative industries, e.g., film, music, text and design industry. Its aim is to enforce the rights of their members and to protect the conditions on which cultural content is offered on the internet. The RettinghedsAlliancen initiates the blocking procedure under the Danish VCP through notifications concerning court resolutions regarding DNS blocking. They also collect evidence and act on behalf of the rightholders in front of Danish courts. The Danish Consumer Council protects consumers' rights in the market and is part of the Danish 'SWC'.

The territorial scope of application of the Danish VCP is limited to Denmark and the Danish internet service providers. Furthermore, the court's resolution must derive from a court in Denmark.

Under the Danish VCP rightholders or the RettinghedsAlliance can initiate a procedure by presenting a claim in front of a Danish court alleging that there exists a website that infringes intellectual property rights. When the procedure starts, the court assesses the infringement alleged by the rightholder, and also informs those people or entities responsible for the conflictive website about the court process and invites them to be involved in it.

If the court resolves in favour of the rightholder, the RettinghedsAlliancen sends the court ruling to the intermediaries and provides a list indicating the particular websites/domains that ought to be blocked. The intermediaries have to implement the blocking within a time-limit of seven days from the notification. As soon as the website has been blocked, a communication of the SWC will be displayed on the website. It redirects consumers to legal alternative websites. SWC refers to the 'Share with care' campaign run by the Danish internet service providers, the Teleindustrien, the Danish Ministry of Culture and the RettinghedsAlliancen.



The subscription to the Danish VCP does not require any special technology. Furthermore, the signatories bear their own costs. No fees arise.

As, it is very likely that the removed websites may return to the internet, e.g., by using another domain, the Danish VCP was amended in 2015. Rightholders will now have the possibility of reporting such movement and the new page will also be blocked by the internet service provider if rightholders guarantee that it has exactly the same content as that covered by the website subject to the prior court ruling.

The Danish VCP is not mandatory but voluntary. It does not contain any penalties or sanctions. Naturally, if the internet service provider to whom the court order is addressed does not comply with that order, they would be subject to sanctions under Danish law.

'The Guide Book of Digital User Behaviour'<sup>38</sup>, published by SWC, reports that, since the implementation of the Danish VCP in September 2014, a high number of websites with illegal content have been blocked. Likewise, due to a proliferation of legal services, such as streaming services for music, the use of illegal websites and resulting copyright infringements are said to have decreased.

#### 4.1.6. The U.S. IACC payment processor initiative & portal program, later named RogueBlock (U.S. VCP)

The U.S. VCP was concluded in January 2012. The Intellectual Property Enforcement Coordinator (IPEC) is a government office that is dedicated to the protection of the American intellectual property. The IPEC's strategy is based on the encouragement of the private sector to effectively combat acts of infringement and the facilitation of cooperation in order to reduce intellectual property infringements occurring over the internet. As a consequence of this new strategy, a variety of voluntary practices were adopted among intermediaries of the private sector aimed at curbing the sale of counterfeit goods and reducing online piracy.

The U.S. VCP is a collaborative effort of the IACC and the payment industry itself. It aims at creating an easy procedure for members (rightholders) to report online sellers of counterfeit goods directly to payment processors and thereby to better protect trade marks, design rights and copyright.

Stakeholders are the IACC, rightholders, payment processors and the IPR Center. The IACC is a not for profit organisation. Its main objective is the protection of intellectual property rights and the prevention of counterfeiting and piracy. Rightholders are the owners of intellectual property rights. They have the possibility to report online sellers of counterfeit goods to the IACC by submitting complaints. Such complaints will be forwarded to the payment processors. Payment processors are partnered with the IACC to identify and take remedial actions against sellers of counterfeit goods on the internet that use their payment services in order to sell these goods.

The territorial scope of the U.S. VCP is not limited to the U.S. In fact, it addresses rightholders and payment processors worldwide.

Rightholders submit their complaint to the IACC which reviews each complaint for sufficiency and compliance. The complaint is made via an online report through the so-called 'Umbrella Portal'. The Umbrella Portal is the master IACC portal and is available on the website of the U.S. VCP.

After the IACC reviews the content of the complaint, an attempt to make an online purchase by using a valid but 'set-to-decline', credit card will be conducted. In order to gather the needed information from each transaction, the IACC uses the transaction records. Such information usually contains the merchant's name, their ID number and country. The IACC then contacts the IPR Center. The IPR Center is the National Intellectual Property Rights Coordinator and is overseen by the U.S. Immigration and Customs Enforcement. If the IPR Center considers that the U.S. VCP procedure can interfere with an on-going investigation or may have criminal implications, it will place a hold on the complaint. In case the IPR Center places a hold on the complaint or decides to start its own investigation due to criminal implications or criminal liability, the procedure under the U.S. VCP stops at that point. If the IPR Center does not place a hold on the complaint, the information will automatically be available to the payment processor. The

---

<sup>38</sup> [http://kum.dk/uploads/tx\\_templavoila/SWC\\_guidebook.pdf](http://kum.dk/uploads/tx_templavoila/SWC_guidebook.pdf)

payment processor accesses the information via the Umbrella Portal. It will check if there is a real payment account on the website concerned. If a real and active payment account exists, the payment processor will analyse the information submitted by the rightholder. Each payment processor will notify its decision and the corresponding remedies as soon as the investigations are completed.

The U.S. VCP does not contain any penalties or sanctions. It is voluntary and not mandatory.

The IACC carries the relevant costs in relation to the Trace Messages. The main cost that may arise for rightholders and e-commerce platforms originates from the need to hire internal or external staff who will be responsible for dealing with the merchant's accounts investigations.

A consumer education campaign to increase awareness of the risks associated with shopping on counterfeit websites was carried out by the IACC after the U.S. VCP was launched. In addition, the IACC organises educational activities for general consumers and users and also events such as the so-called 'Spring Conference' or 'Fall Conference' for industry stakeholders.

Pursuant to the information provided on the IACC website, since the implementation of the U.S. VCP in 2012 the program 'has terminated over 5,000 individual counterfeiters' merchant accounts, which has impacted over 200,000 websites'.

















## 4.2. Comparative table

Country	French VCP	Austrian VCP	UK VCP	Dutch VCP	Danish VCP	U.S. VCP
Date of entry into practice	Concluded in December 2009. After a testing period of 18 months, implemented in February 2012.	April 2014	December 2013	October 2008	September 2014	January 2012
Purpose	Provides a set of preventive measures and reactive procedures to fight against the online sale of counterfeit products.	Establishes that the placing of advertising in unlawful advertising environments (e.g., website, banner advertising) is contrary to general advertising principles and sets forth a procedure to fight against it.  The study focuses exclusively on advertising environments breaching copyright.	Outlines six commitments for all businesses involved in the buying, selling or facilitating of display advertising.  Its main aim is to set out good practices for reducing the amount of advertising that appears on likely infringing websites, i.e., digital media properties likely infringing intellectual property rights.	Establishes a procedure for internet service providers which have to deal with reports of unlawful and undesirable content on the internet.  In this regard, the main purpose of Dutch VCP is to ensure that:  (i) a report is always dealt with and  (ii) the unlawful and undesirable content is removed from the internet.	Establishes the procedures to be followed by communication operators and copyright owners in relation to the blocking of access to illegal services on the internet.  The Danish VCP aims to simplify an efficient implementation of decisions regarding DNS blocking through court orders.	It is a collaborative effort of the IACC and the payment industry to create an easy procedure for members to report online sellers of counterfeit goods or pirated content directly to payment processors.
Intellectual property rights concerned	- Trade marks - Design rights	- Copyright and related rights	- Copyright and related rights - Trade marks - Design rights	- Copyright and related rights - Trade marks - Design rights	- Copyright and related rights - Trade marks - Design rights	- Copyright and related rights - Trade marks - Design rights

Country	French VCP	Austrian VCP	UK VCP	Dutch VCP	Danish VCP	U.S. VCP
Stakeholders participating actively in the VCP or affected by it	<p><b>Signatories</b></p> <ul style="list-style-type: none"> <li>- Rightholders representing any intellectual property rights in relation to physical goods. Their main role is to collaborate with signatory e-commerce platforms and to teach them about how to distinguish counterfeit goods from genuine ones.</li> <li>- E-commerce platforms. Their main role is to implement (i) preventive measures; (ii) technical measures; and (iii) notification procedures addressed to rightholders and e-commerce platform</li> </ul>	<p><b>Werberat</b></p> <ul style="list-style-type: none"> <li>- The Office of the Werberat receives complaints regarding advertising environments breaching copyright and carries out the preliminary examination thereof.</li> <li>- Complaints are forwarded to the Small Senate if they are considered justified (in German 'begründet'), by the Office but the advertiser does not discontinue the campaign or does not provide a response to the Office's request to issue an opinion.</li> <li>- If advertisers do not agree with the Small Senate's decision they may file an appeal before the Ethics Senate.</li> </ul>	<p><b>JICWEBS.</b> Reviewed the VCP and adopted it as an industry standard. It hosts the UK VCP, approves verification providers, conducts independent reviews and appeals, reviews the signatories' submissions and publishes the list of signatories.</p> <p><b>DTSG.</b> It proposed the UK VCP to JICWEBS and updated the VCP in June 2015</p> <p><b>Signatories.</b> All businesses involved in the buying, selling or facilitating of display advertising can be signatories of the UK VCP. They have to implement advertising misplacement minimisation policies and have them independently verified.</p>	<p><b>BREIN</b></p> <ul style="list-style-type: none"> <li>- Private rightholders association in the Netherlands and a central contact for rightholders, government, law enforcement bodies, trade and media regarding issues concerning the unauthorised copying and distribution of entertainment products, both offline and online.</li> <li>- Deals with the majority of reports and claims before Dutch courts.</li> </ul>	<p><b>RettighedsAlliancen</b></p> <ul style="list-style-type: none"> <li>- Danish Rightholder Alliance. It is formed by different organisations belonging to the creative industries such as film, music, text and design industry, with the aim of enforcing their members' rights and protecting the conditions under which cultural content is offered on the internet.</li> <li>- Their role within the Danish VCP is the initiation of the blocking procedure by notifying Teleindustrien the court resolutions regarding DNS blocking. They collect evidence and act on behalf of the rightholders at court.</li> </ul>	<p><b>Rightholders.</b> Owners of the intellectual property rights in relation to physical goods and digital content.</p> <p>Their main role is to report online sellers of counterfeit goods or pirated content to the IACC by submitting complaints which will be forwarded to the payment processors.</p>
	<p><b>Public authorities</b></p> <ul style="list-style-type: none"> <li>- INPI. It supported the CNAC in the drafting of the French VCP. Currently, it has a supervisory role linked to the discussion with stakeholders about the French VCP. When new signatories would like to join the French VCP, it is responsible for providing administrative support.</li> <li>- CNAC. The drafting of the French VCP was entrusted by the French Minister of Economy to the CNAC. Currently, the CNAC does not participate actively and directly in the French VCP.</li> </ul>	<p><b>Association whose main purpose is to fight against intellectual property rights infringements.</b> They are the only ones allowed to submit complaints to the Werberat in the context of the Austrian VCP. They have been the drivers of the Austrian VCP.</p>	<p><b>Verification providers.</b> They carry out an independent assessment and issue a report on whether signatories have implemented the required policies.</p>	<p><b>ECP</b></p> <ul style="list-style-type: none"> <li>- It is an independent foundation which acts as an open platform used by different bodies, for the purpose of exchanging information and knowledge, and joining forces to foster the development of information in the Netherlands.</li> <li>- It did not have an active role in the development of the Dutch VCP at its very beginning but its involvement increased after the Dutch VCP was launched. It is now in charge of the administration and the development of the Dutch VCP.</li> </ul>	<p><b>Danish Ministry of Culture.</b> Public body devoted to the development of the cultural policy in Denmark. It launched in 2012 a copyright package with eight initiatives regarding the defence of intellectual property rights.</p> <p>The Danish Ministry of Culture invited Teleindustrien to adopt Danish VCP as one of the initiatives ('Guidelines for the blocking of illegal services on the internet') of the Copyright Package.</p> <p>Nonetheless, this body did not play an active role within this VCP, as they only took part in the proposal and worked upon the invitation of drafting the Danish VCP.</p>	<p><b>IACC</b></p> <ul style="list-style-type: none"> <li>- The IAC is a non-profit organisation and has as its main objective the protection of intellectual property rights and the deterring of counterfeiting.</li> <li>- The IACC administers and manages the U.S. VCP and the system created to share information between rightholders and payment processors.</li> </ul> <p><b>Payment processors.</b> They are partnered with the IACC to identify and take remedial actions against the online sellers of counterfeit goods or pirated content that use their payment services to sell these goods.</p>

Country	French VCP	Austrian VCP	UK VCP	Dutch VCP	Danish VCP	U.S. VCP
Stakeholders participating actively in the VCP or affected by it	<ul style="list-style-type: none"> <li>- <b>Civil society.</b> They did not collaborate in the drafting of the French VCP and they do not participate in it currently.</li> </ul>	<ul style="list-style-type: none"> <li>- <b>Advertisers / agencies.</b> If the Werberat considers a complaint justified (in German, 'begründet'), it issues a request to the agency / advertiser who placed the advertising to issue an opinion.</li> </ul>	<p><b>Rightholders.</b> Entities holding any intellectual property rights, whose rights may be infringed by intellectual property infringing websites.</p>	<p><b>Intermediaries.</b> Any company or individual which provides third parties access to the internet. They play a key role in the Dutch VCP since they are the ones taking down the allegedly unlawful or undesirable content.</p>	<p><b>Intermediaries</b></p> <ul style="list-style-type: none"> <li>- Teleindustrien acts as the nucleus between all parties involved in the VCP. This body is in charge of receiving claims from rightholders and then informs its members in order to arrange the blocking of infringing websites.</li> <li>- Internet service providers. Danish telecommunications companies which provide internet services. Their role is to implement the blocking on the websites that the court has ordered.</li> </ul>	<p><b>IPR Center</b></p> <ul style="list-style-type: none"> <li>- As a public authority, its main objective is to fight against the activities that constitute theft of intellectual property rights, on criminal grounds.</li> <li>- The IACC forwards information of the complaints they receive from the rightholders to the IPR Center</li> </ul>
		<p><b>Public authorities.</b> They neither took part in the drafting of the Austrian VCP, nor in its implementation.</p>	<p><b>Public authorities.</b> They neither took part in the drafting of the UK VCP, nor in its implementation.</p>	<p><b>Civil society.</b> They did not collaborate in the drafting of the Dutch VCP and they do not participate in it currently.</p>	<p><b>Danish Consumer Council.</b> Its main role is to protect consumer rights in the market. Regarding the Danish VCP, this body has participated in the developing of the SWC.</p>	<p><b>Civil society.</b> They did not collaborate in the drafting of the U.S. VCP and they do not participate in it currently.</p>
		<p><b>Civil society.</b> They did not collaborate in the drafting of the Austrian VCP and they do not participate in it currently.</p>	<p><b>Civil society.</b> They did not collaborate in the drafting of the UK VCP and they do not participate in it currently.</p>			







<div>       </div>						
Country	French VCP	Austrian VCP	UK VCP	Dutch VCP	Danish VCP	U.S. VCP
Scope of application	<b>Subjective scope</b> <ul style="list-style-type: none"> <li>- Rightholders</li> <li>- E-commerce platforms</li> </ul>	<b>Subjective scope.</b> Only associations can submit complaints to the Werberat against what they consider advertising environments breaching copyright.	<b>Subjective scope</b> <ul style="list-style-type: none"> <li>- Buyers of digital display advertising</li> <li>- Sellers of digital display advertising</li> <li>- Facilitators of digital display advertising. However, facilitators providing standalone advertising services are excluded from the scope of application of the UK VCP.</li> </ul>	<b>Subjective scope</b> <ul style="list-style-type: none"> <li>- Rightholders.</li> <li>- Intermediaries.</li> </ul>	<b>Subjective scope</b> <ul style="list-style-type: none"> <li>- Rightholders.</li> <li>- ISPs.</li> </ul>	<b>Subjective scope.</b> It is addressed to any rightholder or payment processor worldwide.
	<b>Territorial scope.</b> No territorial limitation is foreseen. It is addressed to any rightholder or e-commerce platform worldwide.	<b>Territorial scope</b> <ul style="list-style-type: none"> <li>- The advertiser has to be based in Austria</li> <li>- The conflicting advertising has to be directed to an Austrian audience</li> </ul>	<b>Territorial scope</b> <ul style="list-style-type: none"> <li>- -Businesses with a UK presence, targeting UK audiences or users.</li> </ul>	<b>Territorial scope</b> <ul style="list-style-type: none"> <li>- The Intermediary has to provide the telecommunication services on the internet in the Netherlands.</li> </ul>	<b>Territorial scope</b> <ul style="list-style-type: none"> <li>- Limited to Denmark and the Danish internet service providers.</li> <li>- The court resolution must come from a Danish Court.</li> </ul>	<b>The territorial scope</b> in which the U.S. VCP is applied is not limited.
		<b>Material scope.</b> Complaints concerning the following categories of advertising are out of the scope of the Austrian VCP: <ul style="list-style-type: none"> <li>- Party political and election advertising.</li> <li>- Publications promoting the arts and culture alone.</li> <li>- Advertising of and for non-profit organisations</li> </ul>	<b>Material scope.</b> Misplacement of any kind of advertising.	<ul style="list-style-type: none"> <li>- The allegedly unlawful content has to be in conflict with the laws of the Netherlands and is publicly available on the internet.</li> </ul>		

Country	 French VCP	 Austrian VCP	 UK VCP	 Dutch VCP	 Danish VCP	 U.S. VCP
Duties and procedures	<b>Preventive measures addressed to e-commerce platforms before offers are submitted by sellers</b> <ul style="list-style-type: none"> <li>- Exchange of information with rightholders</li> <li>- Provision of information to sellers of products most subject to counterfeiting</li> </ul>	<b>Submission of complaints to the Werberat by associations.</b> Associations are the ones that put forth whether in their opinion an advertising environment infringes copyright.	<b>The six principles envisaged by the UK VCP are the following:</b> <ul style="list-style-type: none"> <li>- Formalisation by buyers and sellers of their trading activities</li> <li>- Indication by buyers and sellers of where advertising should or should not appear and the mechanisms to be used to minimise misplacement</li> <li>- Confirmation by sellers of the measures they apply for minimising advertising misplacement</li> <li>- Explanation by sellers of their specific provisions in order to minimise advertising misplacement</li> <li>- Consequences of advertising misplacement</li> <li>- Independent verification</li> </ul>	First of all, the Dutch VCP does not provide a complete notice-and-take-down procedure, but allows the intermediaries to either subscribe to the Dutch VCP or to draft their own notice-and-take-down-code of conduct observing the guidelines proposed by the Dutch VCP in order to elaborate its individual code of conduct. <ul style="list-style-type: none"> <li>- It starts with the detection of allegedly infringing content on the internet by any individual or organisation and the desire of these individuals or organisations to notify it to an intermediary. The form of notifying it is through a report. In this sense, there are two different kind of reports:</li> </ul>	<b>Presenting the claim.</b> It starts with the initiative of a rightholder or the RettighedsAlliancen, who present a claim before a Danish court alleging there is a website infringing their intellectual property rights.	<b>Submission of the complaints to the IACC by the rightholders.</b> The connection between rightholders and payment processors is made through a master portal of the IACC, the Umbrella Portal. This Portal is the platform through which the rightholders are able to submit complaints. Once the rightholder has collected all the necessary information in order to submit a complaint to the Umbrella Portal, they will need to fill in a standardised notification form.
		<b>Preliminary examination of the complaint by the Werberat's Office.</b> The Werberat's Office examines whether complaints fall within the scope of the Austrian VCP.			Once the claim has been filed, RettighedsAlliancen will inform Teleindustrien about it.  When the process starts, the court evaluates the allegedly <b>infringement</b> and informs the people responsible for the conflictive website about the court process and invites them to be part of it.	

Country	French VCP	Austrian VCP	UK VCP	Dutch VCP	Danish VCP	U.S. VCP
Duties and procedures	<p><b>Proactive measures addressed to e-commerce platforms after offers are submitted by sellers</b></p> <ul style="list-style-type: none"> <li>- Identification of regular sellers</li> <li>- Use of automatic tools to detect offers and sellers</li> <li>- Notification mechanisms to be made available to rightholders and consumers</li> <li>- Temporary conditions for bids of products most subject to counterfeiting</li> <li>- Requests for documentation proving the authenticity of the products</li> <li>- Specific measures for products located outside the EEA and sellers based outside the EEA</li> </ul>	<p><b>Request to issue an opinion from the Werberat to advertisers.</b> When the Office considers a complaint justified (in German 'begründet'), it issues a request to the advertiser asking for its opinion on the complaint within three working days. In cases where the advertiser agrees to discontinue the campaign, the Office closes the file. In practice, so far all advertisers contacted by the Office have removed their conflicting advertising.</p>	<p><b>Definition of likely infringing websites:</b> Signatories use the Infringing Website List of PIPCU (Unit within the City of London Police) for these purposes. Although the Infringing Website List and the UK VCP are two different initiatives, they run in parallel. It is an online register of websites under investigation for intellectual property rights infringements accessible by the advertising industry voluntarily so as to cease placing advertising on it.</p>	<p><b>Report from a Public Prosecutor.</b> These reports are directly sent to the corresponding internet service providers. There is no need for a further analysis and intermediaries, since the evaluation has already been done by an authorised body, and they must proceed to take down the relevant content. This is because, generally when a Public Prosecutor files a report, this concerns, inter alia, other sorts of unauthorised content such as terrorism or child pornography. These reports have imperative character and therefore intermediaries have to deal with them immediately.</p>	<p><b>Court Resolution.</b> When the court resolves in favour of the rightholder, the RettighedsAlliancen or the rightholder itself, must inform Teleindustrien about the court decision. It is mainly important to bear in mind that a previous court order is required in order to implement the blocking.</p>	<p>Once the standardised complaint form is completed and the corresponding documentation submitted to the Umbrella Portal, the IACC must review each complaint for sufficiency and compliance.</p>
		<p><b>Notification by the Office to the owner of the advertising environment breaching copyright of any complaint raised against them.</b> In practice, it is difficult to comply with this duty either because the owners of the environments are not based in Austria or because the environments do not provide sufficient contact details.</p>	<p><b>Compliance and enforcement</b></p> <ul style="list-style-type: none"> <li>- Entities willing to adhere to the UK VCP shall register as formal signatories of it.</li> <li>- An independent policy verification process is conducted by verification providers. The audit report issued is sent to JICWEBS for review. If the report is approved by JICWEBS, signatories will be awarded a seal of compliance and a certificate of compliance.</li> </ul>		<p><b>Teleindustrien</b>, for its part will inform via e-mail all its members about the court decision so they can implement the blocking within a maximum of seven days from the notification.</p> <p>Once the website is blocked, a communication of the SWC will be displayed on the blocked websites redirecting consumers to legal alternatives.</p> <p>The final decision of the court can be appealed to the Supreme Court.</p>	<p>After the IACC reviews the content of the complaint, an attempt to make an online purchase using a valid, yet set-to-decline, credit card will be conducted ('Trace message') and the IACC will access the transaction records of each card in order to gather the information from each transaction which typically includes the Merchant's name, ID number and country.</p> <p>Afterwards, the IACC will contact the IPR Center who will place a hold on the complaint if they consider that the U.S. VCP procedure can interfere with an on-going investigation or may have criminal implications.</p>

Country	French VCP	Austrian VCP	UK VCP	Dutch VCP	Danish VCP	U.S. VCP
Duties and procedures	<p><b>Sanctions applicable by e-commerce platforms to sellers of counterfeit goods.</b></p> <ul style="list-style-type: none"> <li>- Take down of the offer</li> <li>- Prevent its re-publication</li> <li>- Temporarily suspend all accounts identified as belonging to the same seller</li> <li>- Close all accounts and prevent re-registration for a certain period</li> <li>- Ask for justification of the authenticity of the products</li> <li>- Provide documentation evidencing the authorisation to sell the product from the relevant rightholder.</li> </ul>	<p><b>Forward of the complaint to the Small Senate.</b> In cases where the advertisers consider the complaint unfounded and they do not discontinue the advertising campaign or they do not issue a response to the Office's request, the Office forwards the complaint to the Small Senate. The Small Senate may issue a cessation request to the advertisers. No complaints have reached the Small Senate so far.</p> <p><b>Appeal by the advertiser or the owner of the advertising environment breaching copyright before the Ethics Senate if they do not agree with the Small Senate's cessation request.</b> No complaints have reached the Small Senate so far.</p>	<p><b>Timing</b></p> <ul style="list-style-type: none"> <li>- The term for signatories to obtain the first seal is fixed at six months from their adherence to the UK VCP. Subsequent seals have to be issued before the expiration of the current seal</li> <li>- The verification submission form has to be submitted to JICWEBS at least two weeks before the end of the month in which the seal has to be issued</li> <li>- Verification work, has to be completed four months before the month in which the seal has to be issued.</li> </ul>	<p><b>Report from a notifier.</b> The Dutch VCP encourages the notifier to try to reach an agreement with the content provider before addressing the report to the intermediary. In these cases, the intermediary evaluates the report to conclude if the content alleged is unlawful or not. In this sense, there can be three different results:</p> <ul style="list-style-type: none"> <li>- There is no doubt about the unlawfulness of the content, so the intermediary will proceed to take it down;</li> <li>- The intermediary considers the content is legitimate. It will report the notifier with the reasoning of such determination.</li> <li>- The intermediary is unable to unequivocally determine whether the content is unlawful or not. In this situation, two circumstances can happen: <ul style="list-style-type: none"> <li>a. When the content provider is known. If there is no possibility of reaching an agreement, the notifier can also decide to make an official report to the police</li> <li>b. When the content provider is unknown. In practice, when it is not possible to identify the content provider, intermediary usually suggests that the notifier takes an action against the content provider before a court.</li> </ul> </li> </ul>	<p>After the launch of the Danish VCP, stakeholders became aware that after blocking certain websites, the illegal content of such websites will appear again on the internet under a different domain name. Due to this, the Danish VCP was amended in 2015 to allow ISPs to block also the new websites on the basis of the previous court ruling ordering the blocking of the original website. In these cases, the procedure is as follows:</p> <ul style="list-style-type: none"> <li>- The RettighedsAlliancen sends all the information of the new website to Teleindustrien so the latter can distribute it to its members for implementing the new blocking within two days</li> <li>- In this specific situation, the RettighedsAlliancen agrees to indemnify the internet service providers implementing the new blockings in the event they block a website with legal content</li> </ul> <p>This Danish VCP only applies to DNS blocking because for the internet service providers this is the easiest blocking to implement.</p>	<p>If the IPR Center places a hold on the complaint or decides to start its own investigation because there are criminal implications, the U.S. VCP procedure will end at this phase. If, on the contrary, the IPR Center does not place a hold on the complaint, it will be automatically accessible to the payment processors through the Umbrella Portal.</p> <p><b>Once certain payment processors receive the complaint through the Umbrella Portal, they will check whether there is a real payment account on this website or not.</b></p> <p>If there is a real and active payment account, the payment processors will analyse the information uploaded by the rightholders in the Umbrella Portal as their decision will rely on this information.</p> <p>Once the payment processors investigations are completed, each payment processor will notify its decision and the corresponding remedies applied to the Umbrella Portal so that it is accessible to rightholders.</p>



     						
Country	French VCP	Austrian VCP	UK VCP	Dutch VCP	Danish VCP	U.S. VCP
Monitoring enforcement	<p>There are no consequences for not complying with the duties set forth in the French VCP.</p> <p>Adherence to the French VCP is voluntary. It leaves signatories free to implement the corresponding measures for voluntary cooperation, but does not prevent them from implementing different or additional procedures.</p>	<p>Compliance is voluntary and up to advertisers.</p> <p>The Werberat's requests to remove advertising are not legally binding and advertisers may freely decide whether or not to remove their advertising from advertising environments breaching copyright. The Werberat does not have the power to prohibit the operation of advertising environments breaching copyright or to assess with any kind of legal effect whether an advertising environment infringes intellectual property right.</p>	<p>The UK VCP is a voluntary system of self-regulation to which signatories may freely adhere. Being a private arrangement, the UK VCP leaves its signatories free to implement the corresponding measures for voluntary cooperation in order to fight against advertising misplacement.</p>	<p>The Dutch VCP is voluntary and not mandatory. Therefore there are no penalties or sanctions imposed by the Dutch VCP for the non-observance of its provisions.</p> <p>According to some intermediaries interviewed, some hosting providers have been banned from their associations for not complying with the Dutch VCP.</p> <p>In addition to this, if an intermediary refuses to comply with a court order addressed to them, will have to face legal consequences in accordance with Dutch law.</p>	<p>The Danish VCP is voluntary and not mandatory. No penalty is applied. However, if the ISP does not comply with the court order, ISP would be disobeying a court order and Danish law would impose a sanction on it.</p> <p>According to the stakeholders interviewed, there is no IT signatory who has decided not to apply it voluntarily.</p>	<p>There are no consequences or sanctions imposed by the U.S. VCP on the participants for not using the Umbrella Portal or not submitting complaints to it.</p> <p>U.S. VCP is a private practice between its participants and adherence to it is voluntary.</p>
Technologies	<p>E-commerce platforms use the following technological tools in relation to the French VCP:</p> <ul style="list-style-type: none"> <li>- Specific software to detect online offers of counterfeit products and sellers likely to sell counterfeit goods. Inter alia, such software analyses key words in the offers published on e-commerce platforms' websites</li> <li>- Electronic notification procedures addressed to rightholders and to consumers</li> </ul>	<p>Associations have to file their complaints through the online complaint form available on the website of the Werberat.</p>	<p>Signatories have to select from one of the following means of detecting advertising misplacement:</p> <ul style="list-style-type: none"> <li>- Content verification tools. Technological instruments to assess a website's content resolving if it is appropriate or not for an advertiser</li> <li>- Appropriate / inappropriate schedules. In practice, these schedules are supported by technology developed either by the signatories or third party service providers</li> <li>- Submission by signatories of their verification forms to JICWEBS is performed online</li> </ul>	<p>The parties use e-mails for communicating and exchanging information.</p> <p>All the technology used in the Dutch VCP already existed before the implementation of the Dutch VCP.</p>	<p>The parties use e-mails for communicating and exchanging information.</p> <p>The compliance of the Danish VCP does not imply the development of any technologies.</p>	<p>Reporting the sale of counterfeit goods or pirated content is made through the Umbrella Portal. Such reporting is performed by the rightholders through the online complaint form available on the website of the RogueBlock.</p> <p>As stated by certain stakeholders interviewed, rightholders shall implement sufficient measures and tools that allow them to identify the selling of counterfeit products.</p>
Costs	<p>Signatories do not have to pay any member fee in relation to</p>	<p>Associations do not have to pay any administration fees to the</p>	<p>Due to the subscription to the UK VCP, signatories have to</p>	<p>Each signatory of the Dutch VCP and each rightholder</p>	<p>Each party assumes its own costs.</p>	<p>Initially, rightholders participating in the U.S. VCP</p>



Country	French VCP	Austrian VCP	UK VCP	Dutch VCP	Danish VCP	U.S. VCP
	<p>the French VCP.</p> <p>The main cost that may arise for rightholders and e-commerce platforms originate from the need to hire at least an estimated in-house correspondent responsible for dealing with the matters related to the French VCP.</p>	<p>Werberat in relation to the Austrian VCP.</p> <p>Monitoring activities may involve certain costs for them, but they are rather linked to their day-to-day activities.</p>	<p>pay an annual fee amounting to £943 which covers, inter alia, JICWEBS' supervisory role and its support in relation to the UK VCP.</p> <p>The verification process is subject to fees, which vary depending on the verification provider chosen. For example, ABC's fees start at £2,839.</p> <p>There can be additional costs for the signatories as a consequence of complying with the UK VCP (e.g., acquisition of a content verification tool).</p>	<p>assume their own costs.</p>		<p>had to pay an IACC member fee.</p> <p>The IACC supports relevant costs in relation to the Trace Messages they carry out.</p> <p>The main cost that may arise for rightholders and e-commerce platforms originate from the need to hire internal or external staff who will be responsible for dealing with the merchant's accounts investigations.</p>
Education	<p>Signatories are generally not undertaking educational activities.</p> <p>Currently, the INPI does not have a website outlining the background and purposes of the French VCP.</p>	<p>The Werberat organised two events to present the Austrian VCP after its implementation.</p> <p>The Werberat publishes on its website news related to it as well as its decisions.</p> <p>Educational activities mainly focus on advertisers since associations participated in the creation of the Austrian VCP and are therefore aware of it.</p>	<p>JICWEBS' website has a specific section dedicated to the UK VCP which contains detailed information and documentation. JICWEBS regularly publishes press releases on its website relating to the UK VCPs.</p> <p>IAB UK is very active in promoting the UK VCP through their website, press releases and organising different events highlighting the problem of advertising misplacement.</p> <p>Rightholders support the raising of awareness by giving talks about the issues and the VCP at industry events.</p>	<p>There have been no educational activities directed towards consumers.</p> <p>Intermediaries through their associations have provided their members information to facilitate the implementation of the Dutch VCP.</p>	<p>The most important project regarding education is the Share With Care campaign. As with the creation of the Danish VCP; this campaign was also created on the basis of the initiatives included in the 'Copyright Package' where one of the aims was related to a 'mutual information effort between telecom industry, copyright industry and the Danish Ministry of Culture'.</p> <p>Since its launch in 2013, the SWC has been focused on (i) promoting the use of legal content on the internet, such as films, music, books, etc. (ii) studying the needs of the consumers of online content and providing them legal alternatives and (iii) establishing behavioural design mechanisms to face distributing illegal content on</p>	<p>A consumer education campaign to increase awareness of the risks associated with shopping on counterfeit websites was carried out by the IACC after the U.S. VCP was launched.</p> <p>The IACC also organises educational activities for general consumers and users and events for stakeholders of the industry such as the so-called 'Spring Conference' or 'Fall Conference'.</p>

Country	French VCP	Austrian VCP	UK VCP	Dutch VCP	Danish VCP	U.S. VCP
					<p>the internet.</p> <p>For this purpose, the SWC has developed certain actions such as camps, web nudge campaign, polls and reports, going-home meetings, high presence on Facebook, Twitter or Instagram, presentations for interested parties, etc.</p>	
Effectiveness	<p>An assessment on the application of the French VCP was performed by the INPI 18 months after the signature of the French VCP in December 2009. It reports that signatories believed that the objectives of the French VCP had been broadly achieved.</p> <p>The two platforms that signed the French VCP in December 2009 found that during the testing period the selling of counterfeit goods through their websites had decreased.</p> <p>The following figures are provided in the assessment by the mentioned platforms, evidencing the improved detection of counterfeit goods before a sale takes place:</p> <ul style="list-style-type: none"> <li>- Priceminister. Decline in the number of accounts suspended due to counterfeit sales: 2,600 in 2009 and 1,500 in 2010</li> <li>- 2xmoinscher. Decrease of the number of counterfeit items returned by buyers: 166 in 2009 and 101 in 2010</li> </ul>	<p>Between December 2013 and February 2014, prior to the implementation of the Austrian VCP, the Werberat conducted an information campaign addressed to 60 advertisers that were placing advertising in advertising environments breaching copyright. All of these advertisers removed the mentioned advertising.</p> <p>After the implementation of the Austrian VCP, all advertisers contacted removed their advertising upon the request of the Werberat.</p> <p>The Werberat has informed that at the time this study is being drafted, the following number of complaints filed by associations are related to advertising environments breaching copyright:</p> <ul style="list-style-type: none"> <li>- 2014: nine</li> <li>- 2015: one</li> </ul>	<p>JICWEBS released a 'Progress Report' on 12 February 2015 concerning the effectiveness of the UK VCP. Accordingly:</p> <ul style="list-style-type: none"> <li>- 28 advertising businesses have been awarded seals by JICWEBS confirming they meet standards at reducing the risk of online advertising being served next to inappropriate or illegal content. A further 12 are progressing towards this accreditation</li> <li>- At the end of 2014, two thirds (2/3) of the display advertising market was signatory of the UK VCP</li> <li>- By the end of 2015 it was expected to grow to 90 %</li> </ul> <p>A new 'Progress Report' will be released in 2016.</p>	<p>Leaseweb launched a 'Law Enforcement Transparency Report' with the aim of analysing the valid law enforcement requests.</p> <p>BREIN through its 2010 yearbook stated that more than 600 illegal sites were shut down. In the 2015 yearbook it is pointed out that 362 websites were taken down, and that over the 80 % of those take downs were carried out by hosting providers.</p> <p>Intermediaries are working on future actions and tools that could help increase the effectiveness of the VCP, for example a type of help desk formed by experts for evaluating the reports and a complaint centre to address all the reports.</p>	<p>Since the implementation of the Danish VCP in September 2014, and pursuant to the information found in Teleindustrien's web site, 76 websites have been blocked by a court ruling. 'The Guide Book of Digital User Behaviour' from SWC contains data which shows a decrease has been also observed in copyright infringement, but it is difficult to distinguish which concrete actions are responsible for this drop as there has also been a proliferation of copyright legal services such as Spotify for music.</p>	<p>Pursuant to the information provided on the IACC website, since the implementation of the U.S. VCP in 2012 the program has terminated over 5,000 individual counterfeiters' merchant accounts, which has impacted on over 200,000 rogue websites.</p>

### 4.3. Horizontal comparison

Self-regulation can be found in many areas and is subject to a permanent and constant process of optimisation and improvement. The table included in Section 3.2 of this chapter ('Comparative table') compares the six VCPs selected as examples of the self-regulated protection of intellectual property rights in France, Austria, the UK, the Netherlands, Denmark and the U.S.

This short abstract summarises the results obtained from the in-depth examination of the six VCPs selected and, in the end, gives a short conclusion on the operation and organisation of self-regulation through VCPs as an indication based on the six reports.

#### 4.3.1. Similarities between the VCPs examined

The VCPs examined share certain commonalities. They are all carried out on a voluntary basis and participation is not mandatory. Therefore, they do not impose compulsory sanctions for not complying with the duties and procedures envisaged by them.

Most of them entail duties to some of their stakeholders to establish preventive or proactive measures in order to prohibit or detect infringements of intellectual property rights.

Almost none of the VCPs (except for the UK and the U.S. VCPs) involve any costs or fees to stakeholders, though indirect costs may arise in some VCPs in relation to enforcement.

In all VCPs, complaints procedures would usually be dealt with as a form of cooperation between rightholders and either website operators (such as in France, Denmark and the U.S.), rightholders and advertising businesses (Austria and the UK) or vis-à-vis internet services providers (the Netherlands).

Stakeholders will normally have to cover their own expenses.

#### 4.3.2. Differences between the VCPs examined

The following sets out the main differences between the respective VCPs by way of a brief horizontal assessment. Major differences have been found with regard to the scope of application, specifically in relation to the entities involved in enforcement and the material and geographical remit of each VCP, the participants and stakeholders involved, the intellectual property rights concerned, the overall remit as regards the definition of what constitutes infringement, the respective obligations and procedures and the technologies employed.

##### 4.3.2.1. *Origin of the VCP*

Although all of the VCPs were established rather recently, they were initiated by different stakeholder groups, sometimes following the direct or indirect involvement of public authorities such as in France and Denmark, sometimes created by an industry without any involvement of public bodies such as the UK and Austrian VCPs. In addition, the remit of the VCPs differs in terms of their origin and attachment to pre-existing or, as the case may be, new types of collaboration. For example, in France the introduction of the VCP was new and based upon creating a new entity, the French Charter for the Fight against the Sale of Counterfeit Goods on the internet between Intellectual Property Rightholders and E-Commerce Platforms whereas other VCPs were attached to pre-existing self-regulatory schemes, such as the Code of Ethics of the Austrian Werberat. The individual purposes upon which the VCPs have been initially based therefore diverge between VCPs and lead, consequentially, to further differences as regards important aspects such as the scope and remit of each. Generally, such purposes can lie in more direct schemes for tackling counterfeits (i.e., France), or may be anchored in advertising standards (i.e., UK, Austria).

#### *4.3.2.2. IP Rights covered by the VCP*

The intellectual property rights covered in each VCP may and do differ. For example, the French VCP only extends to trade mark and design rights in relation to sales of physical articles and the Austrian VCP is concerned exclusively with copyright; while the rest of VCPs, from the UK, the U.S., The Netherlands and Denmark protect copyright and related rights, trade marks and design rights.

#### *4.3.2.3. Stakeholders involved in the VCP*

In all VCPs, rightholders or relevant associations and industry bodies representing rightholders are involved. Intermediaries are prominently included in France (based upon agreements with e-commerce platforms), the Netherlands (any company providing access to the internet) and Denmark (Teleindustrien or any company providing access to the internet), but are not part of the VCP in Austria, UK (advertising industry) or the U.S. (payment processors).

#### *4.3.2.4. Territorial scope of the VCP*

As regards the scope of geographical application, most VCPs require a connection to the country in which the VCP is based. Some define this in a more detailed manner than others. For example, the Austrian VCP requires both that an advertiser must be based domestically, and that the advertisement is targeted at domestic consumers. A similar provision exists in the UK. In the Netherlands, the territorial application of the VCP is based upon the intermediary who must provide services in that jurisdiction. For the Danish VCP, the service provider must be seated in Denmark and the DNS blocking order has to come from a Danish court. There are no express territorial limits in France and the U.S.

#### *4.3.2.5. Procedures of the VCP*

Individual complaints are generally possible for rightholders, but are limited to rightholders' associations in Austria.

In general, in almost all the selected VCPs the process is initiated at the request of rightholders or their representative bodies and associations. The decision to pursue an alleged infringement is then, ultimately, made by different participants, depending on the VCP examined. The assertion whether, at that stage (i.e., before a possible later litigation), an intellectual property right covered by the individual VCP has been infringed is, therefore, principally in the hands of rightholders. However, there are fundamental differences as regards the overall procedures to be followed. It is only in Denmark where the procedure is inherently attached to a form of judicial control, since here the procedure is instigated following a court order with a leave to appeal option. In the Netherlands (involvement of public prosecution) and the U.S. (the IPR Centre as a public authority deciding whether to follow its own investigation for criminal implications) state authorities are involved, though here the procedure is not initially linked to judicial proceedings – otherwise, the decision to pursue enforcement is left to private entities (such as in France) where the result would be the taking down of the offer, or – as in the UK or Austria – a procedure is foreseen that would result usually in requests to remove advertising from infringing websites without a (legal) obligation to actually do so.

As the VCPs examined included various types of cooperation, there are fundamental differences as regards the outcome of each procedure – these range from blocking orders (Denmark), notice and take down procedures (France and the Netherlands) to requests directed at advertisers / sellers of advertising.

There exist disparities as regards the steps that may be taken, and the addressee of decisions made by individual VCPs. For example, in the Danish VCP, the existing court order is sent to intermediaries who will have 7 days to block the respective website (and any subsequent website with the same content). The approach in the Netherlands is similar, in that ultimately illegal content is removed by the internet service provider. In France, the addressee of complaints is usually an e-commerce platform, rather than an intermediary.

#### *4.3.2.6. Role of technologies*

The level of technology used varies very much. While certain examined VCPs only foresee the use of e-mail technologies and online complaint forms (see Austria, the Netherlands, Denmark or the US), a few systems seem

to be based on rather specific technologies including software to detect online offers of counterfeit products (see France). However, it proved to be impossible to obtain more detailed information on these technologies. In particular, it remained unclear how the detection of offers for counterfeit products is technically achieved (such a system would require a highly intelligent key word mechanism).

#### **4.3.2.7. Effectiveness**

The effectiveness of the VCPs examined could not be measured conclusively. Many parties interviewed in the course of the study transmitted their impression that the respective systems work. But from a scientific perspective, the success of the different national approaches could only be measured with clear indicators including, for example, the numbers of successful complaints, the economic importance of the parties involved or an empirically measurable deterring effect of these systems to potential infringers. Such data was, however, not available. Figures spanning several years were, in any case, only available for the French VCP (number of accounts suspended for the sale of counterfeit products) and the Danish VCP (number of website blockings). In this context it has to be borne in mind that some of the VCPs examined are comparatively new initiatives.

## 5. Legal issues

The analysis of the legal frameworks and related case law that may have an impact on the practical application of the selected VCPs covers a significant part of this study.

The individual VCP reports in the subsequent chapters of this study contain detailed information on specific legal implications in the jurisdictions analysed. This section will therefore provide only a brief summary of the aspects of the legal regimes that have been analysed. It should be noted that no in-depth study of all potential legal implications that might arise with respect to each VCP can be achieved. Nevertheless, specific aspects of particular relevance have been analysed.

It was evaluated, *inter alia*, what potential impact fundamental rights (e.g., freedom of expression, freedom to conduct a business, privacy, right to an effective remedy and to a fair trial) may have *vis à vis* the selected VCPs as well as how the latter may interact with data protection and e-commerce rules.

As a result of the foregoing, each of the subsequent chapters of this study contains an analysis about the coexistence of the VCP measures with the applicable local legal frameworks and related case law. In the case of the five selected VCPs from Member States of the European Union, the analysis is also performed with respect to the Charter of Fundamental Rights, European Union directives and European Union case law.

The purpose of this section is to summarise the key elements of the legal analysis performed concerning the selected VCPs.

### 5.1. VCPs of Member States of the European Union

#### French VCP

From a European Union perspective, the measures envisaged by the French VCP have been analysed from the following standpoints:

- Charter of Fundamental Rights:
  - Article 8 ('Protection of personal data').
  - Article 16 ('Freedom to conduct a business').
  - Article 17 ('Right to property').
  - Article 47 ('Right to an effective remedy and to a fair trial').
- European Union Directives:
  - Articles 14 and 15.1 of the E-Commerce Directive.
  - Article 3 of the Enforcement Directive.
  - Articles 6.1(e) and 7 of the Data Protection Directive.
  - Article 7 of the Data Protection Directive.

From a local French perspective, the measures envisaged by the French VCP have been reviewed according to the following:

- Fundamental rights set forth by the French Declaration of the Rights of Man and of the Citizen of 1789 ('Déclaration des droits de l'homme et du citoyen'), referenced in the French Constitution of 4 October 1958 ('Constitution de la République française'):
  - Article 4: 'Freedom to conduct a business'.
  - Articles 2 and 17: 'Right to property'.

- The right to an effective remedy and to a fair trial set forth under Article 6 of the European Convention on Human Rights of 4 November 1950, which is also applicable in France since the mentioned Convention provides for generally accepted principles before French Courts and might also have an impact on the interpretation of the French VCP.
- French Regulations:
  - Articles 6, 7 and 25 of the French Data Protection Law, which implements the Data Protection Directive.
  - Articles 1, 6 I-2°, 6 I-7° and 6-I-8° of the French E-Commerce Law, which implements the E-Commerce Directive.
  - Article L. 716-6 and following of the French Enforcement Law, which implements the Enforcement Directive.

**RESULT:** Based on the analysis of the aforementioned European and French legal frameworks and after having applied it to the French VCP, it has been concluded that one aspect of the French VCP might raise issues with regard to the right to the protection of personal data of individuals selling goods on e-commerce platforms that have joined the French VCP.

The data processing activities implied from (i) the duty of e-commerce platforms to prevent re-registration of certain sellers for five years after the closure of their accounts and (ii) the duty of e-commerce platforms to store documents evidencing the identity of sellers likely to sell products most subject to counterfeiting for a period of five years after the closure of their accounts, might not be consistent with the general rule under Article 6 of the French Data Protection Law. This general rule envisages that data controllers may only retain personal data as long as it is necessary for the purposes for which the data was initially obtained (in this case, the management of sellers' activities as registered users). This retention period of five years could eventually be considered disproportionate taking into consideration the retention period of one year envisaged by other French regulations aiming to fight online infringements<sup>39</sup>.

#### 5.1.1 Austrian VCP

From a European Union perspective, the measures envisaged by the Austrian VCP have been analysed from the following standpoints:

- Charter of Fundamental Rights:
  - Article 11 ('Freedom of expression and information').
  - Article 16 ('Freedom to conduct a business').
  - Article 17 ('Right to property').
- European Union Directives:
  - Article 3 of the Infosoc Directive.
  - Article 8 of the Infosoc Directive.

From a local Austrian perspective, the measures envisaged by the Austrian VCP have been reviewed according to the following:

---

<sup>39</sup> Article R. 10-13 of the French Code for the Posts and Electronic Communications of 1952 ('Code des Postes et des Communications Électroniques') envisages the obligation for operators of electronic communications to retain personal data allowing the research, the assessment and the prosecution of a criminal infringement or a breach of Article L. 336.3 of the French Intellectual Property Code for a period of one year as from its collection. Also, Decree No 2011-219 of 25 February 2011 relating to the Retention and the Communication of Data Enabling the Identification of Persons that have Contributed to the Creation of Online Contents ('Décret No 2011-219 du 25 février 2011 relatif à la Conservation et à la Communication des Données permettant d'Identifier toute Personne ayant Contribué à la Création d'un Contenu Mis en Ligne') envisages the same data retention obligation as Article R. 10-13 of the French Code for the Posts and Electronic Communications.



- Fundamental rights set forth by the Austrian State Basic Act of 1867 ('Staatsgrundgesetz') which enjoys constitutional status in Austria:
  - Article 5 of the Austrian State Basic Act of 1867: 'Right to property'.
  - Article 6 of the Austrian State Basic Act of 1867: 'Freedom to conduct a business'.
  - Article 13 of the Austrian State Basic Act of 1867: 'Freedom of expression'.
- Austrian Regulations:
  - Article 18.a.1 of the Austrian Copyright Law.
  - Article 81.1 and Article 81.1.a of the Austrian Copyright Law.
  - Article 82 of the Austrian Copyright Law.
  - Article 85 of the Austrian Copyright Law.
  - Article 86 of the Austrian Copyright Law.
  - Article 87 of the Austrian Copyright Law.
  - Article 87.a of the Austrian Copyright Law.
  - Article 87.b of the Austrian Copyright Law.
  - Article 87.c of the Austrian Copyright Law.
  - Article 1.330 of the Austrian Civil Code.

**RESULT:** Based on the analysis of the aforementioned European and Austrian legal frameworks and after having applied it to the Austrian VCP, it has been concluded that in practice such legal frameworks would not impact the duties and procedures envisaged by it.

### 5.1.2. UK VCP

From a European Union perspective, the measures envisaged by the UK VCP have been analysed from the following standpoints:

- Charter of Fundamental Rights:
  - Article 8 ('Protection of personal data').
  - Article 17 ('Right to property').
  - Article 47 ('Right to an effective remedy and to a fair trial').
- European Union Directives:
  - Article 3 of the Infosoc Directive.
  - Article 8 of the Infosoc Directive.
  - Article 3 of the Enforcement Directive.
  - Article 9.1 of the Enforcement Directive.
  - Article 15 of the Enforcement Directive.
  - Article 17.a of the Enforcement Directive.
  - Article 2.a of the Data Protection Directive.

From a local UK perspective, the measures envisaged by the UK VCP have been reviewed according to the following:

- Fundamental rights set forth by UK Human Rights Act:



- Right to the protection of property (Schedule 1, Part II, Article 1 ('Protection of property')).
- Right to an effective remedy and to a fair trial (Schedule 1, Part I, Article 6 ('Right to a fair trial')).
- Right to respect for private and family life (Schedule 1, Part I, Article 8 of the HRA ('Right to respect for private and family life')).
- Freedom to conduct a business, rooted in the UK as follows:
  - The right of property (Schedule 1, Part II, Article 1 of the HRA ('Protection of property')), which has already been mentioned above.
  - The freedom of contract, being the main sources of legal provisions that facilitate the formation and operation of companies and competition law in the UK the Companies Act of 2006, the Competition Act of 1998 and the Enterprise Act of 2002.
- UK Regulations:
  - Section 16 of the UK Copyright, Designs and Patents Act.
  - Section 20 of the UK Copyright, Designs and Patents Act.
  - Section 96 of the UK Copyright, Designs and Patents Act.
  - Section 97 of the UK Copyright, Designs and Patents Act.
  - Section 97.a of the UK Copyright, Designs and Patents Act.
  - Section 107 of the UK Copyright, Designs and Patents Act.
  - Section 226 of the UK Copyright, Designs and Patents Act.
  - Section 227 of the UK Copyright, Designs and Patents Act.
  - Section 229 of the UK Copyright, Designs and Patents Act.
  - Section 7 of the UK Registered Designs Act.
  - Section 7A of the UK Registered Designs Act.
  - Section 24A of the UK Registered Designs Act.
  - Section 9 of the UK Trade Marks Act.
  - Section 10 of the UK Trade Marks Act.
  - Section 14 of the UK Trade Marks Act.
  - Section 15 of the UK Trade Marks Act.
  - Section 16 of the UK Trade Marks Act.

**RESULT:** Based on the analysis of the aforementioned European and UK legal frameworks and after having applied it to the UK VCP, it has been concluded that in practice such legal frameworks would not impact the duties and procedures envisaged by it.

#### 5.1.4. Dutch VCP

From a European Union perspective, the measures envisaged by the Dutch VCP have been analysed from the following standpoints:

- Charter of Fundamental Rights
  - Article 8 ('Protection of personal data').
  - Article 11 ('Freedom of expression and information').

- European Convention of Fundamental Rights:
  - Article 8 ('Right to respect for private and family life').
  - Article 10 ('Freedom of expression').
- European Union Directives:
  - Article 12, Article 13, Article 14 and Article 15 of the E-Commerce Directive.
  - Article 11 of the Enforcement Directive.
  - Article 2, Article 5.1(a) and Article 8(3) of the InfoSoc Directive.
  - Article 7 (f) of the Data Protection Directive.

From a local Dutch perspective, the measures envisaged by the Dutch VCP have been reviewed according to the following:

- Article 7 ('Freedom of expression') and Article 10 ('Privacy') of Dutch Constitution.
- Article 6:162c and Article 6:196c of the Dutch Civil Code.
- Article 54a of the Dutch Criminal Code.
- Article 8 of the PDPA, which implements the Data Protection Directive.

These Dutch Regulations have also been considered by a large number of Dutch Courts. Among others, we could highlight the Decision of the Dutch Supreme Court, 25 November 2005 - *Pessers v Lycos* which has provided the guidelines for the provision of information (name of contact information) by the intermediary.

**RESULT:** After the legal analysis of the Dutch VCP, it can be concluded that the determination by intermediaries of what is considered 'undesirable' and 'unequivocally unlawful' rather than such a determination being undertaken by a public authority or a court which offers solid guarantees, could be, in some circumstances, in conflict with the freedom of expression of the content provider. Notwithstanding this, in practice it is improbable that intermediaries remove content which is not clearly illegal according to their evaluation process. For such less clear cases, they would in practice recommend pursuing a judicial case in order to determine if the disputed content is illegal or not and to remove it.

With respect to the right to the protection of personal data related to the content provider, Article 8 of PDPA and Article 7(f) of the Data Protection Directive, will allow the intermediary to process personal data and provide it to the notifier, without the consent of the content provider, following the criteria of the Dutch Supreme Court and as the balance undertaken implies that the interest of the notifier should prevail.

#### 5.1.5. Danish VCP

From a European Union perspective, the measures envisaged by the Danish VCP have been analysed from the following standpoints:

- Charter of Fundamental Rights:
  - Article 8 ('Protection of personal data').
  - Article 11 ('Freedom of expression and information').
  - Article 16 ('Freedom to conduct a business').
  - Article 17 ('Right to property').
- European Convention of Fundamental Rights:
  - Article 8 ('Right to respect for private and family life').
  - Article 10 ('Freedom of expression').

- European Union Directives and Regulations:
  - Recital 59, Article 2, Article 5.1(a) and Article 8(3) of the InfoSoc Directive.
  - Recital 22, Article 2, Article 3 and Article 11 of the Enforcement Directive.
  - Article 15.1 of the E-Commerce Directive.
  - Article 7(f) of the Data Protection Directive.
  - Articles 3 and 4 of the Open Internet Access Regulation.

From a local Danish perspective, the measures envisaged by the Danish VCP have been reviewed according to the following:

- Section §77 of the Danish Constitution ('Freedom of expression of Danish citizens').
- Article 2(1) and (2), Article 11(a)1 of the Danish Copyright Law.
- Article 411 and Article 413 of the Danish Administration of Justice Law.
- Article 6(1) of Danish Data Protection Law.

These Danish Regulations have been considered by Danish Courts. The following judgments, among others, have been taken into account: Decision of the Copenhagen City Court 25 October 2006, No FI-15124/2006 – *IFPI Danmark v. Tele2 A/S*, the Decision of the Bailiff's Court of Frederiksberg 5 February 2008 - *IFPI Danmark v. DMT2 A/S* and the Decision of the Maritime and Commercial Court in Copenhagen 11 December 2014 - *Fritz Hansen A/S, Louis Poulsen Lighting A/S, Carl Hansen & Son Mobelfabrik A/S, Fredericia Furniture A/S, Erik Jorgensen Mobelfabrik A/S v. Telia Denmark* which determined that blocking should be carried out at DNS level and prevent intermediaries' customers from accessing a website with a UK domain name.

**RESULT:** No legal issues arise from the Danish VCP as its application does not collide with any fundamental rights. Also, it is not necessary to disclose any personal data of the website owner either in the context of applying for an injunction or in the implementation of it by internet services providers.

## 5.2. U.S. VCP

Intellectual property rightholders are afforded a variety of remedies under U.S. law when their intellectual property rights are infringed and perpetrators could be subject to both criminal and civil sanctions. In relation to a possible conflict between the U.S. VCP and U.S. statutes, the following aspects have been evaluated: common law actions such as breach of contract, tortious interference with business relationships, data protection laws and the safe harbours applicable to online service providers based on secondary liability.

As regards the compatibility of the U.S. VCP with U.S. federal law, the U.S. VCP does not collide with any of the fundamental rights envisaged by the U.S. Constitution and its Bill of Rights.

The legal analysis of this VCP has not identified any problems from a legal standpoint. Although in theory it could be possible for a merchant to bring a lawsuit against a payment processor alleging (i) breach of contract for wrongful suspension/termination, or (ii) merchant's damages or (iii) other business relationships based on common law actions. However, it is very unlikely that these actions would be successful as the conditions established for merchants require them to accept the strict terms set by the payment processor. To date, no such cases are known.

## 5.3. CJEU Case Law

CJEU case law has also been analysed in the study. The main rulings studied are the following:

- *eBay* CJEU Ruling

This Ruling establishes guidelines to be followed by online marketplaces such as eBay, when they intend to implement technical procedures to fight against intellectual property rights piracy.

- **Promusicae CJEU Ruling**

This Ruling establishes that the protection of intellectual property rights is not of a higher order than other fundamental rights meaning that the protection of intellectual property rights does not prevail over other rights such as the freedom to conduct a business.

- **Kino.to CJEU Ruling**

This Ruling establishes, inter alia, that where several fundamental rights protected by the European Union legal order are at issue, such legal order and the interpretation thereof shall ensure a fair balance between the various rights at stake and shall avoid conflicts with other general principles of EU law such as the principle of proportionality. Namely, in its Ruling the CJEU highlights the need to strike a balance between (1) copyrights and related rights, which are intellectual property and are therefore protected by Article 17.2 of the Charter of Fundamental Rights, (2) the freedom to conduct a business, which economic agents enjoy under Article 16 of the Charter of Fundamental Rights and (3) the freedom of information of internet users, whose protection is ensured by Article 11 of the Charter of Fundamental Rights.

- **Svensson CJEU Ruling**

This Ruling establishes that the provision of clickable links to protected works constitutes an act of communication to the public. To the extent the links are directed at a 'new public', namely, a public that was not taken into account by copyright holders at the time of the initial communication, the authorisation of copyright holders would be required. This would be the case, for example, in relation to a protected work no longer available to the public on the website on which it was initially communicated or where it is henceforth available on that website but only to a restricted public, while being accessible on another website through a clickable link. In light of the foregoing, it may be considered that intellectual property infringing websites make available protected works to a new public since they are addressed to a public which was not taken into account by the copyright holders, in which case the owners of websites would require copyright holders' consent to perform such a communication legally.

- **Bonnier CJEU Ruling**

This Ruling establishes that an intermediary has to consider the content providers' privacy rights and not only the notifier's intellectual property rights when disclosing personal information from the content provider to the notifier. This may impact on the Dutch VCP since the code foresees the disclosure of the personal data of the content provider<sup>40</sup>.

## 5.4. The legal framework: fundamental aspects for VCPs

### 5.4.1. Legal aspects in the context of the study

VCPs must adhere to relevant legal requirements that are codified at both the national and European level. The breadth of divergent practices addressed in this study means that a detailed comparison of individual legal aspects is difficult since these much depend upon domestic laws and the precise type of procedures and practices established. The more detailed findings are outlined in the individual country reports. Nevertheless, certain more fundamental legal issues affecting VCPs are briefly discussed herein in order to provide a general framework.

This study contains analyses of different VCPs as regards potential collisions of such practices with legal norms and principles including fundamental freedoms, privacy, and data protection laws. This is a complex matter that concerns a number of different legal norms and instruments. While it can never be excluded that there might exist additional norms that were not examined, care has been taken to make certain that the analyses are as detailed as possible. Local law firms in the relevant jurisdictions have supported the analysis of the impact of applicable law on the VCPs in their respective country. The general framework of applicable rules and principles is set out and it is highlighted in which cases a collision of interests will be more likely. The issue of a more complex legal analysis

---

<sup>40</sup><http://curia.europa.eu/juris/document/document.jsf?text=&docid=121743&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=196710>.

depends on the notion and breadth of what is understood, in the highly different contexts of the VCPs examined, as instances where rights shall be enforced.

It should also be noted that this study has generally not found, based upon an analysis of applicable laws, decisions and also the feedback received from interviews, any instance where a clear breach of legal rules could be identified.

As will be examined in the following paragraph, collisions between legally protected interests are more likely the wider the remit of enforcement is defined.

In general, legal and contractual obligations under such regimes arise both with respect to stakeholders who may participate in a VCP as well as, and more importantly, vis-à-vis alleged infringers. The decision whether to take action is made usually by rightholders as those who instigate the procedures. In all VCPs bodies exist that are typically charged with evaluating the issue of infringement. In all cases, it should also be borne in mind that – where there are disputes over whether an infringement is present, the route to litigation remains open to third parties subject to enforcing actions by VCPs. According to the feedback received, in some cases it was reported that VCP bodies are cautious where the legal situation is unclear and would ask participants to revert to judicial actions.

As regards participants to VCPs, no particular problems have been identified given that all VCPs are voluntary. The major issue may arise as regards the relationship between VCPs (including, in particular, intermediaries) and third parties allegedly infringing rights or acting contrary to other principles such as unfair or misleading advertising. As a general rule, all VCPs must ensure that the enforcement of rights does not conflict with third party rights. Often, this will require an assessment based on balancing interests; the participants of the respective VCP initially conduct that exercise.

In very broad terms, the underlying principles are proportionality and fairness, which must be weighed against the right to have intellectual property rights protected.

#### 5.4.2. General legal considerations

The following briefly describes the generally applicable legal framework without regard to any specific VCP examined. The most important issues arise first with respect to data protection and privacy laws, which are generally codified at national level following the implementation of secondary European law. Secondly, concerns may follow from fundamental rights guarantees, here in particular rights under European convention law and domestic constitutional law. These guarantees include, as far as is relevant here, rights to freedom of expression including the right to commercial communication, the right to freely conduct a business and the right to an effective remedy and a fair trial. It should be noted that in general these fundamental rights are addressed to the state but that they may have horizontal effect and can therefore be applicable to private disputes.

From the outset, this means that whilst a notional collision between the interests concerned may be established, the legal assessment of how that conflict must be resolved depends, generally, on conducting a balancing exercise. As mentioned, there is no directly applicable legal authority on how, for the specific case of VCPs, such a balancing exercise should be conducted. The VCPs examined, in addition, are highly heterogeneous in their scope, and this study therefore examines rather divergent practices with, respectively, different scopes as regards the individual understanding of which types of alleged infringements, or other undesirable practices, are covered.

However, in order to explain the general legal framework, some general remarks concerning the relationship between an individual description of practices in VCPs and broader legal issues should be made irrespective of the examination of individual VCPs as can be found in the country reports.

VCPs have to balance between the interests of stakeholders, intermediaries and alleged infringers. In some cases, this is easier than in others. The balance is certainly respected for intermediaries who voluntarily participate, and it is also respected as regards the legal position of those who have clearly violated intellectual property rights that are safeguarded as property under the Charter of Fundamental Rights, for example in cases where identical signs are being used for identical goods or where works, designs and other protected subject matter have been copied as a whole. In such cases, evidently not much of a balancing exercise and legal analysis is required.

However, in cases where a more thorough and detailed legal assessment is required – for example, where issues as regards causing confusion over the use of a protected sign or an imitation (rather than full-scale copying) of a copyright protected work or a design are at stake – legal expertise is essential both as regards the relevant interpretation of statutory IP law but also in relation to assessing potential conflicts with higher ranking principles.

As regards the relationship between stakeholders (as represented in the individual VCPs), it can safely be assumed that overall, data protection issues do not arise under domestic data protection laws. The issue arises only where intermediaries oblige themselves to disclose personal data of alleged infringers. Although it can certainly be suggested that such disclosure constitutes an act of data processing subject to relevant domestic data protection laws and to fundamental rights, it may be justified under the requirement of fairness. The general necessity of a balancing exercise that is to be conducted where the fundamental right to property, which includes intellectual property rights, and rights to privacy and data protection collide has been established by the CJEU in the *Promusicae* decision. Similarly, as regards concerns over freedom to conduct a business or freedom of expression, no truly critical problems arise with regard to intermediaries. In all the VCPs analysed, it is apparent that their voluntary nature and absence of a system of sanctions must exclude such concerns.

Evidently, and as an observation not directly linked to any VCP analysed, the danger of a collision between intellectual property protection and conflicting rules and principles is mitigated to a higher degree where the notion of what constitutes an infringement of rights is defined precisely. In this regard, there are significant differences in scope between the VCPs as regards how blocking actions are pursued that may impact on the legal assessment. For example, the French VCP is limited to counterfeiting only. Other VCPs, however, refer to more general remits, such as ‘unlawful or undesirable content’ in the Netherlands or to ‘unlawful advertising environments’ in Austria.

Whilst – as regards intellectual property rights – it seems certain that such broader formulations will cover counterfeiting and piracy, the term ‘unlawfulness’ and similarly broad descriptions may also extend to rather different situations, such as selling goods outside of a selective distribution system via online platforms or selling goods which may be considered an imitation rather than a copy. In such cases, it may be generally burdensome to conduct a full legal assessment, and hence a certain danger exists that decisions taken to remove such content collide with, in particular, the freedom to conduct business or, as the case may be, freedom of expression as regards commercial communication. For example, where the notion of infringement extends to acts such as an alleged unlawful selling of, for example, goods acquired from a licensed trader who is acting against a contractual stipulation not to resell goods to third parties outside of a ‘closed’ selective distribution scheme, the question of whether a trader using the internet as a sales platform is actually violating intellectual property rights requires a complex legal assessment including questions related to European and domestic competition laws, and in such a case blocking orders based upon private agreements may well additionally collide with fundamental freedoms under European law. This study has, to be sure, not found that any of the VCPs has encountered any such complexities, and again it should be emphasised that disputes over the notion of infringement can ultimately be resolved through judicial proceedings.

Obviously, VCPs must adhere to such fundamental principle of proportionality which arises further out of both constitutional and European law as well as under national statutory data protection law. Thus, for example, retaining personal data of alleged infringers for a lengthy period, such as is the case in the French VCP, may be perceived critically. Proportionality, in that sense, means that data can only be stored and processed in as much and for long as is necessary for conducting the procedures.

This danger may be decreased where it is foreseen that public prosecution authorities are engaged from an early point in time during investigations, and are mitigated entirely where the VCP is based upon judicial proceedings, as is the case in Denmark. Essentially, the establishment of a VCP does not create a self-contained system of private enforcement; alleged infringers can take recourse to litigation.



## **CHAPTER 1: FRENCH CHARTER FOR THE FIGHT AGAINST THE SALE OF COUNTERFEIT GOODS ON THE INTERNET BETWEEN INTELLECTUAL PROPERTY RIGHTHOLDERS AND E-COMMERCE PLATFORMS**





## Chapter 1: Glossary of terms

For the purposes of this Chapter 1, the following definitions apply:

- **Article 29 WP**: the Article 29 Data Protection Working Party that was set up under the Data Protection Directive. It has advisory status, acts independently and is composed of a representative of the supervisory authority(ies) designated by each European Union country, a representative of the authority(ies) established for the European Union institutions and bodies, and a representative of the European Commission<sup>41</sup>.
- **Centraal Bureau voor de Rijwielhandel Decision**: Commission Decision 78/59/EEC of 2 December 1977 relating to a proceeding under Article 85 of the EEC Treaty<sup>42</sup>.
- **Charter**: the French charter for the fight against the sale of counterfeit goods on the internet between intellectual property rightholders and e-commerce platforms<sup>43</sup>.
- **Charter of Fundamental Rights**: the Charter of Fundamental Rights of the European Union<sup>44</sup>.
- **CJEU**: the Court of Justice of the European Union.
- **CNAC**: the French National Anti-Counterfeiting Committee<sup>45</sup> (*Comité National Anti-Contrefaçon*).
- **Counterfeit goods**: non-original physical goods manufactured without the consent of the relevant rightholder.
- **Data Protection Directive**: the Directive of 24 October 1995 on Data Protection<sup>46</sup>. At the moment of the drafting of this Study, the Data Protection Directive was in force. This Directive **has been repealed** by the General Data Protection Regulation on May 2016.
- **eBay CJEU Ruling**: the ruling issued on 12/07/2011 by the CJEU in Case C-324/09, L'Oréal-eBay, ECLI:EU:C:2011:474<sup>47</sup>.
- **E-Commerce Directive**: the Directive of 8 June 2000 on electronic commerce<sup>48</sup>.
- **EEA**: the European Economic Area.
- **Electronic Communications Directive**: the Directive of 12 July 2002 on the processing of personal data and the protection of privacy in the electronic communications sector<sup>49</sup>.
- **Enforcement Directive**: the Directive of 29 April 2004 on the enforcement of intellectual property rights<sup>50</sup>.

---

<sup>41</sup> [http://ec.europa.eu/justice/data-protection/article-29/index\\_en.htm](http://ec.europa.eu/justice/data-protection/article-29/index_en.htm).

<sup>42</sup> Commission Decision 78/59/EEC of 2 December 1977 relating to a proceeding under Article 85 of the EEC Treaty, OJ L 20, 25.1.1978, pp. 18-27.

<sup>43</sup> An English version of the Charter has been provided by the INPI and is attached as Annex 1 to this Chapter 1.

<sup>44</sup> Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, pp. 391-407.

<sup>45</sup> <http://www.cnac-contrefacon.fr/cnac/>.

<sup>46</sup> Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23/11/1995, pp. 31-50.

<sup>47</sup> <http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=324/09&td=ALL>.

<sup>48</sup> Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ L 178, 17/07/2000 pp. 1-16.

<sup>49</sup> Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31.7.2002, pp 37-47.

<sup>50</sup> Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, OJ L 157 of 30 April 2004.

- **European Union Directives:** the E-Commerce Directive, the Enforcement Directive and the Data Protection Directive collectively.
- **French Data Protection Law:** French Law No 78-17, of 6 January 1978, regarding IT, databases and liberties<sup>51</sup> (*Loi n° 78-17 relative à l'informatique, aux fichiers et aux libertés*).
- **French E-Commerce Law:** French Law No 2004-575, of 21 June 2004, regarding confidence in the digital economy<sup>52</sup> (*Loi n° 2004-575 pour la confiance dans l'économie numérique*).
- **French Enforcement Law:** French Law No 2007-1544, of 29 October 2007, regarding the fight against counterfeiting<sup>53</sup> (*Loi n° 2007-1544 de Lutte contre la Contrefaçon*).
- **French Regulations:** the French Data Protection Law, the French E-Commerce Law and the French Enforcement Law collectively.
- **HADOPI:** the French high authority for the diffusion of art works and the protection of rights on the internet<sup>54</sup> (*Haute Autorité pour la Diffusion des Oeuvres et la Protection des Droits sur Internet*).
- **InfoSoc Directive:** the Directive of 22 May 2001 on the information society<sup>55</sup>.
- **INPI:** the French National Industrial Property Institute<sup>56</sup> (*L'Institut National de la Propriété Industrielle*).
- **MOU:** the Memorandum of Understanding on the sale of counterfeit goods via the internet<sup>57</sup> of 4 May 2011, concluded at European Union level under the auspices of the European Commission.
- **Platform:** any online marketplace that provides businesses and/or consumers with a website through which physical goods can be offered, sold or purchased, based on the explanations of the various stakeholders interviewed for the purposes of this Chapter 1.
- **Promusicae CJEU Ruling:** the ruling issued on 29/01/2008 by the CJEU in Case C-275/06, Promusicae, ECLI:EU:C:2008:54<sup>58</sup>.
- **Regular Seller:** according to the Charter, any seller offering goods on Platforms' websites and fulfilling specific criteria defined by the signatories to the Charter (e.g., number of items offered for sale; sales volumes; values; period of completion of operations).
- **Rightholder:** any company owning any intellectual property rights for physical goods that may be sold on platforms' websites, based on the explanations of the various stakeholders interviewed for the purposes of this Chapter 1.
- **VCP:** 'voluntary collaboration practices' developed by industry, public bodies and/or third parties such as non-governmental organisations and then adhered to by the respective industry in addressing infringements of trade mark rights, design rights, copyright and rights related to copyright over the internet.

<sup>51</sup> <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460>.

<sup>52</sup> <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164>.

<sup>53</sup> <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000279082>.

<sup>54</sup> <http://www.hadopi.fr/en>.

<sup>55</sup> Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167, 22/06/2001 pp. 10–19.

<sup>56</sup> <http://www.inpi.fr/fr/accueil.html>.

<sup>57</sup> [http://ec.europa.eu/growth/industry/intellectual-property/enforcement/index\\_en.htm](http://ec.europa.eu/growth/industry/intellectual-property/enforcement/index_en.htm).

<sup>58</sup> <http://curia.europa.eu/juris/liste.jsf?language=en&num=C-275/06>.

## Chapter 1: Structure and content

This Chapter 1 analyses the Charter in depth, assessing the following elements:

- Role of signatories to the Charter and third parties;
- Analysis of the duties and procedures prescribed by the Charter;
- Coexistence of the measures set out in the Charter with European Union and French legal frameworks and related case law;
- Role of technologies used in implementing the duties and procedures laid down by the Charter;
- Costs assumed by the parties involved in the implementation of the Charter;
- Role of educational activities of the parties involved in promoting the Charter;
- Effectiveness of the measures set out in the Charter.

This Chapter 1 initially involved exhaustive desk research to identify the signatories to the Charter and third parties. A sample of these were then contacted; some agreed to be interviewed for the purposes of this Chapter 1, whilst others declined the invitation to participate.

The statements contained in this Chapter 1 on the signatories' and third parties' positions regarding the Charter and day-to-day procedure are based on the feedback and supporting documentation provided by those stakeholders that agreed to participate in the study.

## 1. Introduction

The Charter, which consists of 17 articles, is a VCP that establishes a code of conduct providing a set of preventive measures and reactive procedures to fight against the online sale of counterfeit goods.

It was drafted pursuant to a French government initiative launched in 2008 with the aim of fighting against the online sale of counterfeit goods. At that time, there was no generally established cooperation between platforms and rightholders in this respect.

The French Minister for the Economy entrusted the drafting of the Charter to the Chairman of the CNAC and to Professor of Law Pierre Sirinelli, with the support of the INPI.

Although the Charter was concluded in December 2009, as stated in the ‘Minutes of the meeting of signatories — French charters on the fight against internet counterfeiting’, a copy of which was provided by the INPI for the purposes of this Chapter 1, it was subject to an initial assessment period of 18 months after its signature and was actually implemented in February 2012.

After the implementation of the Charter in February 2012, the French government decided to launch two additional charters related to the fight against the online sale of counterfeiting goods, but addressed to other categories of intermediaries, i.e., small ads platforms<sup>59</sup> and postal operators<sup>60</sup>.

Between the signature of the Charter in 2009 and its implementation in 2012, the MOU was concluded at European Union level under the auspices of the European Commission with the aim of encouraging platforms and rightholders to undertake certain measures to fight against the online sale of counterfeit goods. The MOU has similar goals to the ones pursued by the Charter; in fact, both arrangements run in parallel.

The Charter is divided into the following main parts:

- Foreword: Contains a presentation of the scope of the Charter and the exceptions to it.
- Chapter 1 — Anti-counterfeiting measures. Refers to the preventive and proactive measures and procedures through which platforms can prevent illicit offers from being published or limit the consequences of such publication.
- Chapter 2 — Exchange of information between platforms and rightholders in the fight against counterfeiting. Regulates cooperation between the signatories to the Charter and the exchange of information between them.
- Chapter 3 — Conducting the testing process. Regulates the testing process to which the Charter was initially subject and the assessment of such process that took place 18 months after the signature of the Charter.

The Charter's main objectives are as follows:

- Reducing and stopping counterfeiting on the internet without harming the expansion of platforms.
- Finding concrete measures to prevent the sale of counterfeit goods over the internet.
- Facilitating a closer and constructive dialogue between platforms and rightholders and seeking transparent collaboration between them.
- Protecting consumers from buying counterfeit goods online.
- Introducing technical measures to detect the online sale of counterfeit products:
  - Identification of keywords showing the counterfeit nature of the products offered for sale (e.g., ‘false’; ‘imitation’; ‘fake’; ‘copy’).

---

<sup>59</sup> [http://www.economie.gouv.fr/files/Charte\\_lutte\\_contrefacon\\_internet\\_petitesannonces.pdf](http://www.economie.gouv.fr/files/Charte_lutte_contrefacon_internet_petitesannonces.pdf).

<sup>60</sup> [http://www.economie.gouv.fr/files/Charte\\_lutte\\_contrefacon\\_internet\\_titulaires\\_droits\\_operateurspostaux.pdf](http://www.economie.gouv.fr/files/Charte_lutte_contrefacon_internet_titulaires_droits_operateurspostaux.pdf).

- Identification of suspicious offers, (e.g., source and nature of the product; number of identical products offered for sale; methods of payment or delivery; state of brand new products and their packaging).
- Analysis of sellers' profiles and behaviours.
- Taking action against online sellers of counterfeit goods.

As explained by the INPI in the context of this Chapter 1, the Charter is a private arrangement between its signatories and adherence to it is voluntary. It is a tool that leaves the signatories free to implement the corresponding voluntary cooperation measures in order to fight against the online sale of counterfeit goods. Accordingly, when interviewed for the purposes of this Chapter 1, several signatories and third parties reported that the Charter was a non-binding cooperation tool for fighting against the online sale of counterfeit goods and that it did not prevent them from implementing different or additional procedures to those set out in the Charter.

Even though the text of the Charter refers to specific measures, there are no consequences or sanctions imposed on signatories for not complying with the duties set out in it. This has been confirmed by the INPI in relation to this Chapter 1 and derives from the general principle that the Charter has to be considered as a voluntary and private arrangement. Thus, there are signatories who comply with the measures laid down and are active in relation to the Charter, and there are others who do not play an active role in it but, as explained by the INPI, do not seek to renounce their status as a signatory.

## 2. Signatories to the Charter and third parties

The Charter does not specify which categories of stakeholders can sign. In practice, apart from platforms and rightholders, no additional categories have joined. This is because the duties and procedures laid down by the VCP for fighting against the online sale of counterfeit goods only address platforms and rightholders.

For instance, the Charter was signed in December 2009 by certain rightholders (either individually or as part of a professional federation) and certain platforms during a meeting organised by the French Minister for the Economy<sup>61</sup>. After the initial assessment of the Charter and its durable implementation in February 2012, additional rightholders and platforms decided to join the Charter<sup>62</sup>.

No public authorities, such as the INPI or the CNAC, are signatories to the Charter but both these bodies participated in its drafting. Currently, the INPI plays a supervisory role linked to relevant stakeholder discussions, while the CNAC does not participate explicitly in the Charter.

Finally, consumers, together with rightholders, represent one of the stakeholder categories that may benefit the most from the Charter as one of its main aims is to protect consumers from counterfeit goods. Notwithstanding the foregoing, civil society, in this case namely consumer associations, did not participate in the drafting of the Charter despite being invited to do so. When contacted for the purposes of this Chapter 1, the consumer associations also declined to participate, arguing that they do not deal with intellectual property right enforcement.

This section of the chapter explains the specific roles played in the VCP by the four categories of stakeholders mentioned (i.e., rightholders, platforms, public authorities and civil society).

### 2.1. Role of rightholders<sup>63</sup>

Rightholder signatories to the Charter represent intellectual property rights in relation to physical goods in a variety of sectors (e.g., consumer goods; fashion; consumer electronics; luxury goods; sports goods).

Some rightholders participated in the drafting of the Charter. Among those interviewed, one individual rightholder and one professional federation of rightholders contributed comments as part of a working group set up to that end by the French government.

In general, as explained in detail in Section 3 of this Chapter 1 ('Duties and Procedures'), the main role of rightholders in this VCP is to collaborate with signatory platforms and teach them how to distinguish counterfeit goods from genuine ones so that they acquire a high level of knowledge in this regard and are able to implement or update their mechanisms for fighting against online counterfeiting.

Two rightholders and one professional federation of rightholders stated that, after signing the Charter, they had started organising meetings to train platforms in how to recognise counterfeit goods, for example, showing them which key words to look for in offers submitted or published by sellers.

They also pointed out that, once platforms were knowledgeable about their goods, they only supervised the filters and measures applied by platforms.

### 2.2. Role of public authorities

#### 2.2.1. The INPI

The INPI is a public body, supervised by the French Ministry for the Economy.

---

<sup>61</sup> The list of signatories of the Charter in 2009 can be found in Annex 2 of this Chapter 1.

<sup>62</sup> The list of signatories of the Charter in 2012 can be found in Annex 3 of this Chapter 1.

<sup>63</sup> The Rightholders interviewed for this Chapter 1 represent a sample of those involved in the VCP.

Through the Secretariat of the CNAC, the INPI participated in the creation of all three French charters for the fight against the sale of counterfeit goods, including the Charter itself. It was designated by the Ministry for the Economy as the authority in charge both of the initial 18-month assessment process to which the Charter was subjected after its signature in 2009, and of supervising interaction between signatories.

Despite this supervisory role, as the Charter is not binding, the INPI does not regulate compliance by the signatories with the measures and procedures set out in the Charter. As mentioned, its supervisory role is rather linked to relevant stakeholder discussions.

If a new platform or rightholder wishes to join the Charter, the INPI is the public body responsible for:

- providing administrative support in relation to membership requests;
- informing the other signatories about membership requests;
- requesting the other signatories' opinions on membership requests.

At the time of conducting this Chapter 1, the INPI is in the process of organising new meetings with all signatories to the Charter in order to obtain their feedback regarding implementation of the measures laid down in the Charter and to gather their opinions with a view to improving these measures.

### 2.2.2. The CNAC

The CNAC is composed of public authorities and private sector representatives (i.e., industrial and artistic associations; professional associations; businesses and administrations) involved in the protection of intellectual property rights and in particular in anti-counterfeiting activities.

One of the aims of the CNAC is to strengthen the exchange of information and good practices between stakeholders in order to fight against counterfeiting; it also aims to coordinate and manage concrete actions and formulate new proposals.

The CNAC's activities relate to the infringement of any type of intellectual property right, including copyright and related rights, designs, patents and trade marks.

Even though the CNAC was involved in the drafting of the Charter, it does not participate actively and directly in it. However, it provides a forum where stakeholders can discuss enforcement matters related to the Charter, such as proposals for developing or modifying the Charter or the drafting of new charters.

## 2.3. Role of platforms<sup>64</sup>

Platform signatories to the Charter enable different types of transactions between buyers and sellers (e.g., consumer to consumer; business to consumer); their common characteristic is that they do not take title to the goods being sold.

Certain platforms participated in the drafting of the Charter as part of the working group set up by the French government.

The participation of platforms in the Charter enhances their image in the eyes of rightholders and consumers. One of the platforms interviewed explained that participation was one way of underscoring its commitment to the fight against the online sale of counterfeit goods.

The main duties required of platforms in this VCP are:

- implementing preventive measures that assume constant cooperation with rightholders;
- implementing technical measures with the aim of detecting offers of counterfeit products and identifying sellers offering and/or selling counterfeit products;

---

<sup>64</sup> The Platforms interviewed for this Chapter 1 are a sample of those involved in the VCP.



- implementing easy procedures for the notification of counterfeit offers by rightholders and consumers.

The platforms interviewed stated that the implementation of the Charter had not caused major changes in their internal procedures and measures for fighting against the online sale of counterfeit goods, apart from improving their relationship with rightholders, as they had already been taking action against online offers/sales of counterfeit goods prior to signing the Charter.

Platforms interviewed pointed out that the main objective of the Charter was precisely to strengthen the link between platforms and rightholders, so that both parties would be collaborating in the fight against the online sale of counterfeit goods. Such platforms indicated that the Charter had significantly improved communication between them and rightholders, with regular meetings being held with rightholders in order to learn, for example, how to detect offers of counterfeit goods by identifying keywords, and how to know when a good is counterfeit or not.

## 2.4. Role of civil society

One of the main aims of the Charter is to protect consumers from buying counterfeit goods online.

The French government, when drafting the Charter, considered that consumers' voices were important and decided to include, as one of the measures aimed at platforms, the implementation of an electronic mechanism that permits consumers to submit complaints regarding the online sale of counterfeit goods. This mechanism is explained in more detail in Section 3.3.3.2. of this Chapter 1 ('Electronic notification procedure addressed to consumers').

However, as pointed out by the interviewed platforms and rightholders and the INPI, consumer associations did not collaborate while the Charter was being drafted and they do not participate in it currently. This circumstance was also highlighted by Professor Sirinelli in the report he prepared for delivery at the presentation of the Charter before the World Intellectual Property Organisation in September 2011<sup>65</sup>.

Several French consumer associations were contacted in connection with this Chapter 1 in order to gather their opinion about the Charter. Unfortunately, none of them provided any input to this Chapter 1. Those contacted replied that they were not involved in the enforcement of intellectual property rights and thus could not contribute.

---

<sup>65</sup> [http://www.wipo.int/edocs/mdocs/enforcement/en/wipo\\_ace\\_7/wipo\\_ace\\_7\\_8.pdf](http://www.wipo.int/edocs/mdocs/enforcement/en/wipo_ace_7/wipo_ace_7_8.pdf).

### 3. Duties and procedures

This section summarises the duties and procedures laid down in the Charter. Nevertheless, as pointed out by the INPI, as the Charter merely makes collaboration between signatories voluntary, the duties and procedures mentioned are not always implemented in practice or exercised automatically by platforms and rightholders — or at least not in the way envisaged by the Charter.

In this sense, the Charter specifically provides in its foreword that ‘Whatever legislation governs their activities, the signatory platforms and right holders are free to commit themselves to implementing the practical measures defined [...] [and] these actions shall have no consequences on current or future legal proceedings.’

Some signatories indicated during the interviews conducted that they considered this VCP to be ‘soft law’, as they can adapt the duties and procedures laid down in it to their own businesses and know-how, and implement them at their own convenience.

Some platforms and rightholders interviewed underlined that they had already implemented some measures to fight against the online sale of counterfeit products prior to signing the Charter. Therefore, they did not have to change their policies and procedures radically in order to be in line with the spirit of the Charter.

In day-to-day practice, not all signatory platforms comply with all the duties and procedures laid down by the Charter, and there are no consequences to suffer for this. Indeed, although the Charter stipulates that a party may request the intervention of the INPI in the event that another party does not respect its obligations (Article 16 of the Charter (‘Durable deployment of the Charter’)), and that the defaulting party may no longer promote itself as a signatory where such a breach is confirmed, this has, according to the INPI, never happened in practice.

Apart from fighting the online sale of counterfeit products, one of the main objectives of the Charter is to establish close and flexible collaboration between rightholders and platforms; this is primarily based on an exchange of information as explained under Section 3.2.1. of this Chapter 1 (‘Exchange of information between platforms and rightholders’).

Having said that, the duties and procedures imposed by the Charter on its signatories in order to achieve its objectives can be categorised as follows:

- **Becoming a signatory.** Rightholders and platforms that wish to become signatories to the Charter must submit their requests to the INPI.
- **Preventive measures.** The Charter contains various measures to enable platforms, with rightholders’ support, to prevent the submission of offers related to counterfeit products.
- **Proactive measures.** The Charter proposes a wide range of measures to enable platforms, with the assistance of rightholders and consumers, to fight against the online sale of counterfeit products after offers have been submitted to them.
- **Sanctions.** When a platform effectively confirms that a seller is offering or selling online counterfeit goods, specific sanctions need to be imposed on the seller by the platform (e.g., suspending or closing the seller’s account(s)).

## 3.1. Becoming a signatory

### 3.1.1. Territorial scope

Although French public authorities drafted the Charter, and some of its provisions make specific reference to France<sup>66</sup>, it does not contain any precise reference to its territorial scope of application.

When interviewed for this Chapter 1, the INPI explained that the Charter was in fact aimed not only at French territory but could also be joined by rightholders or platforms located in other countries — in the case of platforms, regardless of whether or not their websites addressed French users.

### 3.1.2. Timeframe

Although all the current signatories joined the Charter either when it was signed (December 2009) or, after testing, when it was implemented (February 2012), stakeholders can apply to join whenever they like.

### 3.1.3. Procedure

The Charter does not indicate the joining procedure.

The INPI has clarified that rightholders or platforms interested in joining the Charter merely have to send a corresponding application; there are no specific formalities — applications can even be made by email.

The INPI examines applications received and in parallel offers existing signatories the opportunity to comment on and/or object to candidates' applications. Where no issue is raised concerning a potential candidate during the month following its application to join, the INPI approves its application.

One of the platforms interviewed explained that existing signatories had not opposed any new candidates' applications so far. However, where there were opposition, the INPI would request that the stakeholder concerned adapt its anti-counterfeiting procedures and then file a new application.

## 3.2. Preventive measures aimed at platforms before offers are submitted by sellers

### 3.2.1. Exchange of information between platforms and rightholders

As explained under Section 3.3. of this Chapter 1 ('Proactive measures to be applied by platforms after offers are made available to the public'), Platforms and rightholders are required to exchange information and collaborate proactively when they suspect that an offer concerns a counterfeit product or a seller is likely to sell counterfeit goods. Beyond such collaboration regarding concrete offers/sellers, the categories of signatories mentioned are also required to cooperate continuously and exchange information that may be of help in the fight against the online sale of counterfeit products. Indeed, signatories commit themselves to repeatedly gathering new and updated information and sharing it.

In this sense, platforms and rightholders are obliged to designate at least one correspondent within their organisations who will be responsible for dealing with matters related to the Charter, one of the most important of such matters being to ensure collaboration between signatories to the Charter (Article 10 of the Charter ('Correspondents and contact methods dedicated to anti-counterfeiting')).

---

<sup>66</sup> E.g. Article 9 of the Charter ('Offers of sale from regular sellers of products of categories identified as the most subject to counterfeiting') reads as follows: '[...] The platforms agree to identify the individuals, whether based in France or selling products on the French market [...]'.

Moreover, as often as is needed and at least once a year, rightholders and platforms have to organise meetings (either bilateral or multilateral) to exchange specific information for defining and adapting the platforms' tools in order to detect offers of counterfeit goods or sellers likely to sell counterfeit goods (Article 12 of the Charter ('Development, adaptation and update of detection tools')).

Two of the rightholders interviewed said that they sometimes organised meetings to explain to platforms how to identify counterfeit versions of their brands. In this regard, the criteria they transmit to platforms are based, for example, on prices (e.g., too low or too high), pictures (e.g., quality of the pictures shown in the offers), texts (e.g., strange description of the product) and comments made by users about the seller or the product itself. They informed platforms about which of their products were most likely to be counterfeited so that platforms could pay special attention to them.

The Charter places great emphasis on confidentiality when it comes to the exchange of information between platforms and rightholders; both parties are required to take all necessary measures to maintain confidentiality (e.g., specific contractual provisions with their own staff and/or contractors).

### 3.2.2. Provision of information to sellers of products most subject to counterfeiting

According to Article 1 of the Charter ('Providing information to sellers and ensuring consumer awareness'), platforms have to inform sellers of 'products within the categories most subject to counterfeiting' about the following:

- their obligation to guarantee the authenticity of the products they propose for sale;
- the sanctions they risk under penal law and under the general terms and conditions of sale of platforms if they sell counterfeit goods.

Thus, even before sellers of the category of products mentioned start to offer them, they need to be informed about the consequences of counterfeiting.

Generally speaking, the platforms determine the products most subject to counterfeiting mainly on the basis of the following resources:

- information collected through their own means, including, inter alia, complaints received directly from consumers who have been the victims of counterfeiters;
- information supplied by rightholders, based on the collaboration tools mentioned under Section 3.2.1. of this Chapter 1 ('Exchange of information between platforms and rightholders'), as rightholders are the ones that handle the most complete data about their own products.

The platform PriceMinister, for example, drafts a report on a yearly basis that shows its results in relation to the implementation of measures against counterfeiting and includes a ranking of the products most counterfeited: 'Bilan de la Lutte Anti-Contrefaçon Priceminister-Rakuten'<sup>67</sup>. According to PriceMinister's 2014 report, mobile phone brands (e.g., Samsung; Apple), mobile accessories (e.g., Monster Cable; Spigen) and high-tech accessories (e.g., Toshiba; Kingston; SanDisk) top the rankings of counterfeit goods. Other brands represented are leading fashion brands (e.g., Nike; Armani; Guess; Chanel), while yet others, like Babyliiss hair care products, are newcomers to the rankings.

Once it is determined by each platform which of the products are most subject to counterfeiting, platforms are alerted whenever a seller offers a product that falls within this category; alerts are given using technologically state-of-the-art measures implemented specifically for this purpose (see Section 3.3.2. of this Chapter 1 ('Use of automatic tools to detect offers and sellers')). The relevant sellers are then informed of their obligation to guarantee the authenticity of the products they offer for sale as well as of the sanctions that might apply to them for any counterfeit activities.

The Charter requires platforms to comply with this duty to inform by means of messages transmitted automatically when the seller submits the offer to the platform. Nevertheless, in practice, as explained by platforms interviewed,

---

<sup>67</sup> <http://www.priceminister.com/blog/bilan-anti-contrefacon-2014-13251>.

not all platforms use specific messages to inform the sellers in question about their obligations. Rather than using customised warnings for specific sellers, the relevant information is sometimes set out in platforms' legal terms, which must be accepted by sellers before they can sell their products through platforms' websites. Additionally, some platforms, such as one of those interviewed, have a specific section on anti-counterfeiting policies on their websites that users can visit at any time.

### 3.3. Proactive measures aimed at platforms after offers have been submitted by sellers

The preventive measures described in the preceding section of this Chapter 1 may not always be sufficient to guarantee the authenticity of all the products offered on platforms.

Counterfeiters may circumvent the preventive measures set out by the Charter, for example, by selling products that may not be categorised as most subject to counterfeiting.

Indeed, despite the preventive measures provided for by the Charter, offers of counterfeit goods might still be submitted to platforms and become available on platforms' websites. To fight such offers, the Charter has laid down several specific procedures.

#### 3.3.1. Identification of Regular Sellers

Platforms have to identify Regular Sellers (Article 9 of the Charter ('Offers of sale from regular sellers of products of categories identified as the most subject to counterfeiting')).

Regular Sellers are categorised as such if they fulfil certain criteria related to the number of articles offered for sale, sales volumes, sales values and the period of completion of the operations. The behavioural criteria mentioned are provided as examples by the Charter, but signatories are expected to cooperate to adopt additional ones.

The platforms interviewed clarified that, to identify Regular Sellers, they use automated filters that detect sellers fulfilling the two following conditions:

- they sell products that fall within the categories most subject to counterfeiting; and
- they match the selling behaviour criteria defined jointly by platforms and rightholders.

Sellers categorised as Regular Sellers are asked by platforms to verify their identity and their address on threat of suspension of their account; such procedures have to be clearly indicated in platforms' general terms and conditions.

French Regular Sellers, for example, are asked to provide a copy of their 'Kbis' declaration<sup>68</sup>, their identity card, their SIREN/SIRET<sup>69</sup> number and/or a French bank account number.

One of the platforms interviewed stated that in practice they directly categorise professional sellers (i.e., businesses) as Regular Sellers. They require such Regular Sellers to provide evidence of their identity when they first register on the platform's website.

Finally, as Article 9 of the Charter ('Offers of sale from regular sellers of products of categories identified as the most subject to counterfeiting') stipulates, platforms keep the information they receive from Regular Sellers for at least as long as the sellers' accounts remain operational and for a period of 5 years after their closure.

---

<sup>68</sup> Document evidencing the registration of a company at the French Commercial Registry.

<sup>69</sup> French Business Register.

### 3.3.2. Use of automatic tools to detect offers and sellers

Platforms and rightholders agreed to test, during a period of 18 months from the signature of the Charter, the use of technologically state-of-the-art measures (e.g., keyword searches) for monitoring and immediate detection of the following categories of offers and sellers:

- offers of sale of counterfeit products;
- offers that use well-known trade marks for 'keyword spamming'<sup>70</sup>;
- sellers of counterfeit products based on their behaviour.

The underlying principle behind these measures, set out in Article 3 of the Charter ('Measures to detect counterfeiting'), is that certain offers/sellers of counterfeit products can be detected by analysis of their content, while others can be identified by examining general selling behaviours.

Although the Charter was implemented definitively after the 18-month test period following its signature, signatory platforms and rightholders have continued to use these measures.

Article 5 of the Charter ('Handling offers of sale of counterfeit goods and sellers of counterfeit products') stipulates that platforms need to refrain from publishing online offers of sale concerning counterfeit products that have been detected using the aforementioned measures.

As already indicated under Section 3.2.2. of this Chapter 1 ('Provision of information to sellers of products most subject to counterfeiting'), the information that serves as a basis for the technical tools used to detect the categories of offers and sellers referred to by the Charter (i.e., offers of sale of counterfeit products; offers that use well-known trade marks for 'keyword spamming'; and sellers of counterfeit products based on their behaviour) is obtained by platforms either directly, through their own means, or gathered through rightholders' collaboration with platforms.

Based on the feedback obtained by platforms interviewed during this Chapter 1, the parameters they take into account to feed and enhance the technical tools used include the following:

- Detection of offers:
  - the categories of products identified as most subject to counterfeiting (see Section 3.2.2. of this Chapter 1 ('Provision of information to sellers of products most subject to counterfeiting'));
  - the text of the offer itself (e.g., photograph; description of the product);
  - location of the product.
- Detection of sellers:
  - seller's behaviour (e.g., sales history; non-professional sellers with a huge quantity of a particular product; price of the products);
  - location of the seller.

In cases where the monitoring activities performed by platforms based on their automatic tools match an offer of a counterfeit product or a seller of counterfeit products, the offer/seller is considered suspicious; in accordance with the Charter, this triggers certain procedures against sellers as explained in the following sections of this Chapter 1.

### 3.3.3. Notification mechanisms to be made available to rightholders and consumers

The Charter provides for two electronic notification procedures through which platforms can be informed about counterfeit goods or sellers of counterfeit goods, namely:

---

<sup>70</sup> Keyword spamming means advertising a well-known trade mark with no relation to the product for sale.

- electronic notification procedure specific to rightholders;
- electronic notification procedure specific to consumers.

### *3.3.3.1. Electronic notification procedure specific to rightholders*

The focus of rightholders' participation in the VCP is not only on providing general information to platforms about their products to enable them to identify counterfeit products as explained under Section 3.2.1. of this Chapter 1 ('Exchange of information between platforms and rightholders').

Additionally, through effective, efficient, easily accessible and electronic means (e.g., a specific section on platforms' websites or a specific email address), rightholders can inform platforms about specific offers of sale concerning counterfeit products or sellers that are offering counterfeit products for sale.

Rightholders therefore need to adopt a proactive attitude as they have to search these offers/sellers and inform the platforms about them. The Charter requires that rightholders indicate in their notifications why they consider the notified goods to be counterfeit; this helps platforms develop and build the detection measures outlined in Section 3.3.2. of this Chapter 1 ('Use of automatic tools to detect offers and sellers').

Some of the rightholders interviewed see the rightholders' specific notification procedure as a way of creating a connection between platforms and rightholders; as one platform pointed out during interview, the training and support from rightholders is what really makes their assistance efficient.

Two of the rightholders interviewed pointed out that, in practice, aside from the official notification procedure, rightholders sometimes also spontaneously notify platforms. For example, one of the luxury brands interviewed does not produce phone covers as such but small wallets in which mobile phones can be kept. Some sellers were offering on platforms' websites phone covers that appeared to be of this brand as they were well designed and expensive, which made platforms believe that they were genuine. When the rightholder became aware of what was going on, it notified the platforms informally rather than through the electronic notification procedure, and provided specific documents which proved that it did not produce the phone covers in question.

### *3.3.3.2. Electronic notification procedure specific to consumers*

Consumers can use an easily accessible and readily visible section of platforms' websites to inform platforms that they are victims of counterfeiters (Article 8 of the Charter ('Consumer complaints')).

Likewise, platforms can feed their databases with the information received via consumer complaints.

Platforms sometimes forward consumers' complaints to rightholders if they need the latter's expertise to determine whether a product is genuine or not.

In practice, once a complaint has been made, the user most often sends the actual product to the platform. If the latter has any doubt about the authenticity of the product, it contacts the relevant rightholder.

The platforms interviewed found that the notification procedure for consumers generally worked in practice as intended by the Charter. Once an offer of a counterfeit product is published, it is usually detected as a result of notifications received from customers since, as explained above, rightholders do not use their specific notification procedure very often. One of the platforms interviewed stated that the number of counterfeit offers taken down as a result of the consumers' notification procedure was even higher than that resulting from the detection measures implemented by platforms.

### *3.3.4. Temporary conditions for bids of products most subject to counterfeiting*

The Charter provides for a second action for platforms regarding products most subject to counterfeiting in addition to the identification of such products explained under Section 3.2.2. of this Chapter 1 ('Provision of information to sellers of products most subject to counterfeiting').

This second action consists of prohibiting bid periods of less than ten days for such products (Article 7 of the Charter ('Handling offers of sale of products in the categories most subject to counterfeiting')).



Therefore, when a bid for a product that falls within the category in question is detected by the platforms' technologically state-of-the-art measures, it will have to last for at least 10 days from its publication.

### 3.3.5. Request for documentation proving the authenticity of the products

The Charter provides that platforms have to request from sellers documents that prove the authenticity of the products they are offering for sale when the sellers are considered likely to sell counterfeit products (Article 5 of the Charter ('Handling offers of sale of counterfeit goods and sellers of counterfeit products')).

Such requests for documentary proof of the authenticity of products does not follow a suspicious offer but is based on the seller itself, i.e., if it is considered likely to sell counterfeit products. This means that, even where the offer may not seem suspicious (e.g., the price is not too low and/or the image shows a genuine product), sellers may still be considered suspicious in terms of selling counterfeit products.

Whether or not a seller is considered likely to sell counterfeit goods is based on, for example, the platforms' technologically state-of-the-art measures, or follows from the electronic notification procedures laid down by the Charter.

The platforms interviewed specified that they usually requested documentation to prove the authenticity of products as soon as they had suspicions and not only in the specific cases envisaged by the Charter. Some platforms even contact suspicious sellers by telephone to ask them to clarify any doubts they may have and to prove the authenticity of the product.

In practice, when an offer concerning a counterfeit good is detected directly rather than by requesting documentary proof of the authenticity of products from sellers likely to sell counterfeit products, the sanctions (see Section 3.4. of this Chapter 1 ('Sanctions')) will be directly applied. This may be the case, for example, when a rightholder has confirmed that certain goods are not genuine. Similarly, some platforms receive the goods before they are sold, and verify then if they are counterfeit or not. In other situations, sellers use pictures from which it is obvious that the goods are not genuine.

### 3.3.6. Specific measures foreseen for products located outside the EEA and sellers based outside this Area

Article 6 of the Charter ('Handling offers of sale of goods imported into the European Economic Area')) applies where platforms identify through their technologically state-of-the-art measures that either the seller or the product offered for sale is located outside the EEA.

The Charter reminds us that, if there is no international exhaustion of intellectual property rights, imports of products bearing trade marks protected in France are subject to the authorisation of the rightholder concerned.

Therefore, when goods located outside the EEA are offered through a signatory platform, or a seller located outside the EEA offers goods through a signatory platform, the platform in question must ask the seller to provide documentary proof that appropriate authorisation has been received from the underlying rightholder.

The foregoing does not prevent rightholders from notifying platforms directly if they become aware of such circumstances by means of their own, for example, through the procedure described under Section 3.3.3.1. of this Chapter 1 ('Electronic notification procedure addressed to rightholders'). In such cases, platforms would no longer require sellers to provide documentary proof that they have obtained the rightholders' authorisation to sell the product but would proceed directly to apply the sanctions described under Section 3.4.3. of this Chapter 1 ('Sanctions envisaged for sellers based outside the EEA or products located outside the EEA borders').

## 3.4. Sanctions

The Charter provides for three different categories of sanctions:

- sanctions applicable to offers of counterfeit goods;

- sanctions applicable to sellers likely to sell counterfeit goods;
- sanctions applicable to sellers/products located outside the EEA.

#### 3.4.1. Sanctions foreseen for offers of counterfeit goods

Article 5 of the Charter ('Handling offers of sale of counterfeit goods and sellers of counterfeit products') states that if, despite use of the measures described under Section 3.2. ('Preventive measures to be applied by platforms before offers being made available to the public') and Section 3.3. ('Proactive measures to be applied by platforms after offers are made available to the public') of this Chapter 1, offers of counterfeit goods still become available on platforms' websites, platforms must:

- take down the relevant offer immediately;
- take all necessary measures to prevent its republication;
- suspend immediately and for a period of 6 months all accounts identified as belonging to the seller that has submitted the offer concerned, including any opened under different usernames;
- in the event that another such offer from the same seller is detected, close all accounts belonging to the seller and deploy all measures at their disposal to prevent the reregistration of the seller for a period of 5 years.

#### 3.4.2. Sanctions foreseen for sellers likely to sell counterfeit goods

Under Article 5 of the Charter ('Handling offers of sale of counterfeit goods and sellers of counterfeit products'), if platforms identify sellers likely to sell counterfeit products, they undertake to act as follows after having asked sellers to prove the authenticity of the products they are offering for sale:

- pending delivery of documentary proof of authenticity of the products, platforms must suspend sellers' accounts.
- where sellers cannot provide such documentation, platforms must close all sellers' accounts, including any opened under different usernames, and deploy all measures to prevent the reregistration of those sellers for a period of 5 years.

#### 3.4.3. Sanctions foreseen for sellers based outside the EEA or products located outside the EEA borders

Under Article 6 of the Charter ('Handling offers of sale of goods imported into the European Economic Area'), where platforms identify (i) sellers located outside the EEA or (ii) offers of goods located outside the EEA, they undertake to act as follows after having asked sellers to provide documentary proof of having received appropriate authorisation to sell the goods from the underlying rightholder:

- platforms must withdraw the offer of sale concerned where sellers cannot produce documentary proof of authorisation from the rightholders to sell the products or where the rightholders directly inform the platforms accordingly.
- in the event that another such offer is detected subsequently, platforms must close sellers' accounts without time limit.

#### 3.4.4. Practical considerations concerning sanctions

Platforms interviewed reported that, in practice, when they detect a suspicious offer or seller, for example through their technologically state-of-the-art measures or other means (e.g., notification procedures), they generally give sellers the chance to defend their position with appropriate arguments. Indeed, in most cases sellers are given the

opportunity to prove the authenticity of their products (sometimes before and sometimes after the sanction is applied, depending on the platform).

The two platforms interviewed stated that when they confirmed that a product sold through their website was not genuine, they went beyond the sanctions laid down by the Charter and automatically blocked sellers' accounts for a period of 5 years.

## 4. Coexistence of the measures set out in the VCP with European Union and French legal frameworks and related case law

This section of Chapter 1 ('Coexistence of the measures set out in the VCP with the European Union and French legal frameworks and related case law') summarises the European Union and French legal framework and related case law that may have an impact on the practical application of the Charter's provisions.

The considerations included in this section are based upon the following legal sources:

- Charter of Fundamental Rights of the European Union (Section 4.1. of this Chapter 1 ('Charter of Fundamental Rights')).
- European Union Directives (Section 4.2. of this Chapter 1 ('European Union Directives')).
- Constitutional prerequisites and fundamental rights in France (Section 4.3. of this Chapter 1 ('Constitutional prerequisites and fundamental rights in France')).
- French Regulations (Section 4.4. of this Chapter 1 ('French Regulations')).

### 4.1. Charter of Fundamental Rights

The fundamental rights set out below, provided for by the Charter of Fundamental Rights of the European Union, might potentially have an impact on the duties laid down by the Charter<sup>71</sup>:

- Article 8: 'Protection of personal data'. This right generally serves to protect the self-determination right of individuals regarding the use of personal data related to them.
- Article 16: 'Freedom to conduct a business'. This right includes the freedom to exercise an economic or commercial activity and the freedom of contract.
- Article 17: 'Right to property'. This right stipulates that no one will be deprived of his or her possessions except in the public interest and in the cases and under the conditions provided for by law, subject to fair compensation being paid in good time for the loss. Protection of intellectual property (including literary and artistic property, as well as patent and trade mark rights and associated rights) is explicitly covered by this right.
- Article 47: 'Right to an effective remedy and to a fair trial'. This right establishes that everyone whose rights and freedoms guaranteed by the law are violated has the right to an effective remedy before a tribunal. It includes the right to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law.

The enforceability and acceptability of self-regulatory measures like the Charter depends, inter alia, on whether the fundamental rights of the persons concerned have been taken into consideration.

Insofar as a fair balance between the interests of the parties concerned is needed, VCP models have to respect and safeguard the aforementioned fundamental rights.

### 4.2. European Union Directives

The following provisions of the European Union Directives might potentially have an impact on the duties laid down by the Charter<sup>72</sup>:

- Article 14 of the E-Commerce Directive. This Article essentially states that hosting service providers are not liable for information stored at the request of the recipient of the services, provided that (i) they do

---

<sup>71</sup> See complete wording in Annex 4 of this Chapter 1.

<sup>72</sup> See complete wording in Annex 4 of this Chapter 1.

not have actual knowledge of illegal activity or information and, as regards claims for damages, are not aware of facts or circumstances from which the illegal activity or information is apparent; or (ii) upon obtaining such knowledge or awareness, they act expeditiously to remove or to disable access to it.

- Article 15(1) of the E-Commerce Directive. This Article states that providers of intermediary services are not subject either to an obligation to monitor the information that they transmit or store, or to a general obligation actively to seek facts or circumstances indicating illegal activity.
- Article 3 of the Enforcement Directive. This Article provides that the measures and remedies aimed at ensuring the enforcement of intellectual property rights must be (i) fair, (ii) equitable, (iii) not unnecessarily complicated or costly, or entailing unreasonable time limits or unwarranted delays, (iv) effective, (v) proportionate, (vi) dissuasive, and (vii) applied in such a manner as to avoid the creation of barriers to legitimate trade and to provide for safeguards against their abuse.
- Article 6(1)(e) of the Data Protection Directive. This Article provides that personal data must be kept for no longer than is necessary for the purposes for which it was collected.
- Article 7 of the Data Protection Directive. This Article establishes the circumstances under which the processing of personal data is considered legal: for example, when the data subject has given his or her unambiguous consent thereto, when processing is necessary for compliance with a legal obligation or when it is necessary for the purposes of the legitimate interests of the data controller or a third party.

The aforementioned European Union Directives have been interpreted, *inter alia*, in the following CJEU cases<sup>73</sup>:

- eBay CJEU Ruling

This Ruling establishes guidelines to be followed by online marketplaces such as eBay for implementing technical procedures to fight against piracy in respect of intellectual property rights and may impact on the French VCP since it provides for the implementation of technologically state-of-the-art measures to monitor and detect, *inter alia*, offers of sale of counterfeit products and sellers offering counterfeit products for sale.

- Promusca CJEU Ruling

This Ruling establishes that the protection of intellectual property rights is not of a higher order than that of other fundamental rights; this means that the protection of intellectual property rights does not prevail over other rights, such as the freedom to conduct a business.

It is important to consider the *Centraal Bureau voor de Rijwielhandel* Decision. This decision was the first and is the leading European Union case to determine the legal limitations of self-regulation and codes of conduct among private entities and individuals. The European Commission in this case held that a code of conduct adopted by the Central Bicycle Trade Association in the Netherlands (*Algemeen Reglement*<sup>74</sup>) could only be enforced if the rules either 'represent existing legislation' or 'are based on the established case law related to unfair competition'<sup>75</sup>. This case is thus the main reference for codes of conduct and their implications for restriction of freedom of trade.

### 4.3. Constitutional prerequisites and fundamental rights in France

The following fundamental rights set out in the French Declaration of the Rights of Man and of the Citizen of 1789 (*Déclaration des droits de l'homme et du citoyen*), referenced in the French Constitution of 4 October 1958 (*Constitution de la République française*) may have an impact on certain measures envisaged by Charter<sup>76</sup>:

- Article 4: 'Freedom to conduct a business'.

---

<sup>73</sup> See detailed description in Annex 5 of this Chapter 1.

<sup>74</sup> The *Algemeen Reglement* can be described as a general and comprehensive system organising the market for the distribution and servicing of bicycles and related articles in the Netherlands, set up as a private initiative but claiming and receiving general recognition.

<sup>75</sup> Note 27 of the *Centraal Bureau voor de Rijwielhandel* Decision.

<sup>76</sup> <http://www.assemblee-nationale.fr/connaissance/constitution.asp#preamb>; Annex 6 of this Chapter 1 contains the complete wording in English of the articles mentioned.

- Articles 2 and 17: 'Right to property'.

In addition, the right to an effective remedy and to a fair trial set out in Article 6 of the European Convention on Human Rights of 4 November 1950 is also applicable in France since this Convention lays down principles generally accepted before French Courts and might also have an impact on the interpretation of the Charter.

These fundamental rights have been considered by French courts. Below are some examples of relevant cases:

- French Constitutional Council Decision No 2000-436 DC of 7 December 2000

In this decision, the French Constitutional Council considered that it would be against the freedom to conduct a business if administrative authorisation was required to change the location of commercial premises.

- French Constitutional Council Decision No 2010-614 DC of 4 November 2010

This decision concerns a French law whose aim was to implement an agreement between France and Romania in order to regulate the escort of isolated minors located in France back to their country. The authorisation of such escort was taken by, inter alia, the office of the French special prosecutor for children. The French Constitutional Council considered that the law was contrary to the French Constitution as no appeal was granted to minors against the prosecutor's decision, and this was against the right to an effective judicial remedy.

#### 4.4. French Regulations

As a member of the European Union, France has converted the European Union Directives analysed previously in this Chapter 1 into national law. The following articles of the French Regulations may have an impact on certain measures envisaged by the Charter:

- Articles 6, 7 and 25 of the French Data Protection Law, which implements the Data Protection Directive.
- Articles 1, 6 I-2°, 6 I-7° and 6 I-8° of the French E-Commerce Law, which implements the E-Commerce Directive.
- Article L. 716-6 et seq. of the French Enforcement Law, which implements the Enforcement Directive.

The French Regulations have been taken into consideration by French Courts in the following cases:

- Decision of the Commercial Court of Paris of 30 June 2008, No 2006-065217 — *Christian Dior/E-Bay*

This decision held that a general filtering system implemented by an online marketplace such as eBay to fight against piracy in respect of intellectual property rights was permissible in the light of the European Union legal framework. In a decision dated 3 September 2010, the Court of Appeal of Paris confirmed that decision.

However, both decisions were handed down prior to the implementation in France of the French E-Commerce Law and before the eBay and Promusicae CJEU Rulings and are not consistent with them.

- Decision of the Tribunal de Grande Instance of Paris of 10 February 2012

This decision held that the blocking by an internet services provider of any future website on the grounds of a previous court decision that declared that a specific website edited unlawful content would not be in line with Article 6 I-8° of the French E-Commerce Act. This would grant internet services providers the powers of a judge (however, a judge is not allowed to delegate his or her powers without legislative authorisation).

## 4.5. Analysis of the VCP in relation to the European Union and French legal frameworks and case law

In the light of the European Union and French legal frameworks and related case law discussed in the preceding sections of this Chapter 1, it appears that certain duties and procedures envisaged by the Charter may be considered inconsistent with certain fundamental rights or legal provisions as mentioned below. Specifically, this section contains an analysis of the following three articles of the Charter, assessing their compatibility with the European Union and French legal frameworks and case law:

- Article 3 of the Charter ('Measures to detect counterfeiting').
- Article 5 of the Charter ('Handling offers of sale of counterfeit goods and sellers of counterfeit products').
- Article 9 of the Charter ('Offers of sale from regular sellers of products of categories identified as the most subject to counterfeiting').

Pursuant to the Promusicae CJEU Ruling, the protection of intellectual property rights must not be understood as being of a higher interest than that of other fundamental rights. Therefore, during the subsequent analysis the coexistence of the Charter with the following fundamental rights will be reviewed in detail:

- right to the protection of personal data related to sellers;
- right of sellers to an effective remedy and to a fair trial;
- right of sellers and platforms to conduct a business.
- There is also an analysis of whether certain duties established by the Charter are in line with Articles 14 and 15(1) of the E-Commerce Directive and Articles 6 I-2° and 6 I-7° of the French E-Commerce Act.

As previously explained in this Chapter 1, the Charter is a voluntary cooperation tool to which platforms can adhere and which leaves them free to implement the corresponding measures for fighting against the online sale of counterfeit goods. Therefore, the analysis below is valid for cases where the Charters' signatories actually implement the duties and procedures laid down by the Charter. Under any other circumstances (e.g., signatories not complying, or only partially complying, with those duties and procedures) both the analysis performed and conclusions reached would be distorted.

### 4.5.1. Coexistence of the Charter with the protection of personal data related to sellers

This section analyses whether certain duties relating to platforms laid down by the Charter are in line with the Data Protection Directive and French Data Protection Law.

To clarify: the considerations below only apply to the processing of personal data of sellers that are natural persons, as the processing of information related to sellers that are legal persons is outside the scope of the Data Protection Directive and French Data Protection Law.

#### 4.5.1.1. *Coexistence of the automated monitoring activities required by the Charter with the protection of personal data related to sellers*

This section analyses whether the protection of personal data related to sellers may have an impact on the platforms' technical monitoring duties laid down by the Charter, specifically the duty to monitor offers and sellers (Article 3 of the Charter ('Measures to detect counterfeiting')) and the duty to detect and identify sellers likely to sell products most subject to counterfeiting (Article 9 of the Charter ('Offers of sale from regular sellers of products of categories identified as the most subject to counterfeiting')).



#### 4.5.1.1.1. LEGITIMACY OF THE AUTOMATED DATA PROCESSING ACTIVITIES FOLLOWING FROM PLATFORMS' MONITORING ACTIVITIES

It will first be analysed whether the processing of personal data related to sellers following from the technical monitoring activities provided for by the Charter is in line with the French Data Protection Law.

Article 7 of the French Data Protection Law, which implements Article 7 of the Data Protection Directive, provides that the processing of personal data generally requires data subjects' consent or, alternatively, must be based on one of the following conditions:

- the data processing activities are necessary to comply with a legal obligation;
- the data processing activities are necessary to preserve the vital interests of the data subject;
- the data processing activities are necessary for the execution of a public service mission;
- the data processing activities are necessary for the execution of a contract to which the data subject is a party, or for the application of pre-contractual measures;
- the data processing activities are necessary for the protection of a legitimate interest provided such interest does not override the fundamental rights of data subjects.

In order for the data processing activities that follow from platforms' technical monitoring duties to be duly legitimised, one of the grounds provided for by Article 7 of the French Data Protection Law must apply. As not all the grounds mentioned seem appropriate for platforms due to their nature, only the following alternatives may be considered:

- Obtaining sellers' consent to perform the data processing activities. Based on the information provided by platforms interviewed, it seems that platforms do not always specifically request sellers' consent to the monitoring activities envisaged by the Charter.
- Arguing that the data processing activities are required to protect platforms' legitimate interests and that the interests and fundamental rights of sellers are not overridden.
  - It would seem reasonable to assume that the automated data processing activities envisaged by Article 3 of the Charter ('Measures to detect counterfeiting'), which may result in the application of the sanctions provided for by Article 5 of the Charter ('Handling offers of sale of counterfeit goods and sellers of counterfeit products'), are conducted by platforms based on their legitimate interests and do not breach sellers' rights, as explained in more detail in Section 4.5.1.2 of this Chapter 1 ('Coexistence of the retention of sellers' personal data for a period of 5 years with the protection of personal data related to sellers'). Indeed, these monitoring activities may fulfil certain criteria provided for by the Article 29 WP in its Opinion 06/2014<sup>77</sup> that lead to reinforce platforms' legitimate interests, for example: platforms are not only acting in their own legitimate interests but also in the interests of rightholders and consumers (Section III.3.4(a)(ii) of Opinion 06/2014); they do not comprise the processing of sensitive personal data related to sellers or data of sellers obtained from public sources (Section III.3.4(b)(ii) of Opinion 06/2014); sellers do not belong to a vulnerable segment of population (Section III.3.4(b)(v) of Opinion 06/2014).
  - Section 4.5.1.2 of this Chapter 1 ('Coexistence of the retention of sellers' personal data for a period of 5 years with the protection of personal data related to sellers') explains that the monitoring activities established by Article 9 of the Charter ('Offers of sale from regular sellers of products of categories identified as the most subject to counterfeiting') must fulfil the same criteria mentioned in the previous point, as laid down by the Article 29 WP in its Opinion 06/2014.

---

<sup>77</sup> Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. Section III.3.4 ('Key factors to be considered when applying the balancing test') ([http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf)).

Therefore, in light of the foregoing, the protection of personal data of sellers may not impact on the technical monitoring activities provided for by Article 3 of the Charter ('Measures to detect counterfeiting') and Article 9 of the Charter ('Offers of sale from regular sellers of products of categories identified as the most subject to counterfeiting') as even if platforms did not request sellers' consent it could be argued that the activities are performed to protect the legitimate interests of platforms.

#### 4.5.1.1.2. FORMAL REQUIREMENTS APPLICABLE TO AUTOMATED DATA PROCESSING ACTIVITIES

In addition, as a general rule, automated data processing activities are subject to authorisation from the French Data Protection Authority when they might exclude data subjects from the benefit of a right (Article 25.4 of the French Data Protection Law).

Therefore, it must be assessed whether or not the automated monitoring duties provided for by Article 3 of the Charter ('Measures to detect counterfeiting') and Article 9 of the Charter ('Offers of sale from regular sellers of products of categories identified as the most subject to counterfeiting') fall within the scope of the aforementioned formal requirement.

Guidance issued by the French Data Protection Authority contains the following explanation concerning Article 25.4 of the French Data Protection Law: 'it deals with 'blacklists': internal databases to fight against fraud, shared debtors databases in the areas of fixed or mobile telephony, bank credits, insurances, location of vehicles but also credit scoring'.<sup>78</sup> In addition, the Article 29 WP has defined blacklists as 'the collection and dissemination of specific information relating to a specific group of persons, which is compiled to specific criteria according to the kind of blacklist in question, which generally implies adverse and prejudicial effects for the individuals included thereon and which may discriminate against a group of people by barring them access to a specific service or harming their reputation'.<sup>79</sup>

Considering the doctrine of the French Data Protection Authority and Article 29 WP, platforms would need to obtain authorisation from the French Data Protection Authority to conduct the automated data processing activities following from their monitoring activities only if such activities would lead to:

- the creation of internal databases of sellers to fight illegal activities; and
- the exclusion of sellers from the benefit of a right.

On the one hand, Article 3 of the Charter ('Measures to detect counterfeiting') does not seem to meet the first criterion of the mentioned doctrine. Although it establishes the use of technical tools for detecting suspicious offers and sellers, it does not require the creation of any database of sellers. Thus, it may be argued that the technical monitoring activities set out in Article 3 of the Charter ('Measures to detect counterfeiting') are not subject to authorisation from the French Data Protection Authority.

On the other hand, the technical monitoring measures envisaged by Article 9 of the Charter ('Offers of sale from regular sellers of products of categories identified as the most subject to counterfeiting') do lead to the creation of databases of sellers likely to sell products most subject to counterfeiting, as platforms have to keep copies of documents proving the identity of these sellers, with the aim of fighting against online counterfeiting. However, the Charter does not directly impose any sanction or negative consequences on the sellers, so it may be difficult to argue that this Article would exclude sellers from the benefit of a right.

Therefore, in light of the foregoing, it may be argued that platforms would not need to obtain authorisation from the French Data Protection Authority in order to process automatically personal data related to sellers as provided for

---

<sup>78</sup> The Act of 6 August 2004 on the protection of natural persons regarding the processing of personal data: what changes have been introduced by the Act on IT and Freedoms of 6 January 1978? (*Loi du 6 Août 2004 relative à la Protection des Personnes Physiques à l'Égard des Traitements de Données à Caractère Personnel: quels changements dans la Loi 'Informatique et Libertés' du 6 Janvier 1978?*). (<http://www.cnil.fr/fileadmin/documents/approfondir/dossier/loi78-17/CNIL-dossier-nouvelleloi.pdf>).

<sup>79</sup> Article 29 WP 'Working Document on Blacklists' ([http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp65\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp65_en.pdf)).

by Article 3 of the Charter ('Measures to detect counterfeiting') and Article 9 of the Charter ('Offers of sale from regular sellers of products of categories identified as the most subject to counterfeiting').

#### *4.5.1.2. Coexistence of the retention of sellers' personal data for a period of 5 years with the protection of personal data related to sellers*

This Section analyses whether the protection of personal data related to sellers might have an impact on certain duties laid down in the Charter that imply the retention of personal data related to sellers for a period of 5 years after the closure of their accounts.

##### 4.5.1.2.1 GENERAL RULE APPLICABLE TO THE RETENTION OF PERSONAL DATA

As a general rule, Article 6 of the French Data Protection Law, which implements Article 6 of the Data Protection Directive, stipulates that data controllers may only retain individuals' personal data as long as such data is necessary for the purposes for which it was initially obtained. Such a requirement is also implicit from the right to the protection of personal data laid down in Article 8 of the Charter of Fundamental Rights ('Protection of personal data').

Applying the general rule of Article 6 of the French Data Protection Law to the Charter, it appears that platforms could only store and process personal data related to sellers as long as sellers' accounts are active, as such personal data is primarily collected for the purpose of managing the activity of sellers as registered users of platforms' websites.

Therefore, the data processing activities following from the duty to prevent the re-registration of certain sellers for 5 years after the closure of their accounts (Article 5 of the Charter ('Handling offers of sale of counterfeit goods and sellers of counterfeit products')) and from the duty to store documents providing evidence of the identity of sellers likely to sell products most subject to counterfeiting for a period of 5 years after the closure of their accounts (Article 9 of the Charter ('Offers of sale from regular sellers of products of categories identified as the most subject to counterfeiting')) are not consistent with the general rule laid down by Article 6 of the French Data Protection Law.

##### 4.5.1.2.2 EXCEPTION TO THE GENERAL RULE APPLICABLE TO THE RETENTION OF PERSONAL DATA

As explained in the previous Section, platforms are not allowed to process personal data related to sellers after the closure of the latter's accounts, in view of the general rule applicable to the retention of personal data. However, data protection regulations permit an exception to such a general rule when the data processing activities concerned aim to protect the legitimate interests of data controllers, provided the fundamental rights and freedoms of data subjects are respected (Article 7(f) <sup>80</sup> of the Data Protection Directive and Article 7.5° of the French Data Protection Law).

In relation to the Charter it is to be assessed whether the exception to the general rule applicable to the retention of personal data is applicable to the data processing activities set out in Article 5 of the Charter ('Handling offers of sale of counterfeit goods and sellers of counterfeit products') and Article 9 of the Charter ('Offers of sale from regular sellers of products of categories identified as the most subject to counterfeiting') that may imply the retention of personal data related to sellers after the closure of their accounts.

The Article 29 WP in its 'Opinion 06/2014 on the notion of legitimate Interests of the data controller under Article 7 of Directive 95/46/EC' <sup>81</sup> states that a balancing test between the legitimate interests of platforms on the one hand and the interests or fundamental rights of sellers on the other hand is required when applying Article 7(f) of the

---

<sup>80</sup> Regulation of the European Parliament and of the Council 2016/679, of 27<sup>th</sup> April, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, which will be applicable as from May 2018, also permits the processing of personal data without the consent of the data subject for the purposes of protecting the legitimate interests pursued by the controller or by a third party.

<sup>81</sup> Section III.3.4 ('Key factors to be considered when applying the balancing test') ([http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf)).

Data Protection Directive. In this context, the Article 29 WP provides examples of certain elements that may help to reinforce the data controller's legitimate interests:

- The data processing is necessary to preserve a fundamental right of the data controller, and the processing is necessary and proportionate in relation to the exercise of such a right (Section III.3.4(a)(i) of Opinion 06/2014 of the Article 29 WP).
- The data controller acts not only in its own legitimate interests (e.g., business), but also in the interests of a wider community (Section III.3.4(a)(ii) of Opinion 06/2014 of the Article 29 WP).
- The existence of some duly adopted non-binding guidance issued by authoritative bodies, for example regulatory agencies, encouraging data controllers to process data in pursuit of the interests concerned (Section III.3.4(a)(iv) of Opinion 06/2014 of the Article 29 WP).

In addition, the Article 29 WP provides examples of certain situations where the impact of data processing activities on data subjects may be reduced or increased depending on a combination, inter alia, of the following elements:

- The nature of the data, such as whether the processing involves data that may be considered sensitive or has been obtained from publicly available sources (Section III.3.4(b)(ii) of Opinion 06/2014 of the Article 29 WP).
- The way the data is processed, including whether the data is publicly disclosed or otherwise made accessible to a large number of persons, or whether large amounts of personal data are processed or combined with other data (Section III.3.4(b)(iii) of Opinion 06/2014 of the Article 29 WP).
- The reasonable expectations of data subjects, especially with regard to the use and disclosure of the data in the relevant context (e.g., status of the data controller, the nature of the service provided, applicable legal or contractual obligations) (Section III.3.4(b)(iv) of Opinion 06/2014 of the Article 29 WP).
- The status of the data controller and data subjects, including the balance of power between data subjects and the data controller, or whether data subjects are children or otherwise belong to a more vulnerable segment of population (Section III.3.4(b)(v) of Opinion 06/2014 of the Article 29 WP).

On top of that, the Article 29 WP also explains that having an appropriate legal ground does not relieve data controllers of their obligations under Article 6 of the Data Protection Directive with regard to, inter alia, necessity and proportionality (Section II.3 of Opinion 06/2014). For instance, even if the processing of personal data were based on the legitimate interests ground, this would not allow for any collection of data that was excessive in relation to the purpose specified.

Turning to the Charter, some of the criteria provided as examples by the Article 29 WP that may reinforce data controllers' legitimate interests may be fulfilled regarding the retention of personal data of certain sellers after the closure of their accounts. For example: platforms not only act in their own legitimate interest, but also in the interests of rightholders and consumers (Section III.3.4(a)(ii) of Opinion 06/2014); platforms' data processing activities do not comprise the processing of sensitive personal data related to sellers or data of sellers obtained from publicly available sources (Section III.3.4(b)(ii) of Opinion 06/2014); platforms do not need to publicly disclose the data or to combine it with other data (Section III.3.4(b)(iii) of Opinion 06/2014); and sellers do not belong to a vulnerable segment of population (Section III.3.4(b)(v) of Opinion 06/2014).

To complete the balancing test, it remains to be analysed whether the retention of the data for a period of five years can be considered proportionate in light of the objectives to be achieved. There is no case law in France that is directly applicable to the case analysed here but, by way of examples, the following French regulations may be taken into account regarding the length of period for retention of personal data for fighting infringements in the online environment:

- Article R. 10-13 of the French Code for post and electronic communications of 1952 (*'Code des Postes et des Communications Électroniques'*)<sup>82</sup> obliges operators of electronic communications to retain personal data allowing the research, assessment and prosecution of a criminal infringement or a breach of Article L. 336.3 of the French Intellectual Property Code<sup>83</sup> for a period of one year from its collection.
- Decree No 2011-219 of 25 February 2011 relating to the retention and communication of data enabling the identification of persons that have contributed to the creation of online content (*'Décret n°2011-219 du 25 février 2011 relatif à la Conservation et à la Communication des Données permettant d'Identifier toute Personne ayant Contribué à la Création d'un Contenu Mis en Ligne'*)<sup>84</sup> envisages the same data retention obligation as Article R. 10-13 of the French Code for post and electronic communications.

In light of the foregoing, it cannot be discounted that the five-year retention period provided for by Article 5 of the Charter ('Handling offers of sale of counterfeit goods and sellers of counterfeit products') and Article 9 of the Charter ('Offers of sale from regular sellers of products of categories identified as the most subject to counterfeiting') could be considered disproportionate as the regulations mentioned establish a retention period of one year.

Consequently, it can be argued regarding Article 5 of the Charter ('Handling offers of sale of counterfeit goods and sellers of counterfeit products') and Article 9 of the Charter ('Offers of sale from regular sellers of products of categories identified as the most subject to counterfeiting') that the protection of platforms' legitimate interests can be relied on as a legal ground for processing personal data related to sellers after the closure of their accounts. However, although there is no case law in France directly applicable to the VCP, the retention period of five years could be considered disproportionate taking into consideration the retention periods envisaged by other French regulations for fighting online infringements.

#### 4.5.2. Coexistence of the Charter with the right of sellers to an effective remedy and to a fair trial

This Section analyses whether sellers' right to an effective remedy and to a fair trial may have an impact on certain measures provided for by the Charter.

The right to an effective remedy and a fair trial is established by Article 47 of the Charter of Fundamental Rights ('Right to an effective remedy and to a fair trial') as well as by Article 9 of the Declaration of the Rights of Man and of the Citizen of 1789 ('Presumption of innocence and right of defence') (as referenced in the French Constitution) and by Article 6 of the European Convention on Human Rights of 4 November 1950 ('Right to a Fair Trial').

This right seeks to provide effective recourse to anyone who alleges that his or her rights have been violated. This right requires inter alia that:

- decisions be issued by impartial and independent bodies, through equitable processes and within reasonable timeframes;
- persons concerned be able to ascertain the reasons on which decisions are based, either by reading the decisions themselves or by requesting and obtaining disclosure of those reasons;
- decisions be taken on the basis of sufficiently solid facts, not mere general assertions;
- persons concerned be able to contest the grounds on which decisions are based and make submissions on evidence relating to the decisions, to ensure compliance with the adversarial principle.

<sup>82</sup> <http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070987>.

<sup>83</sup> 'The incumbent for providing services for accessing online publicly available communications has the duty to ensure that such access is not used for reproduction, representation, provision or public communication of works or objects protected by copyright or related rights without the permission of copyright holders [...]'.  
<sup>84</sup> <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023646013&categorieLien=id>.

As explained by the CJEU, for example in its Ruling issued on 22 December 2010 in Case C-279/09<sup>85</sup>, although Article 47 of the Charter of Fundamental Rights ('Right to an effective remedy and to a fair trial') uses the word 'person', the right to an effective remedy and a fair trial can also cover legal persons, which is what in many cases sellers could be.

In relation to the Charter, when an offer of a counterfeit product becomes available on a platform's website, the Charter directly envisages the application by platforms of the sanctions established by Article 5 of the Charter ('Handling offers of sale of counterfeit goods and sellers of counterfeit products'), which are in essence: removal of the offer, suspension of the account and closure of the account. The Charter does not specifically provide for the implementation of any safeguards towards sellers in cases where it requires the application of sanctions against them. The following would be examples of possible safeguards that could have been stipulated by the Charter:

- provision of a protocol to be followed by platforms before applying sanctions against sellers (e.g., asking sellers to physically provide them with the suspect product in order to verify whether or not it is counterfeit);
- provision of information by platforms to sellers in relation to the grounds on which they have decided to apply sanctions;
- provision of an opposition procedure for sellers allowing them to defend their position either before or after the application of sanctions against them;
- participation of an independent third party to verify the fairness of platforms' decisions;
- compensation to sellers for sanctions proven to be unjustified.

Therefore, if we contrast the content of the right to an effective remedy and a fair trial with the absence of safeguards under the Charter towards sellers, there is a risk that sellers could potentially argue that the Charter violates the right mentioned. That being said, based on the interviews conducted with platforms for the purposes of this Chapter 1, it seems that in practice platforms are applying at least certain safeguards towards sellers, for example, offering sellers the possibility of defending their position before the application of sanctions, which may lead to the minimisation of potential conflicts with the right to an effective remedy and a fair trial.

#### 4.5.3. Coexistence of the Charter with sellers' freedom to conduct a business

This Section analyses whether sellers' freedom to conduct a business may have an impact on certain measures provided for by the Charter.

The freedom to conduct a business is enshrined in Article 16 of the Charter of Fundamental Rights ('Freedom to conduct a business') and in Article 4 of the Declaration of the Rights of Man and of the Citizen of 1789 ('Freedom to conduct a business') (as referenced in the French Constitution).

This freedom includes, without limitation, the right for any business to be able to freely use within the limits of its liability for its own acts the economic, technical and financial resources available to it. It has been pointed out in the literature<sup>86</sup> that this freedom recognises the right to economic initiative, its main function being to foster social, economic and political integration and to protect consumers.

In relation to the Charter, sellers, as economic agents, enjoy the freedom to conduct a business granted by the Charter of Fundamental Rights and by the Declaration of the Rights of Man and of the Citizen of 1789, which give them the freedom to choose, inter alia, where to sell their products, how to sell them and what prices shall apply.

---

<sup>85</sup> <http://curia.europa.eu/juris/document/document.jsf?text=&docid=83452&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=131344>.

<sup>86</sup> Andrea Usai. 'The Freedom to Conduct a Business in the EU, Its Limitations and Its Role in the European Legal Order: A New Engine for Deeper and Stronger Economic, Social, and Political Integration' ([https://www.germanlawjournal.com/pdfs/Vol14-No9/14.9.10\\_Usai\\_Business%20Freedom.pdf](https://www.germanlawjournal.com/pdfs/Vol14-No9/14.9.10_Usai_Business%20Freedom.pdf)).



That being said, the prohibition of the re-registration of sellers for a period of five years in cases where platforms detect that sellers have submitted new offers of counterfeit products (Article 5 of the Charter ('Handling of offers of sale of counterfeit goods and sellers of counterfeit products')) may, to some extent, interfere with sellers' business activities (whether justified or not). In reality, banning sellers from using a platform's services for a period of five years would deprive sellers of the opportunity to sell goods (even genuine products) through a specific platform, which may lead to the following risks for their business:

- loss of sales opportunities;
- surplus stocks, which would lead to lower average selling prices.

These risks are also mentioned by the European Commission in relation to the dissuasive actions established by the MOU<sup>87</sup>.

Another fact that may generate similar risks for sellers' business is that rightholders and platforms consider low prices as one of the criteria for classifying a product offered for sale as counterfeit, which may result in the imposition of sanctions by platforms. This would lead to the automatic classification of products under a certain price as counterfeit. Although this is not expressly envisaged by the Charter, it follows from the requirement of Article 3 ('Measures to detect counterfeiting') to use technologically state-of-the-art tools to detect suspect offers or sellers and is widely applied in practice, as explained by the stakeholders interviewed.

As low prices may determine the classification of a product as counterfeit, in certain cases sellers may decide to fix concertedly higher selling prices to avoid the imposition of sanctions by platforms. In this sense, Article 101.1.a of the Treaty on the Functioning of the European Union<sup>88</sup> prohibits all agreements between undertakings, decisions by associations of undertakings and concerted practices that directly or indirectly fix purchase or selling prices or any other trading conditions<sup>89</sup>.

That being said, the risks mentioned may not generally be seen as endangering the existence of sellers' businesses. Indeed sellers would not necessarily be left out of the market as they would still be able to offer their products to the public, for example, via other platforms' websites or through other means offered by the e-commerce environment<sup>90</sup>.

Even if it were established that sellers' freedom to conduct a business would be affected, such freedom is already subject to limits and restrictions that have been recognised by the CJEU in various decisions since its ruling issued on 14 May 1974 in Case C-4/73, *Nold KG v Commission*<sup>91</sup>. Limits to the freedom to conduct a business are accepted provided that the two following conditions are satisfied:

- the restriction must protect the general interest proportionately; and
- the restriction must not hinder the substance of the right.

As to the first condition, the Charter's main aims are to safeguard rightholders' intellectual property rights and protect consumers from buying counterfeit goods online. In this sense, the CJEU has found that consumer protection and the protection of intellectual property rights may be construed as a general interest that would justify restrictions to the freedom to conduct a business (see CJEU rulings of 8 October 1986 in Case C-234/85, *Keller*<sup>92</sup>

<sup>87</sup> Section 3.4 ('Repeat Infringers') of the 'Report of the Commission to the European Parliament and the Council on the Functioning of the MOU' (<http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52013DC0209>).

<sup>88</sup> Treaty on the Functioning of the European Union, OJ C 326, 26/10/2012 p. 1-390.

<sup>89</sup> See also ruling issued on 4 June 2009 by the CJEU under Case C-8/08, *T-Mobile Netherlands* (paragraph 39) (<http://curia.europa.eu/juris/document/document.jsf?sessionid=9ea7d0f130d5c066df415b246629de7ac2c66904659.e34KaxiLc3eQc40LaxqMbN4ObN8Te0?text=&docid=74817&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=744088>) and ruling issued by the CJEU under joined Cases C-89/85, C-104/85, C-114/85, C-116/85, C-117/85 and C-125/85 to C-129/85, *Ahlström Osakeyhtiö and Others v Commission* (paragraph 63) (<http://curia.europa.eu/juris/liste.jsf?num=C-89/85&language=en>).

<sup>90</sup> In this regard, we have to bear in mind that only six Platforms are signatories of the Charter as indicated in Annexes 2 and 3 of this Chapter 1.

<sup>91</sup> <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:61973CJ0004>.

<sup>92</sup> <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:61985CJ0234>.



and 30 July 1996 in Case C-84/95, *Bosphorus v Minister for Transport, Energy and Communications and Others*<sup>93</sup>, respectively).

As to the second condition, the sanctions envisaged by the Charter are not likely to lead to the exclusion of sellers from the market and therefore would not hinder the substance of the freedom to conduct a business.

In light of the foregoing, the prohibition on the use of a platform's website for a period of five years may not be regarded as generally damaging the sellers' business. Even if this were to be the case, the CJEU accepts certain limitations to such a right that would be applicable in the case of the Charter.

#### 4.5.4. Coexistence of the Charter with the provisions of the E-Commerce Directive and the French E-Commerce Law and impact on Platforms' freedom to conduct their businesses

This Section analyses whether the Charter is in line with Article 15(1) of the E-Commerce Directive and whether platforms may benefit from the liability rules established by Article 14 of the E-Commerce Directive, as well as the potential consequences of these aspects for platforms' freedom to conduct business.

##### 4.5.4.1. Coexistence of the Charter with Article 15(1) of the E-Commerce Directive

Article 15(1) of the E-Commerce Directive, as implemented by Article 6 I-7° of the French E-Commerce Law, prohibits the imposition of any general monitoring requirement on information society intermediary service providers, or any general obligation to actively seek facts or circumstances indicating illegality.

Article 3 of the Charter ('Measures to detect counterfeiting') implies a general duty for platforms to monitor, and be able to detect immediately, certain categories of offers or sellers. Due to such monitoring activities, platforms may acquire knowledge or become aware of facts or circumstances that make the illegal nature of the goods proposed for sale apparent.

As the Charter puts the burden of monitoring sales activities on platforms, the monitoring activities established by Article 3 of the Charter ('Measures to detect counterfeiting') could be regarded as not in line with Article 15(1) of the E-Commerce Directive. That being said, the Charter is a non-binding instrument that leaves platforms freedom to implement voluntarily the corresponding measures for fighting against the online sale of counterfeit goods. Therefore, it may be argued that in practice the monitoring duties provided for by the Charter do not count as an imposition of a general monitoring obligation, as referred to by Article 15(1) of the E-Commerce Directive, but rather as a recommendation or best practice; consequently they cannot be regarded as not in line with the aforementioned Article of the Directive.

##### 4.5.4.2. Application to Platforms of the exemption of liability provided for by Article 14 of the E-Commerce Directive

Article 14 of the E-Commerce Directive, as implemented by Article 6 I-2° of the French E-Commerce Law, establishes that hosting service providers who store information supplied by and at the request of a recipient of the service are not liable if:

- they do not have actual knowledge of illegal activity or information as regards claims for damages, and are not aware of the facts or circumstances from which the illegal activity or information is apparent (Article 14(1)(a) of the E-Commerce Directive); or
- upon obtaining such knowledge or awareness, they act expeditiously to remove or disable access to the information (Article 14(1)(b) of the E-Commerce Directive).

As platforms are hosting service providers that store information supplied by and at the request of sellers, they may benefit from the exemption of liability provided for by Article 14 of the E-Commerce Directive on condition that they meet the requirements established by it.

---

<sup>93</sup> <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:61995CJ0084>.

As far as the first part of the path leading to exemption of liability is concerned (Article 14(1)(a) of the E-Commerce Directive), it may be argued that platforms could not benefit from it as the monitoring activities envisaged by Article 3 ('Measures to detect counterfeiting') could give them knowledge of illegality<sup>94</sup>.

As far as the second part of the path leading to exemption of liability is concerned (Article 14(1)(b) of the E-Commerce Directive), it will only apply to platforms to the extent that they proceed to remove or disable access to offers upon detection through their monitoring activities that the products proposed for sale are counterfeit goods. It would seem reasonable to assume that platforms will undertake to remove such offers as this is a requirement provided for by Article 5 of the Charter ('Handling of offers of sale of counterfeit goods and sellers of counterfeit products'), in which case the exemption of liability of Article 14(1)(b) of the E-Commerce Directive will apply to them.

#### *4.5.4.3. Consequences for platforms' freedom to conduct a business*

As already explained in Section 4.5.3 of this Chapter 1 ('Coexistence of the Charter with sellers' freedom to conduct a business'), the freedom to conduct a business established by Article 16 of the Charter of Fundamental Rights ('Freedom to conduct a business') and by Article 4 of the Declaration of the Rights of Man and of the Citizen of 1789 ('Freedom to conduct a business') (as referenced in the French Constitution) recognises the right to economic initiative.

Platforms, as economic agents, enjoy the freedom to conduct a business, meaning that they have freedom, inter alia, to choose how to conduct their business.

In relation to the Charter, Article 3 ('Measures to detect counterfeiting') establishes a general duty for platforms to monitor and to be able to detect immediately certain categories of offers or sellers.

In addition, according to Article 5 of the Charter ('Handling of offers of sale of counterfeit goods and sellers of counterfeit products'), platforms have to remove or disable access to offers upon detection through their monitoring activities that the products proposed for sale are counterfeit. Although this obligation is in line with Article 14 of the E-Commerce Directive, it may lead to a substantial increase in removal-related activities by platforms.

That being said, as already mentioned in Section 4.5.4.1 of this Chapter 1 ('Compatibility of the Charter with Article 15(1) of the E-Commerce Directive'), the Charter is a non-binding instrument that leaves platforms free to implement voluntarily the corresponding measures for fighting against the online sale of counterfeit goods. Thus, it may be argued that in practice the duties mentioned for the platforms may not be regarded as impinging on their freedom to conduct their business as they are to be understood as recommendations.

#### **4.5.5. Summary of findings relating to the coexistence of the Charter with the European Union and French legal frameworks and case law**

This Section summarises the findings made under Section 4 of this Chapter 1 ('Coexistence of the measures set out in the VCP with European Union and French legal frameworks and related case law') regarding the compatibility of the Charter with the European Union and French legal frameworks and case law.

##### *4.5.5.1. Coexistence of the Charter with fundamental rights*

The following conclusions have been reached concerning the coexistence of the Charter with certain fundamental rights:

- Right to the protection of personal data related to sellers

An analysis has been performed concerning the compatibility of the following data processing activities established by the Charter and a sellers' right to the protection of personal data related to them:

---

<sup>94</sup> See paragraph 122 of the *eBay* CJEU Ruling.

- **Automated monitoring activities required by the Charter.** The protection of personal data of sellers may not impact on the technical monitoring activities provided for by Article 3 of the Charter ('Measures to detect counterfeiting') and Article 9 of the Charter ('Offers of sale from regular sellers of products of categories identified as the most subject to counterfeiting') as ultimately it may be argued that they are performed by platforms to protect their legitimate interests. In addition, Article 25.4 of the French Data Protection Law establishes that automated data processing activities are subject to authorisation from the French Data Protection Authority when they may exclude data subjects from the benefit of a right. It is difficult to argue that the automated monitoring activities provided for by the aforementioned Articles of the Charter would exclude sellers from such a benefit; therefore, they would not be subject to authorisation from the French Data Protection Authority.
- **Retention of personal data of sellers for a period of five years.** As sellers' data is collected by platforms for the purpose of managing the activities of sellers' as registered users, the data processing activities following from Article 5 of the Charter ('Handling offers of sale of counterfeit goods and sellers of counterfeit products')) and Article 9 of the Charter ('Offers of sale from regular sellers of products of categories identified as the most subject to counterfeiting') applying for a period of five years after the closure of sellers' accounts may not be consistent with the general rule of Article 6 of the French Data Protection Law, which stipulates that data controllers may only retain personal data as long as it is necessary for the purposes for which the data was initially obtained. Despite the foregoing, as an exception to the general rule mentioned, it may still be argued that the protection of platforms' legitimate interests may be relied on as a legal ground for processing personal data related to sellers after the closure of their accounts. Although there is no case law in France directly applicable to the VCP, the retention period of five years could be considered disproportionate taking into consideration the retention period of one year envisaged by other French regulations for fighting online infringements.
- **Right of sellers to an effective remedy and to a fair trial**  
Given that the Charter does not specifically provide for the implementation of any safeguards for sellers where it requires the application of sanctions against them, there is a risk that sellers could potentially argue that the Charter violates their right to an effective remedy and to a fair trial, provided for by Article 47 of the Charter of Fundamental Rights ('Right to an effective remedy and to a fair trial'), Article 9 of the Declaration of the Rights of Man and of the Citizen of 1789 ('Presumption of innocence and right of defense') (as referenced in the French Constitution) and Article 6 of the European Convention on Human Rights of 4 November 1950 ('Right to a Fair Trial'). However, in practice platforms provide certain safeguards for sellers, for example, offering them the possibility of defending their position before the application of sanctions, which may minimise potential conflicts with the fundamental right mentioned.
- **Right of sellers and platforms to conduct a business**  
Platforms and sellers, as economic agents, benefit from the freedom to conduct a business enshrined in Article 16 of the Charter of Fundamental Rights ('Freedom to conduct a business') and in Article 4 of the Declaration of the Rights of Man and of the Citizen of 1789 ('Freedom to conduct a business') (as referenced in the French Constitution). Even if certain duties of the Charter relating to platforms and sellers might imply certain risks for their businesses, they would not generally be seen as endangering the existence of the sellers' and platforms' businesses as they would not necessarily leave such players out of the market. In addition, concerning the duties imposed on platforms, given that the Charter leaves them free to implement voluntarily the duties and procedures envisaged thereby, it may be argued that, in practice, the duties mentioned may not be regarded as impinging on platforms' freedom to conduct their business.

#### 4.5.5.2. *Coexistence of the Charter with the E-Commerce Directive and the French E-Commerce Law*

On the one hand, as far as the compatibility of the Charter with Article 15(1) of the E-Commerce Directive and Articles 6 I-2° and 6 I-7° of the French E-Commerce Law is concerned, given that the Charter is a non-binding

instrument, it may be argued that, in practice, the monitoring duties provided for by Article 3 of the Charter ('Measures to detect counterfeiting') do not count as the imposition of a general monitoring requirement; therefore, this Article may not be regarded as not in line with the aforementioned Articles of the E-Commerce Directive and the French E-Commerce Law.

On the other hand, concerning platforms' exemption of liability for sellers' offers of counterfeit products, although platforms' monitoring activities would give them knowledge of illegality, which prevents application of the first part of the path leading to exemption of liability (Article 14(1)(a) of the E-Commerce Directive), they could benefit from the second part of the path to the aforementioned exemption (Article 14(1)(b) of the E-Commerce Directive) if they proceed to remove or disable access to offers upon detection through their monitoring activities that the products proposed for sale are counterfeit. The removal by platforms of offers of counterfeit goods is in fact established by Article 5 of the Charter ('Handling of offers of sale of counterfeit goods and sellers of counterfeit products').

## 5. Technologies

Whereas rightholders do not have to use technical tools to comply with the duties and measures laid down in the Charter, platforms do benefit from their use.

One of the duties of platforms envisaged in the Charter is to detect, as soon as possible, online offers of counterfeit products and sellers likely to sell counterfeit goods, and to activate the measures analysed already, such as requesting proof of the authenticity of the products or withdrawing offers of counterfeit goods. As explained under Section 3 ('Duties and Procedures') of this Chapter 1, compliance with this obligation necessitates, as a fundamental basis, a certain degree of technological development. To that end, platforms interviewed have developed specific software that, inter alia, analyses key words (e.g., 'fake'; 'counterfeit') in the offers published on their websites.

Furthermore, platforms are compelled to implement electronic notification procedures, which implies the development of additional technological measures. As mentioned in Section 3.3.3. of this Chapter 1 ('Notification mechanisms to be made available to rightholders and consumers'), these notification procedures have to be available not only to rightholders, but also to consumers that want to submit a complaint if they have been the victims of counterfeiters.

Although each platform has developed its own technological measures to comply with the obligations mentioned (because there are no standardised technical tools), most of the methods used are similar. The 2 platforms interviewed were already developing and making use of technical tools to fight counterfeiting even before having signed the Charter and are now, with rightholders' assistance and training, improving them.

## 6. Costs

The signatories to the Charter do not have to pay any membership fees. Nor does the INPI charge any administration fees for its supervisory role and support during the joining procedure.

However, expenses may arise for active signatories to the Charter as a consequence of complying with the duties and measures laid down by the VCP.

The main costs that both rightholders and platforms have to assume arise from the need to hire at least one in-house correspondent, who will be responsible for dealing with matters related to the Charter. Such a person's tasks are, inter alia, collaborating with other signatories' correspondents and, in the case of platforms' correspondents, reviewing and updating platforms' procedures, checking offers before they are published, and submitting or receiving notices and take downs.

One of the platforms interviewed, for example, has 30 people working for it (either full-time or part-time) on counterfeiting issues in different departments (e.g., IT department) in order to implement new technical measures or update existing ones. Similarly, 2 of the rightholders interviewed have their own departments dedicated to the fight against counterfeit goods. However, these departments/areas were not created just to comply with the Charter but in general to fight against counterfeiting.

Both categories of signatories see these costs and expenses as an investment that contributes to the good reputation of their businesses.

## 7. Education

To reach the desirable level of consumer participation in the VCP, awareness raising is necessary. For instance, awareness raising serves to achieve the following two main objectives:

- to inform consumers about what counterfeiting is, what risks it poses and how to recognise counterfeit products;
- to inform consumers about all mechanisms and tools available for denouncing the sale of counterfeit goods on the internet.

One signatory federation of rightholders interviewed stated that it had created a 'Museum of Counterfeiting'<sup>95</sup>. The museum has a didactic function, allowing visitors to learn about counterfeiting and its impact on the economy. It shows a large range of fake and authentic products so that visitors can learn how to spot the differences between the two. Most of the fake products shown in the museum are provided by platforms, which received them from users of their services. In addition, the museum has a dedicated website<sup>96</sup> for making consumers aware of the importance of intellectual property rights and informing them of the risks of and legal sanctions imposed breaches of those rights.

The other signatories interviewed have stated that they are not undertaking any educational activities at the moment regarding the Charter. Neither the INPI nor the CNAC has a website that specifically outlines the background and purpose of the Charter.

Some signatories interviewed believe that the Charter is barely known to consumers or even platforms, as no relevant public awareness campaigns are being undertaken. As explained, in practice, signatory rightholders that want to fight against the online sale of counterfeit versions of their brand sometimes do contact platforms that they detect selling those products and introduce them to the Charter.

In general, very few press releases mention the Charter and those that do are old. Therefore, consumers are not always aware of the Charter's existence<sup>97</sup>. In addition, the majority of those press releases were published in specialist media relating to counterfeiting and not in general national media. In this regard, some signatories have confirmed that, in their opinion, consumer habits have not changed since the implementation of the Charter.

---

<sup>95</sup> Located in Montreuil, France.

<sup>96</sup> [www.musee-contrefacon.com](http://www.musee-contrefacon.com).

<sup>97</sup> Some examples of online press releases are:

<sup>(1)</sup> Portail du Gouvernement Français, *Signature d' une charte pour lutter contre la contrefaçon sur internet*(2009) [http://archives.gouvernement.fr/fillon\\_version2/gouvernement/signature-d-une-charte-pour-lutter-contre-la-contrefacon-sur-internet.html](http://archives.gouvernement.fr/fillon_version2/gouvernement/signature-d-une-charte-pour-lutter-contre-la-contrefacon-sur-internet.html).

<sup>(2)</sup> Katie Bird 'Fight against the online sale of counterfeits continues in France' (2010) <http://www.cosmeticsdesign-europe.com/Market-Trends/Fight-against-online-sale-of-counterfeits-continues-in-France>.

<sup>(3)</sup> Marc Rees *Marques et plateformes signent une charte anti-contrefaçon sans eBay ni Amazon* (2009) <http://www.nextinpact.com/archive/54575-lutte-contrefacon-charte-ebay-priceminister.htm>.



## 8. Effectiveness

An assessment<sup>98</sup> of the application of the Charter was made under the authority of the INPI, 18 months after its signature in December 2009.

In November 2012, during the General Assembly of the signatories to the Charter that took place to evaluate the VCP's testing process (see Article 15 of the Charter ('Evaluation of the testing process')), the French Industry Minister underlined the efficiency of the cooperation established by the Charter between economic operators and announced the final implementation of the Charter. During this General Assembly, the signatories considered that the Charter had accomplished one of its main objectives: the establishment of a direct and solid dialogue between platforms and rightholders. In addition, signatories pointed out that no litigation case between the parties had taken place since the implementation of the Charter.

The assessment, a copy of which has been provided by the INPI for the purposes of this Chapter 1, states that 'at the end of the experimentation process the signatories unanimously believe that the objectives of the Charter have been broadly achieved', as the counterfeiting rate observed on the signatory platforms has reached minimum levels.

In this regard, as underlined by the assessment, since its implementation the Charter has established:

- the development or strengthening of the relationship of mutual trust between platforms and rightholders;
- the regular transmission of information relating to online anti-counterfeiting by rightholders to platforms to implement appropriate proactive and preventive measures for detection;
- the simplification of notifications by rightholders to platforms on counterfeit offers;
- the training to be provided to platforms by rightholders about their specific products;
- the regular and reciprocal exchange of information in relation to the fight against counterfeiting;
- measures that benefit consumers in their purchasing acts on the internet.

The assessment also lists some proposals made by the signatories to the Charter to enhance the VCP, namely:

- communication by the competent Ministry to the self-employed;
- visible and regular communication by the authority [the INPI] responsible for proper operation of the Charter, to expand cooperation between professionals and other signatories;
- a national consumer awareness campaign on the dangers of internet counterfeiting, which could be launched by the CNAC in connection with the signatories to the Charter.

For instance, the assessment states that two of the platforms that signed the Charter in December 2009 (i.e., PriceMinister and 2xmoinscher) found that, during the testing period, the selling of counterfeit goods through their websites had decreased.

According to the Platform PriceMinister, the year 2012 was marked by a significant decline in accounts suspended due to counterfeit sales (down to 1 500 in 2010 from around 2 600 in 2009 and 2008). In over 99% of cases, goods detected were not sold on PriceMinister, and 12 000 product pages for counterfeit products created by sellers were removed in 2011.

In addition, 2xmoinscher provided the following statistics related to the number of counterfeit items returned by buyers, which they say is explained by the improved detection of counterfeits before the sale takes place:

---

<sup>98</sup> *Charte de lutte contre la contrefaçon sur Internet. Evaluation du processus d'expérimentation. Bilan d'application.*

- 101 returns on orders placed in 2010;
- 166 returns on orders placed in 2009;
- 218 returns on orders placed in 2008.

More recently, according to PriceMinister's latest publicly available report relating to its fight against online counterfeiting, in 2014 this platform blocked the selling of nearly 98% of counterfeit goods even before the relevant offers were published on their website, thanks to close collaboration with rightholders and the implementation of dissuasive measures and detection tools. For this platform, it is becoming increasingly difficult to discern counterfeits of small accessories both because they look very similar to original articles and because of the general improvement in the quality of counterfeits.

Another of the interviewed signatory platforms considers the measures implemented to fight against online counterfeiting efficient because it hardly ever gets notices from rightholders, as in most cases the offers are withdrawn before rightholders become aware of them.

One of the platforms interviewed is of the opinion that public bodies should be more involved in the VCP and should increase their supervisory activities.

According to one of the rightholders interviewed, the sale of counterfeit goods has dropped to approximately 1% or even less on each platform since they actively collaborate with platforms. In fact, the rightholders interviewed barely take action in this regard as platforms detect their counterfeit goods even before rightholders do.

As mentioned in previous Sections of this Chapter 1, in 2012, after implementation of the Charter, two more charters were signed in France between rightholders and (i) small ads platforms and (ii) postal operators<sup>99</sup>. In relation to this and regarding the feedback from the INPI and the CNAC, both the latter are now looking into extending the scope of these types of VCPs by including other categories of intermediaries, such as advertising service providers, payment services and shippers.

---

<sup>99</sup> See footnotes 58 and 59 of this Chapter 1.

## Chapter 1: Annex 1

### Charter for the Fight Against the Sale of Counterfeit Goods on the Internet between Intellectual Property Rightholders and e-Commerce Platforms

#### Foreword

1. Counterfeiting is a real scourge on today's society. It can fool consumers and threaten their health and safety, especially when counterfeit products do not respect applicable standards or contain toxic substances. By encouraging an underground economy, it constitutes unfair competition for companies and destroys jobs.
2. Counterfeiting is growing via new distribution channels offered by the Internet. Counterfeiters are exploiting services provided by e-commerce platforms to try to distribute illicit merchandise. By doing this, they are harming the image of these platforms and reducing consumer confidence in online commerce, thereby holding back its growth.
3. In order to curb these practices, to protect consumers who are endangered or fooled by counterfeit goods and to encourage growth in online business, e-commerce platforms and the holders of industrial property rights signing this Charter have decided to work together under the auspices of national authorities.
4. The signatory platforms and rightholders shall work together to implement concrete means that ensure a tangible and effective response to the sale of counterfeit goods on ecommerce websites, i.e., fake products that are manufactured or reproduced without the permission of the rightholders concerned.
5. The signatory platforms and rightholders consider that it is possible to use measures and the exchange of information to deploy firm anti-counterfeiting measures. The parties are conscious that these measures must be implemented and jointly tested in order to examine their pertinence and regularly modified in order to be effective against counterfeiting. The parties therefore agree to test the arrangements stipulated by this Charter for a period of eighteen months. After this testing period, the arrangements will be subject to a global evaluation in order to determine the conditions of their deployment on a more durable basis, ensuring that they are continuously adapted and improved.
6. Whatever legislation governs their activities, the signatory platforms and rightholders are free to commit themselves to implementing the practical measures defined in this Charter. Signing this Charter and implementing the mechanisms stipulated within shall not prejudice the legal status of the signatories nor their current or future liability regime; these actions shall have no consequences on current or future legal proceedings. The objective of this Charter is neither to deal with matters relating to selective retailing of authentic products nor to fight against 'para-commercialisme' and define the threshold of sales beyond which the sellers on platform websites should be considered as acting as professionals.

## Chapter I: Anti-counterfeiting measures

### *Article 1 – Providing information to sellers and ensuring consumer awareness*

The platforms shall inform sellers of products within the categories most subject to counterfeiting of their obligation to guarantee the authenticity of the products they propose for sale and/or use and the sanctions they risk under penal law and under the general terms and conditions of sale and/or use of the platform in the event they sell counterfeit goods. Sellers will be informed of this through messages transmitted automatically when the advertisements in question are submitted to the platform.

The rightholders and platforms shall cooperate to inform consumers about the risks of counterfeiting, especially via the Internet.

### *Article 2 – Offers of sale concerning medicines*

The sale of medicines is restricted to pharmacists, the only professionals certified to provide the necessary advice to ensure the health and protection of consumers. The platforms and rightholders acknowledge that the sale of medicines shall not be possible via their ecommerce websites and exclude the existence of a resale market of such products.

The platforms undertake to implement state-of-the-art measures to detect offers of sale concerning medicines and to prevent their publication online.

If despite the deployment of these measures, such an offer of sale is only detected after its publication online, the platforms undertake to withdraw it immediately and to take all necessary measures to prevent its later re-publication online.

In all events, the platforms will immediately suspend, upon the occurrence of the first such offer, all accounts identified as belonging to the seller in question, including those opened under different usernames, for a period of six months. In the event another offer is detected, they shall close all this user's accounts and shall deploy all measures at their disposal to prevent the re-registration of the seller for a period of five years.

### *Article 3 – Measures to detect counterfeiting*

The platforms and rightholders are conscious of the fact that counterfeit products may be offered for sale in several different forms on the websites belonging to the platforms. Certain offers of sale of counterfeit products can be detected by the intrinsic analysis of their content, while others can be identified by examining the general behaviour of the seller and all information concerning said seller. In both cases, measures can be implemented to automatically analyse all pertinent information.

The platforms and rightholders agree to test the use of state-of-the-art measures for a period of eighteen months, in order to:

- a) detect offers of sale of counterfeit products or offers that use well-known trade marks for keyword spamming (advertising a well-known trade mark with no relation to the product for sale), by the content of advertisements and before they are published online;
- b) detect sellers of counterfeit products based on their behaviour.

The rightholders and platforms will cooperate in deploying the testing process.

### *Article 4 – Notification procedures for rightholders*

The notification procedures by which the rightholders will indicate to the platforms which offers of sale concern counterfeit products or which sellers are offering counterfeit products for sale, are one of the measures used to prevent the sale of counterfeit products on the websites concerned.

The platforms undertake to set up effective and efficient notification procedures that are easily accessible by electronic means. These procedures shall be simple, understandable and limited to the information required to clearly identify the declaring party and the offers of sale or sellers concerned.

The rightholders shall use the notification procedures provided by the platforms to identify the offers of sale of counterfeit goods or the sellers of such products. The rightholders shall comply with these procedures in good faith and will ensure the procedures are applied efficiently. The platforms shall inform the rightholders of the outcome of their notifications.

The platforms and rightholders shall cooperate in order to enable the extensive and continuous use of the notification procedures, also to ensure their efficiency and responsiveness to new methods. The right holders may indicate in their notifications why they consider that the notified goods are counterfeit products, and the platforms may use those informations to develop and implement the detection measures outlined in the previous article.

#### *Article 5 – Handling offers of sale of counterfeit goods and sellers of counterfeit products*

The platforms undertake to refrain from publishing online offers of sale concerning counterfeit products that have been detected by the measures outlined in Article 3 a). If despite the use of these measures, such an offer of sale is only detected after its publication online, at the initiative of the platform or subsequent to notification by the rightholder concerned by application of Article 4, the platforms agree to withdraw the offer of sale immediately and to take all necessary measures to prevent its re-publication at a later time. In all events, the platforms will immediately suspend, upon the occurrence of the first such offer, all accounts identified as belonging to the seller in question, including those opened with different usernames, for a period of six months. In the event another such offer is detected, they shall close all this user's accounts and shall deploy all measures at their disposal to prevent the re-registration of the seller for a period of five years.

In the event of detection of a seller likely to sell counterfeit goods, at the initiative of the platform by application of Article 3 b) or subsequent to notification by the rightholder concerned by application of Article 4, the platforms undertake to demand justification of the authenticity of the product(s) proposed for sale and to suspend the seller's account pending the delivery of such justification. If the seller cannot provide suitable documentation proving the authenticity of the product(s), the platforms agree to close all the seller's accounts, including those opened under different usernames and to deploy all measures at their disposal to prevent the re-registration of the seller for a period of five years.

To prevent the circumvention of these measures, the platforms shall deploy all measures at their disposal to identify all accounts opened by the sellers in question and which they may open subsequently using other usernames.

#### *Article 6 – Handling offers of sale of goods imported into the European Economic Area*

The platforms and rightholders shall be especially vigilant concerning products proposed to consumers in France from outside of the borders of the European Economic Area or proposed by sellers based outside this territory. In the absence of the international exhaustion of intellectual property rights, such importations of products bearing trade marks protected in France are subject to the authorisation of the rightholder concerned.

The platforms undertake to deploy appropriate measures that enable the verification of the localisation of the products proposed to consumers in France or the location of the sellers offering such products.

If the sellers are based outside the European Economic Area or if they propose products localised outside this area, the platforms shall request that the sellers provide documentation proving that they have received the appropriate authorisation from the rightholder concerned.

Rightholders who identify unauthorised sellers located outside the European Economic Area or proposing products localised outside this area via websites owned by the platforms shall use the procedures outlined in Article 4 to notify the platforms about these sellers and to expressly indicate that the sellers do not have the appropriate authorisation.

If a seller cannot produce documentation to justify he has the authorisation of the rightholder or in the event the rightholder issues a notification, the platforms will withdraw the offer of sale concerned and, in the event another such offer is detected on the account of the same seller, will close the account.

#### *Article 7 – Handling offers of sale of products in the categories most subject to counterfeiting*

For the categories of products identified as the most subject to counterfeiting, the platforms undertake to prohibit bid periods for a duration of less than 10 days.

#### *Article 8 – Consumer complaints*

The platforms agree to receive complaints from consumers who are victims of offers of sale of counterfeit products. To this end, they shall set up an easily accessible and visible section on their websites where consumers can notify them of counterfeit products or sellers of counterfeit goods.

The platforms shall transmit all complaints collected to the rightholders concerned, when counterfeit products require special expertise, receive their comments on the content of the complaints and if the complaint has suitable grounds based on the general terms and conditions of sale and/or use of the platform, shall apply the sanctions defined in Article 5.

#### *Article 9 – Offers of sale from regular sellers of products of categories identified as the most subject to counterfeiting*

The platforms and rightholders shall agree to consider as a regular seller of products of categories identified as the most subject to counterfeiting under the terms of this charter, any person fulfilling suitable criteria based on the number of articles offered for sale, sales volumes and values, as well as the period of completion of these operations, in those categories. The parties will define such criteria jointly.

The platforms agree to identify the individuals, whether based in France or selling products on the French market, whether using one or several accounts, who correspond to these criteria. The platforms will request that these persons provide proof of identity and address on pain of suspension of their account(s) (for French sellers, this includes the 'Kbis' declaration or their identity card, SIREN/SIRET number, French bank account number, etc.) and the platforms shall verify the documents provided.

The platforms shall retain this identity and address information and the corresponding justifying documentation for the duration of operation of the account(s) concerned and for a period of five years after the closure of the account(s) concerned.

The platforms shall clearly indicate the conditions and methods of collection of this information in their general terms and conditions of sale and/or use.

### **Chapter 2: Exchange of information between platforms and rightholders in the fight against counterfeiting**

#### *Article 10 – Correspondents and contact methods dedicated to anti-counterfeiting*

To facilitate the exchange of information and cooperation between the parties, the platforms and rightholders shall designate one or more correspondents within their respective organisations, who shall be responsible for all matters concerning the implementation of this Charter. The parties shall exchange the contact details of their respective correspondents.

To inform consumers, the parties shall set up dedicated anti-counterfeiting contact points by all appropriate telecommunication methods (phone, fax, e-mail, etc.). The list of dedicated contacts shall be published in an easily-accessible section on the websites owned by the platforms.

### *Article 11: Information concerning offers of sale and sellers*

The platforms have information enabling the detection of offers of sale of counterfeit products and of sellers likely to sell counterfeit products (seller identification information, IP address, sales history, financial information, etc.).

The rightholders possess information that may contribute to the efficiency of the anti-counterfeiting measures stipulated by this Charter. They know their products well and can distinguish them from counterfeit products. They may have put in place measures to this end or developed expertise that would identify offers of sale of counterfeit goods or the profiles of sellers likely to sell such products.

The rightholders undertake to transmit to the platforms all elements in their possession that may contribute to identifying offers of sale of counterfeit products or seller profiles likely to sell such products. On the basis of these elements, the platforms agree to train their personnel involved in the implementation of this Charter.

### *Article 12: Development, adaptation and update of detection tools*

To ensure efficient operations, the development, adaptation and update of the detection measures stipulated by this Charter require the periodical exchange of information between the platforms and the rightholders.

The detection criteria must be specifically adapted to each category of products concerned and according to the diversity of the sectors affected by counterfeiting activities. The platforms and rightholders agree to organise bilateral or multilateral meetings to exchange the information required for the definition and adaptation of these specific criteria. The platforms and rightholders undertake to supply each other with a list of criteria that they have identified as pertinent.

These meetings shall be held as often as needed and at least once a year.

### *Article 13: Confidentiality*

All the information transmitted between platforms and rightholders under application of this Charter is confidential, except that appearing in the assessment of its application indicated in Article 15 below.

The platforms and rightholders undertake to respect and ensure the respect of the strictest confidentiality of this information and to take all necessary measures to preserve this confidentiality, in particular concerning their personnel and co-contractors.

## Chapter 3: Conducting the testing process

### *Article 14: Implementation of the testing process*

The measures stipulated in Articles 2, 3, 4, 5, 6 and 9 will be put into action no later than six months after the signature of this Charter.

At this time, an authority appointed by the minister(s) responsible for industry and consumption will assess whether the parties have indeed taken the measures necessary to implement the testing process.

### *Article 15: Evaluation of the testing process*

The platforms and rightholders agree to hold a general assembly under the chairmanship of the authority appointed by the minister(s) for industry and consumption, eighteen months after the signature of this Charter, in order to:

- exchange information about evolutions in counterfeit practices observed on the websites owned by the platforms;
- jointly update the list of categories of products identified as the most subject to counterfeiting;
- draw up an assessment of the application of this Charter; this assessment shall indicate the results obtained via the testing process, the correct operation of the cooperation mechanisms and the mutual respect of obligations as stipulated by this Charter. The assessment shall be provided to the minister(s) responsible for industry and consumption.



### *Article 16: Durable deployment of the Charter*

After the testing period, the parties may agree to extend the deployment of the provisions of this Charter.

As part of the durable implementation of the provisions of this Charter, the parties respecting their obligations may indicate on their website and in any of their corporate communications, whatever the medium, that they are a signatory to this Charter.

At any moment, all parties may request the intervention of the authority appointed by the minister(s) for industry and consumption in the event another party does not respect their obligations. The authority shall decide to convoke all signatories to this Charter to a General Assembly held under its supervision, in order to discuss any such non-respect of obligations. If the non-respect is indeed confirmed, it is made public and the defaulting party may no longer promote its quality of signatory to this Charter.

This Charter will be subject to annual assessments concerning its application, transmitted to the minister(s) for industry and consumption, also to periodical evaluations in order to envisage modifications that are obligatory or possible to ensure greater efficiency. If in the course of these assessments, it is observed that a party no longer respects its obligations, it will cease to promote its quality of signatory to this Charter.

### *Article 17: Membership and renunciation of the Charter*

After its signature, the Charter shall remain open to new platform or rightholder members.

The signatory platforms and rightholders shall have the right to renounce their membership of this Charter, by registered letter addressed to the authority appointed by the minister(s) for industry and consumption and to the other signatory parties. The renouncement shall only take effect for the future and shall only involve the renouncing party, which shall nonetheless remain bound by the obligations of confidentiality stipulated in Article 13 of this Charter.

## Chapter 1: Annex 2

### Signatories that joined the Charter in December 2009

- Professional federations
  - Comité Colbert
  - Fédération des Entreprises de la Beauté (FEBEA)
  - Fédération Française des Industries Jouet Puériculture (FJP)
  - Fédération Française des Industries du Sport et des Loisirs (FIFAS)
  - Istituto di Centromarca per la Lotta alla Contraffazione (INDICAM)
  - Les Entreprises du Médicament (LEEM)
  - Union des Fabricants (UNIFAB)
- Rightholders:
  - Berluti
  - Burberry
  - Celine
  - Chanel
  - Christian Dior Couture
  - Emilio Pucci International
  - Givenchy
  - Gsk
  - Kenzo
  - Lacoste
  - Les Laboratoires Servier
  - Lilly France
  - L'Oréal
  - Loewe
  - Louis Vuitton Malletier
  - LVMH Moët Hennessy Louis Vuitton
  - Marc Jacobs International
  - Microsoft France
  - MSD
  - Nike Europe
  - Novartis
  - Pierre Fabre Médicament
  - Pierre Fabre Dermo-Cosmétique
  - Pfizer
  - PPR
  - Roche
  - Sanofi Aventis
  - The Millennium Essence Company (Parfums Corolle, Kaloo Parfums, Parfums Clayeux)
  - Würzburg Holding Sa (Marithe+Francois Girbaud)
- Platforms:
  - PriceMinister

- Trokers SA (2xmoinscher.Com)

## Chapter 1: Annex 3

### Signatories that joined the Charter in February 2012

- Professional federations:
  - Asociación Nacional para la Defensa de la Marca (ANDEMA)
- Rightholders:
  - Adidas France
  - Adobe System France
  - Groupe Clarins (Clarins, Clarins Fragrances Group, Thierry Mugler)
  - Fondation Alberto et Annette Giacometti
  - Longchamp
  - Procter & Gamble France
- Platforms:
  - Instantluxe.com
  - Ugotawish.com
  - Videdressing.com
  - Vestiairedecopines.com
  - Leboncoin.fr

## Chapter 1: Annex 4

### European Union legal framework

#### Charter of Fundamental Rights of the European Union

- Article 8: Protection of personal data.
  - '1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority'.
- Article 16: Freedom to conduct a business.
  - 'The freedom to conduct a business in accordance with Union law and national laws and practices is recognised.'
- Article 17: Right to property.
  - '2. Intellectual Property shall be protected'.
- Article 47: Right to an effective remedy and to a fair trial.
  - '1. Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article. ... Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented.'

#### European Union Directives

- Article 14 of the E-Commerce Directive.
  - '1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that: (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information. 2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider. 3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.'
- Article 15(1) of the E-Commerce Directive.
  - 'Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.'

- Article 3 of the Enforcement Directive.
  - '1. Member States shall provide for the measures, procedures and remedies necessary to ensure the enforcement of the intellectual property rights covered by this Directive. Those measures, procedures and remedies shall be fair and equitable and shall not be unnecessarily complicated or costly, or entail unreasonable time-limits or unwarranted delays. 2. Those measures, procedures and remedies shall also be effective, proportionate and dissuasive and shall be applied in such a manner as to avoid the creation of barriers to legitimate trade and to provide for safeguards against their abuse.'
- Article 6(1)(e) of the Data Protection Directive.
  - '1. Member States shall provide that personal data must be (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.'
- Article 7 of the Data Protection Directive.
  - 'Member States shall provide that personal data may be processed only if: (a) the data subject has unambiguously given his consent; or (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or (d) processing is necessary in order to protect the vital interests of the data subject; or (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1).'

## Chapter 1: Annex 5

### CJEU Case Law

EBAY CJEU RULING (12 JULY 2011)	
Parties	<ul style="list-style-type: none"> <li>▪ L'Oréal SA</li> <li>▪ Lancôme parfums et beauté &amp; Cie SNC</li> <li>▪ Laboratoire Garnier &amp; Cie</li> <li>▪ L'Oréal (UK) Ltd</li> </ul> <p>(hereinafter, jointly referred as 'L'ORÉAL')</p> <p>AND</p> <ul style="list-style-type: none"> <li>▪ eBay International AG</li> <li>▪ eBay Europe SARL</li> <li>▪ eBay (UK) Ltd</li> <li>▪ Stephen Potts</li> <li>▪ Tracy Ratchford</li> <li>▪ Marie Ormsby</li> <li>▪ James Clarke</li> <li>▪ Joanna Clarke</li> <li>▪ Glen Fox</li> <li>▪ Rukhsana Bi</li> </ul> <p>(hereinafter, jointly referred as 'eBay')</p>
Facts	<ul style="list-style-type: none"> <li>▪ L'ORÉAL is a manufacturer and supplier of perfumes, cosmetics and haircare products. In the United Kingdom it is the proprietor of a number of national trade marks. It is also the proprietor of Community trade marks. L'ORÉAL operates a closed selective distribution network, in which authorised distributors are restrained from supplying products to other distributors.</li> <li>▪ eBay operates an electronic marketplace on which are displayed listings of goods offered for sale by persons who have registered for that purpose with eBay and have created a seller's account with it. eBay charges a percentage fee on completed transactions. Sellers and buyers must accept eBay's online-market user agreement. One of the terms of that agreement is a prohibition on selling counterfeit items and on infringing trade marks.</li> <li>▪ In May 2007, L'ORÉAL sent eBay a letter expressing its concerns about the widespread incidence of transactions infringing its intellectual property rights on eBay's European websites. L'ORÉAL was not satisfied with the response it received and brought actions against eBay before the High Court of Justice (England &amp; Wales).</li> <li>▪ The High Court of Justice took the view that eBay could do more to reduce the number of sales on its online marketplace that infringe intellectual property rights. According to the High Court of Justice, eBay could use additional filters. It could also include in its rules a prohibition on selling, without the consent of the</li> </ul>



EBAY CJEU RULING (12 JULY 2011)	
	rightholders, trade-marked goods originating from outside the EEA. It could also impose additional restrictions on the volumes of products that can be listed at any one time and apply sanctions more rigorously.
Preliminary Ruling	<p>Under the circumstances, the High Court of Justice decided to refer inter alia the following question to the CJEU for a preliminary ruling:</p> <ul style="list-style-type: none"> <li>Whether the service provided by operators of online marketplaces was covered by the E-Commerce Directive and, if so, under what circumstances it might be concluded that such operators had 'awareness' within the meaning of that Directive.</li> </ul>
CJEU Decision	<ul style="list-style-type: none"> <li>This Ruling establishes guidelines to be followed by online marketplaces, such as eBay, for implementing technical procedures to fight against piracy in respect of intellectual property rights.</li> <li>The CJEU ruled that operators of online marketplaces could not rely on the liability exemption referred to in Article 14 of the E-Commerce Directive if they played an 'active role' that would give them knowledge of, or control over, the data relating to offers for sale. Operators of online marketplaces played such a role when they provided assistance entailing, in particular, optimising the presentation of or promoting the online offers for sale.</li> <li>In the case of eBay, the CJEU held that eBay processed the data entered by sellers. The sales in which the offers might result took place in accordance with terms set by eBay. In some cases, eBay also provided assistance intended to optimise or promote certain offers for sale. However, it was for the referring Court to examine whether eBay played an active role such as that described in the preceding bullet point in relation to the offers for sale at issue in the case before it.</li> <li>The CJEU also confirmed that even if operators of online marketplaces did not play the aforementioned 'active role', they might nonetheless be held liable if they were aware of facts or circumstances from which the illegal information was apparent and failed to remove this information from their websites. To ensure that there was a right to an effective remedy against sellers who used such operators' services for intellectual property right infringements, operators of online marketplaces might be ordered to take measures to make it easier to identify those persons.</li> <li>According to the CJEU, in contrast to the 'active role' mentioned above, the following activities conducted by operators of online marketplaces do not have the effect of denying exemption from liability: (i) storage of offers for sale on its server; (ii) setting the terms of its service; (iii) receiving remuneration for that service; and (iv) provision of general information to its customers.</li> </ul>

PROMUSICAE CJEU RULING (29 JANUARY 2008)	
Parties	<ul style="list-style-type: none"> <li>Productores de Música de España (hereinafter, '<b>PROMUSICAE</b>').</li> <li>Telefónica de España, S.A.U. (hereinafter, '<b>TELEFONICA</b>').</li> </ul>
Facts	<ul style="list-style-type: none"> <li>PROMUSICAE is a Spanish non-profit-making organisation of producers and publishers of musical and audiovisual recordings.</li> <li>TELEFONICA is a Spanish commercial company whose activities include the provision of internet access services.</li> <li>PROMUSICAE asked for TELEFONICA to be ordered to disclose the identities and physical addresses of certain persons whom it provided with internet access services, whose IP address and date and time of connection were known. According to PROMUSICAE, those persons used a file exchange program (peer-to-peer) and provided access in shared files of personal computers to phonograms in which the members of PROMUSICAE held the exploitation rights.</li> <li>The Spanish Judge ordered the preliminary measures requested by PROMUSICAE. TELEFONICA appealed against that order, arguing that under the Spanish Law implementing the E-Commerce Directive, the communication of data required by PROMUSICAE was authorised only in a criminal investigation or for the purpose of safeguarding public security and national defence, not in civil proceedings or as a preliminary measure relating thereto.</li> <li>PROMUSICAE argued that the Spanish Law implementing the E-Commerce Directive had to be interpreted in accordance with various provisions of the E-Commerce Directive, the InfoSoc Directive and the Enforcement Directive and with Articles 17(2) ('Right to Property') and 47 ('Right to an effective remedy and to a fair trial') of the Charter of Fundamental Rights. Such provisions did not allow a Member State to limit the obligation to communicate the data in question solely to the purposes expressly mentioned in that law.</li> </ul>
Preliminary Ruling	<p>The Spanish Court asked essentially whether Community law, in particular the E-Commerce Directive, the InfoSoc Directive and the Enforcement Directive, read also in the light of Articles 17 ('Right to Property') and 47 ('Right to an effective remedy and to a fair trial') of the Charter of Fundamental Rights, had to be interpreted as requiring Member States to impose , an obligation to communicate personal data in order to ensure effective protection of copyright also in the context of civil proceedings.</p>
CJEU Decision	<ul style="list-style-type: none"> <li>The CJEU has established that the E-Commerce Directive, the InfoSoc Directive, the Electronic Communications Directive, the Enforcement Directive and the E-Commerce Directive do not require Member States to impose an obligation to communicate personal data in order to ensure effective protection of copyright in the context of civil proceedings.</li> <li>However, according to the CJEU, European law requires that, when converting those Directives into national law, Member States must take care to rely on an interpretation of them that allows a fair balance to be struck between the various fundamental rights protected by the EU legal order, namely, between the protection of personal data on the one hand and the protection of property (including intellectual property) and the right to an effective remedy on the other hand.</li> <li>The mechanisms allowing those different rights and interests to be balanced are contained in the Electronic Commerce Directive, in that it provides for rules that determine in what circumstances and to what extent the processing of personal data is lawful and what safeguards must be provided for, and in the E-Commerce Directive, the InfoSoc Directive and the Enforcement Directive, which reserve the</li> </ul>

#### PROMUSICAE CJEU RULING (29 JANUARY 2008)

cases in which the measures adopted to protect the rights they regulate affect the protection of personal data. They further result from the adoption by Member States of national provisions converting those Directives into national law and their application by national authorities.

- Furthermore, when implementing those Directives, the authorities and courts of the Member States must not only interpret their national laws in a manner consistent with those Directives but also make sure that they do not rely on an interpretation of them that would be in conflict with the fundamental rights mentioned above or with the other general principles of European law, such as the principle of proportionality.

## Chapter 1: Annex 6

### French legal framework

#### Constitutional prerequisites and fundamental rights in France

- French Declaration of the Rights of Man and of the Citizen of 1789 (referenced in the French Constitution).
  - Article 4: Freedom to conduct a business. 'Liberty consists in being able to do anything that does not harm others: thus, the exercise of the natural rights of every man has no bounds other than those that ensure to the other members of society the enjoyment of these same rights. These bounds may be determined only by Law'.
  - Article 2: Right to property. 'The aim of every political association is the preservation of the natural and imprescriptible rights of Man. These rights are Liberty, Property, Safety and Resistance to Oppression'.
  - Article 17: Right to property. 'Since the right to Property is inviolable and sacred, no one may be deprived thereof, unless public necessity, legally ascertained, obviously requires it, and just and prior indemnity has been paid'.
  - Article 9: Presumption of innocence and right of defense. 'As every man is presumed innocent until he has been declared guilty, if it should be considered necessary to arrest him, any undue harshness that is not required to secure his person must be severely curbed by Law'.

#### French Regulations

- French Data Protection Law.
  - Article 6: 'Processing may be performed only on personal data that meet the following conditions: 1° the data shall be obtained and processed fairly and lawfully; 2° the data shall be obtained for specified, explicit and legitimate purposes, and shall not subsequently be processed in a manner that is incompatible with those purposes. [...]; 3° they shall be adequate, relevant and not excessive in relation to the purposes for which they are obtained and their further processing; 4° they shall be accurate, complete and, where necessary, kept up-to-date. Appropriate steps shall be taken in order to delete and rectify data that are inaccurate and incomplete with regard to the purposes which they are obtained and processed for; 5° they shall be retained in a form that allows the identification of the data subjects for a period no longer than is necessary for the purposes for which they are obtained and processed.'
  - Article 7: 'Processing of personal data must have received the consent of the data subject or must meet one of the following conditions: 1° compliance with any legal obligation to which the data controller is subject; 2° the protection of the data subject's life; 3° the performance of a public service mission entrusted to the data controller or the data recipient; 4° the performance of either a contract to which the data subject is a party or steps taken at the request of the data subject prior to entering into a contract; 5° the pursuit of the data controller's or the data recipient's legitimate interest, provided this is not incompatible with the interests of the fundamental rights and liberties of the data subject.'
  - Article 25: '1. The following [instances of processing] may be carried out after authorisation by the CNIL, with the exception of those mentioned in Articles 26 (State security and criminal offences processing) and 27 (public processing NIR, i.e., social security number – State biometrics – census – e-government online services): [...] 4° automatic processing which may, due to its nature, importance or purposes, exclude persons from the benefit of a right, a service or a contract in the absence of any legislative or regulatory provision; [...]'.
- French E-Commerce Law.

- Article 1: 'The exercise of that freedom may be limited only in so far as it is required on the one hand for the respect of human dignity, the freedom and property of others, the pluralist nature of the expression of schools of thought and opinion and on the other hand for the maintenance of 'public order' (public policy), national defence interests, public service requirements, technical constraints inherent to means of communication as well as for the necessity of audiovisual services to develop the audiovisual production. [...]'
- Article 6 I-2°: 'Natural or legal persons who make available to the public through online publicly available communications services, even free of charge, the hosting of signals, writing, images, sounds or messages of any kind provided by the recipients of those services will not be considered civilly liable for activities or information stored at the request of a recipient of these services if they do not have effective knowledge of their illegal nature or of facts and circumstances showing that character or if, from the time when they had this knowledge, they acted promptly to remove such data or make access impossible. The preceding paragraph does not apply when the recipient of the service acts under the authority or control of the provider'.
- Article 6 I-7°: '[Internet service providers or hosting providers] are not bound by a general obligation to monitor information transmitted or stored, neither by a general obligation to actively seek facts or circumstances indicating illegal activity. This is without prejudice to any targeted and temporary surveillance activities required by national judicial authorities. [...]'
- Article 6 I-8°: 'Judicial Authorities may request in a summary procedure or upon request, to any person referred to in 2 [hosting providers] or, failing that, to any person mentioned in 1 [internet service provider], to take all measures to prevent damage or to halt damage caused by the content of an online communications service addressed to the public.'
- French Enforcement Law.
  - The French Enforcement Law converts the Enforcement Directive into French national law under Article L. 716-6 et seq. of the French Intellectual Property Code (*Code de la Propriété Intellectuelle*) and imposes sanctions for intellectual property right infringements.

## CHAPTER 2: ARTICLE 1.7 OF THE ETHICS CODE OF THE AUSTRIAN ADVERTISING INDUSTRY



## Chapter 2: Glossary of terms

For the purposes of this Chapter 2, the following definitions apply:

- **Advertiser:** the client of the advertising campaign placed in an Unlawful Advertising Environment.
- **Advertising Environment Breaching Copyright:** an Unlawful Advertising Environment with a primary purpose and mode of operation obviously in violation of Austrian Copyright Law<sup>100</sup>, as established by Article 1.7 of the Ethics Code<sup>101</sup>.
- **Agency:** the communications agency responsible for Advertisers' advertising campaigns.
- **Associations:** the associations referred to by Article 3.3 of the Rules of Procedure and whose main purpose is to fight against intellectual property rights infringements. These associations are allowed to submit complaints regarding Advertising Environments Breaching Copyright.
- **Austrian Copyright Law:** the Austrian Federal Law No 111/1936 of 9 April 1936 on Copyright in Works of Literature and Art and on Related Rights (*Bundesgesetz über das Urheberrecht an Werken der Literatur und der Kunst und über verwandte Schutzrechte*)<sup>102</sup>.
- **Austrian Data Protection Law:** the Austrian Federal Law No 165/1999 on the Protection of Personal Data (*Bundesgesetz über den Schutz personenbezogener Daten*)<sup>103</sup>.
- **Austrian Regulations:** collectively, the Austrian Copyright Law and the Austrian Civil Code.
- **Charter of Fundamental Rights:** the charter of fundamental rights of the European Union<sup>104</sup>.
- **E-Commerce Directive:** the Directive of 8 June 2000 on electronic commerce<sup>105</sup>.
- **Ethics Code:** the code of ethics of the Austrian advertising industry (*Ethik-Kodex der Werbewirtschaft*)<sup>106</sup>.
- **Ethics Senate:** the independent appeal body attached to the SASR, whose main function is to review the decisions of the Werberat.
- **FAMA:** the Austrian Association for the Music and Film Industry (*Fachverband der Film- und Musikwirtschaft Österreichs*)<sup>107</sup>. FAMA is one of the associations covered by Article 3.3 of the Rules of Procedure.
- **IFPI:** the International Federation of the Phonographic Industry<sup>108</sup>. IFPI is one of the associations covered by Article 3.3 of the Rules of Procedure.
- **INCOPRO:** the United Kingdom company specialising in, inter alia, statistical analysis and in-depth strategic consultation<sup>109</sup>.
- **INCOPRO's Report:** the report issued by INCOPRO on March 2015 entitled, The revenue sources for websites making available copyright content without consent in the EU<sup>110</sup>.

<sup>100</sup> European Digital Right (EDRI), an association of civil and human rights organisations from across Europe, in commenting on a draft of this document, stated 'the term 'advertising environment breaching copyright' is not a legal term and, in all cases, it is used to refer to online resources that are either assumed or alleged to be involved in 'obvious' breaches of copyright. It is therefore inappropriate to use this term without using the word 'alleged', regardless of whether the bureaucratic procedure of the Werberat has been followed or not'.

<sup>101</sup> An unofficial English version of Article 1.7. of the Ethics Code is attached as Annex 2 of this Chapter 2.

<sup>102</sup> <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001848>.

<sup>103</sup> <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597>.

<sup>104</sup> Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, pp. 391-407.

<sup>105</sup> Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ L 178, 17/07/2000 pp. 1–16.

<sup>106</sup> [http://www.werberat.at/layout/ETHIK\\_KODEX\\_4\\_2014.pdf](http://www.werberat.at/layout/ETHIK_KODEX_4_2014.pdf).

<sup>107</sup> <http://www.filmundmusicaustria.at/>.

<sup>108</sup> <http://www.ifpi.at/>.

<sup>109</sup> <http://www.incopro.co.uk/>.



- **Infosoc Directive:** the Directive of 22 May 2001 on copyrights and related rights in the information society<sup>111</sup>.
- **Kino.to CJEU Ruling:** the judgment of 27/03/2014, C-314/12, UPC Telekabel Wien, EU:C:2014:192<sup>112</sup>.
- **Office:** the area of the Werberat that is responsible for processing complaints related to Unlawful Advertising Environments in the scope of a preliminary examination.
- **Pammer CJEU Ruling:** the judgment of 07/12/2010, joined cases C-585/08 and C-144/09, Pammer and Hotel Alpenhof, EU:C:2010:740<sup>113</sup>.
- **Promusicae CJEU Ruling:** the judgment of 29/01/2008, C-275/06, Promusicae, EU:C:2008:54<sup>114</sup>.
- **Rules of Procedure:** the Rules of Procedure of the Werberat (*Verfahrensordnung*)<sup>115</sup>.
- **SASR:** the Austrian Society for Advertising Self-regulation (*Gesellschaft zur Selbstkontrolle der Werbewirtschaft*). The purpose of this entity is to maintain principles of ethics and morality as well as to protect consumers from improper advertising. The SASR is composed of the following bodies: General Assembly, Directors, Working Groups and the Werberat.
- **Small Senate:** the area of the Werberat to whom complaints related to Unlawful Advertising Environments are forwarded by the Office for screening purposes in cases where Advertisers/Agencies do not discontinue their advertising campaigns or do not issue a response to the Office's request within three working days.
- **Svensson CJEU Ruling:** the judgment of 13/02/2014, C-466/12, Svensson and Others, EU:C:2014:76<sup>116</sup>.
- **Trade Association for Advertising:** the trade association for market, communication and advertising in Austria (*Fachverband Werbung und Marktkommunikation*) within the Austrian Chamber of Commerce.
- **Unlawful Advertising Environment:** a website with a primary purpose and mode of operation obviously in violation with the Austrian Laws outlined by Article 1.7. of the Ethics Code, including the Austrian Copyright Law.
- **VAP:** the Austrian Film and Video Anti-piracy Association (*Verein für Anti-Piraterie der Film- und Videobranche*)<sup>117</sup>. VAP is one of the associations covered by Article 3.3 of the Rules of Procedure.
- **VCP:** 'voluntary collaboration practices', developed by industry, public bodies and/or third parties, such as non-governmental organisations and then adhered to by the respective industry in addressing infringements of trade mark rights, design rights, copyright and rights related to copyright over the internet. Here, with regard to the present Chapter 2 'VCP' shall comprise, in particular, Article 1.7 of the Ethics Code as well as the provisions of the Rules of Procedure relating to Article 1.7 of the Ethics Code.
- **Werberat:** the Austrian advertising council, which is the executive body of the SASR<sup>118</sup>.

<sup>110</sup> <http://www.incopro.co.uk/wp-content/uploads/2015/05/Revenue-Sources-for-Copyright-Infringing-Sites-in-EU-March-2015.pdf>.

<sup>111</sup> Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167, 22/06/2001 pp. 10-19.

<sup>112</sup> [http://curia.europa.eu/juris/document/document.jsf?sessionid=9ea7d0f130d5682c6360d7a642ab82679809c8f7b53e\\_e34KaxiLc3eQc40LaxqMbN4ObNmPe0?text=&docid=149924&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=141830](http://curia.europa.eu/juris/document/document.jsf?sessionid=9ea7d0f130d5682c6360d7a642ab82679809c8f7b53e_e34KaxiLc3eQc40LaxqMbN4ObNmPe0?text=&docid=149924&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=141830).

<sup>113</sup> <http://curia.europa.eu/juris/document/document.jsf?text=&docid=83437&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=507786>.

<sup>114</sup> <http://curia.europa.eu/juris/liste.jsf?language=en&num=C-275/06>.

<sup>115</sup> <http://www.werberat.at/beschwerdeverfahrensordnung.aspx>. An unofficial English version of the Rules of Procedure is attached as Annex 3 of this Chapter 2.

<sup>116</sup> <http://curia.europa.eu/juris/liste.jsf?num=C-466/12>.

<sup>117</sup> <http://www.vap.cc>.

## Chapter 2: Structure and content

This Chapter 2 analyses the application of Article 1.7 of the Ethics Code in depth, as well as the articles of the Rules of Procedure linked to it to the Advertising Environments Breaching Copyright, by assessing the following elements:

- Role of the parties involved in the implementation of this VCP.
- Analysis of the duties and procedures prescribed by this VCP.
- Coexistence of the measures established under this VCP with the European Union and Austrian legal frameworks and related case law.
- Role of technologies used in implementing the duties and procedures envisaged by this VCP.
- Costs assumed by the parties involved in the implementation of this VCP.
- Role of educational activities of the parties involved in the promotion of this VCP.
- Effectiveness of the measures established by this VCP.

This Chapter 2 initially involved exhaustive desk research to identify the stakeholders involved in the VCP. A sample of them were then contacted and some agreed to be interviewed for the purposes of this Chapter 2, whilst others declined the invitation to participate.

The statements contained in the Chapter 2 on the stakeholders' position regarding the VCP and their day-to-day procedure are based on the feedback and supporting documentation provided by those stakeholders that agreed to participate in the study.

Although Article 1.7 of the Ethics Code refers to Unlawful Advertising Environments breaching various Austrian regulations, this Chapter 2 focuses exclusively on Advertising Environments Breaching Copyright.

---

<sup>118</sup> <https://www.werberat.at/>.

## 1. Introduction

The Ethics Code, adopted in 2012<sup>119</sup>, is a self-regulatory tool of the Austrian advertising industry whose main aim is to protect consumers from abusive advertising. It comprises all the self-regulatory rules that the Austrian advertising industry has voluntarily imposed on its work.

As established in its introduction, the Ethics Code forms part of the voluntary guidelines, which together with the legal regulations, comprise the dual system of restrictions on advertising in Austria. These self-disciplinary mechanisms are used for monitoring and the early correction of aberrations and undesirable developments in the advertising arena, complementary to the relevant legal provisions.

The Ethics Code aims to support these statutory provisions by being more receptive to the ever-increasing rate of change in society regarding ethics and morality and by responding more quickly to emerging developments in society and in the advertising industry.

The Ethics Code contains the following four sections:

- Section 1 — ‘Basic rules of conduct’. This section includes guidelines addressed to Advertisers relating to general advertising principles (i.e., ethics and morality, violence, health, security, environment). Article 1.7 of the Ethics Code is included in this section.
- Section 2 — ‘Special rules of conduct — persons’. This section includes specific guidelines addressed to Advertisers relating to sexist advertising, advertising featuring or aimed directly at children and young people<sup>120</sup> and advertising featuring older people.
- Section 3 — ‘Special rules of conduct — addictive drugs’. This section includes specific guidelines addressed to Advertisers relating to addictive drugs advertising (i.e., alcohol and tobacco) in order to avoid encouraging consumption of such substances.
- Section 4 — ‘Special rules of conduct — motor vehicles’. This section includes specific guidelines addressed to Advertisers relating to motor vehicle advertising in order to avoid risky, unsocial or environmentally hazardous driving.

The Rules of Procedure are linked to the Ethics Code as they regulate how individuals and associations submit complaints about advertising and how these complaints are dealt with by the Werberat. Currently, two main procedures are established by the Rules of Procedure:

- A specific procedure to submit complaints related to Article 1.7 of the Ethics Code; and
- A general procedure to submit complaints related to the remaining articles of the Ethics Code.

Although, in its initial drafting, the Ethics Code and the Rules of Procedure did not have any mechanisms in place to fight against placing advertising in Unlawful Advertising Environments, including Advertising Environments Breaching Copyright, they were amended by the Werberat in April 2014 to include this possibility. For example, Article 1.7 was added to the Ethics Code and Article 8 to the Rules of Procedure.

According to Article 1.7 of the Ethics Code, an Unlawful Advertising Environment is a web media (e.g., website, banner advertising, internet spot) with a primary purpose and mode of operation obviously in violation to the following Austrian laws:

- The Austrian Data Protection Law (Bundesgesetz über den Schutz personenbezogener Daten)<sup>121</sup>.
- The Austrian Copyright Law.
- The Austrian (NS) Prohibition Law of 1947 (*Verbotsgesetz 1947*)<sup>122</sup>.
- The Austrian Pornography Law (*Bundesgesetz über die Bekämpfung unzüchtiger Veröffentlichungen und den Schutz der Jugend gegen sittliche Gefährdung*)<sup>123</sup> and the provisions of the criminal code

<sup>119</sup> <http://www.werberat.at/selbstdisziplin.aspx>.

<sup>120</sup> Persons between the ages of 12 and 18.

<sup>121</sup> <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597>.

<sup>122</sup> <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10000207>.

<sup>123</sup> <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10005226>

relating to offences against sexual integrity and self-determination (*Bundesgesetz über die mit gerichtlicher Strafe bedrohten Handlungen*)<sup>124</sup>.

- The provisions of the criminal code relating to offences against the public peace (especially dissemination of terrorist and hateful content) (*Bundesgesetz über die mit gerichtlicher Strafe bedrohten Handlungen*)<sup>125</sup>.
- The Austrian Law on War Materials (*Bundesgesetz über die Ein-, Aus- und Durchfuhr von Kriegsmaterial*)<sup>126</sup> and the Austrian Arms Law (*Bundesgesetz über die Waffenpolizei*)<sup>127</sup>.
- The Austrian Addictive Substances Law (*Bundesgesetz über Suchtgifte, psychotrope Stoffe und Drogenausgangsstoffe*)<sup>128</sup>.

As previously explained, this Chapter 2 focuses exclusively on Unlawful Advertising Environments with a primary purpose and mode of operation obviously in violation to Austrian Copyright Law.

In 2012, following stakeholder interviews, FAMA and the Austrian trade association for marketing communications and advertising (*Fachverband Werbung und Marktkommunikation*) issued a joint recommendation to all its member companies not to advertise in Unlawful Advertising Environments. The main objective of such a recommendation was to ensure that members were aware of the implications of advertising misplacement in Unlawful Advertising Environments. Despite doing this, associations saw the need for more commitment by the industry and they decided to approach the Werberat in 2013 to try to find a solution.

Aware of the situation, from December 2013 to February 2014 the Werberat conducted an information campaign to Advertisers to make them aware that sometimes they were placing advertising in Unlawful Advertising Environments and the consequences of such behaviours. As stated by one of the interviewed Associations, the Werberat sent screenshots of advertising in Unlawful Advertising Environments, which had been identified by one association during its monitoring activities, to sixty of the most important Advertisers. These entities were unaware that they were placing advertising in Unlawful Advertising Environments and were unhappy about it. Once notified by the Werberat, they removed such advertising from the mentioned Environments, which included Advertising Environments Breaching Copyright.

Following its information campaign on Unlawful Advertising Environments, the Werberat decided that its Ethics Code should be amended as well as its Rules of Procedure, as explained above. As stated by one of the interviewed stakeholders, the amendments to the Ethics Code and to the Rules of Procedure are the result of a close collaboration between the Werberat and associations.

Interviewed stakeholders explained in the context of this Chapter 2 that the main objectives of Article 1.7 of the Ethics Code and Article 8 of the Rules of Procedure are as follows:

- To create a safer internet for users, since advertising campaigns of well-known brands placed in Unlawful Advertising Environments can give the impression to users that those websites are providing services that are legal.
- To protect Advertisers' reputation.
- To promote the value of the Austrian online market.
- To reduce the revenues of Unlawful Advertising Environments.

As provided for by Article 1.7 of the Ethics Code and as explained by the Werberat interviewed for the purposes of this Chapter 2, this VCP is a supplementary and voluntary initiative which must not interfere with applicable Austrian or European law. Compliance with the provisions of the Ethics Code or with the cessation requests of the Werberat in relation to Advertising Environments Breaching Copyright is voluntary and up to Advertisers.

<sup>124</sup> <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296>.

<sup>125</sup> <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296>.

<sup>126</sup> <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10000609>.

<sup>127</sup> <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10006016>.

<sup>128</sup> <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10011040>.

## 2. Stakeholders and third parties<sup>129</sup>

The activities of the Werberat as executive body of the SASR are supported by its Rules of Procedure and the Ethics Code. In April 2014, these industry self-regulatory tools were amended by the Werberat to include explicitly the possibility to fight, inter alia, against the placement of advertising in Advertising Environments Breaching Copyright through a specific procedure.

Although, according to Article 1.1 of the Rules of Procedure, anyone is entitled to submit complaints about advertising with the Werberat, when it comes to Advertising Environments Breaching Copyright, Article 3.3 of the Rules of Procedure restrains such faculty of complaining to associations.

Complaints raised by associations before the Werberat are sent by the latter to Advertisers or Agencies, who may remove the advertising from the conflicting Advertising Environment Breaching Copyright.

As the Ethics Code is an initiative of the advertising industry, public authorities do not participate explicitly in the VCP and were not involved in its drafting.

Finally, one of the main aims of the Ethics Code is to protect consumers from browsing through Advertising Environments Breaching Copyright. Notwithstanding this, civil society was not involved in the drafting of the Ethics Code.

This Section of Chapter 2 explains the specific roles regarding the VCP played by the five mentioned categories of stakeholders (i.e., the Werberat, associations, advertisers/agencies, public authorities and civil society).

### 2.1. Role of the Werberat

The Werberat is the executive body of the SASR. It was created in 1974<sup>130</sup> and it acts independently in its decision-making.

The Werberat is constituted by experts from companies in the advertising arena, namely Advertisers, Agencies and media as well as by prominent personalities from other disciplines (e.g., lawyers and psychologists). All of its members are natural persons and they are elected by the General Assembly of the SASR for renewable periods of three years.

Inter alia, the Werberat's main functions are the following:

- To deal with consumer complaints related to commercial advertising.
- To deal with association complaints related to the placement of advertising in Unlawful Advertising Environments, including Advertising Environments Breaching Copyright.
- To initiate proceedings *ex officio* about advertising.
- To act as a contact point for consumers as regards commercial advertising.
- To develop self-regulatory guidelines for the advertising industry.
- To draft publicly available reports in relation to its activities.

The Ethics Code and the Rules of Procedure were amended to include specific provisions related to Unlawful Advertising Environments, following the information campaign carried out by the Werberat from December 2013 to February 2014, which aimed to prevent the placement of advertising in such Environments. These amendments were the result of close cooperation between the Werberat and associations.

In the context of this VCP, the Office is the body that receives complaints regarding Advertising Environments Breaching Copyright and carries out the preliminary examination thereof<sup>131</sup>. Such complaints may be eventually

<sup>129</sup> A list of the stakeholders interviewed for the purposes of this Chapter 2 is attached as Annex 1 of this Chapter 2.

<sup>130</sup> The Werberat was subject to an important reorganisation in 2008.

forwarded to the Small Senate in cases where the complaint is considered justified (in German *begründet*) by the Office, but the relevant Advertiser or Agency does not discontinue the advertising campaign concerned nor does it provide a response to the Office's request to issue an opinion<sup>132</sup>. Should Advertisers not agree with the Small Senate's decision, they may file an appeal before the Ethics Senate of the SASR.

It is not within the scope of the Werberat's powers to sanction infringers of Austrian Copyright Law. In particular, the Werberat does not have the power to prohibit the operation of Advertising Environments or assess with any kind of legal effect the question of whether or not an Advertising Environment is infringing any statutory intellectual property rights. If the Werberat receives a complaint from an association relating to an Advertising Environment, it can advise the Advertiser who publishes advertising on the respective Environment to refrain from doing so. However, Advertisers are by no means legally obliged to comply<sup>133</sup>.

Concerning the non-binding nature of the Werberat's decisions, there are only two rulings of the Austrian Supreme Court mentioning such decisions<sup>134</sup> and in both cases, where the admissibility of advertising campaigns was at stake, the Supreme Court ruled against it.

## 2.2. Role of associations<sup>135</sup>

Associations (e.g., FAMA, VAP, IFPI) are the only category of stakeholders permitted to submit complaints to the Werberat regarding advertising they consider having been placed in Advertising Environments Breaching Copyright in the context of Article 1.7 of the Ethics Code, as established by Article 3.3 of the Rules of Procedure. Complaints must be based on a coherent exposition of facts and may end up with the removal of the advertising from the Environment by the Advertiser.

As stated by the Werberat interviewed for the purposes of this Chapter 2, the reason behind the restriction on associations in relation to the submission of complaints is that associations' main purpose is the prevention of illegal practices in advertising media. They are, therefore, supposed to be able to determine whether a website may be considered an Advertising Environment Breaching Copyright and what criteria to follow to come to this conclusion. Indeed, as one of the interviewed associations stated, their daily business is to monitor what is happening online and determine which websites are making online content illegally available; as such, they consider themselves a one-stop shop for information on Advertising Environments Breaching Copyright.

One of the associations, interviewed for the purposes of this Chapter 2, explained that prior to the introduction of Article 1.7 under the Ethics Code and Article 8 under the Rules of Procedure they occasionally contacted Advertisers and Agencies identified through their website monitoring activities to alert them that they were placing advertising in Advertising Environments Breaching Copyright. However, this measure was not always effective as only about one in five Advertisers/Agencies ended up in removing their advertising from such Advertising Environments after receiving the association's warning.

<sup>131</sup> As explained by the Werberat for the purposes of the Chapter 2, in practice they consider a complaint justified (in German *begründet*) when the complaint meets the territorial, material and subjective scope of the VCP and do not analyse whether the Advertising Environment identified in the complaint effectively infringes copyright (See Section 3.3.2 of this Chapter 2 ('Preliminary examination of the complaint by the Office (Articles 8.1, and 8.2 of the Rules of Procedure')).

<sup>132</sup> See Article 8(3), 8(5), Rules of Procedure of the Werberat, if the complaint is considered 'justified' or 'founded' (in German: *begründet*). In this context, EDRI, in commenting on a draft of this document, stated that 'the word 'justified' is misused ... a complaint is 'justified', ... means that it is valid ... the rightholders make complaints and these are unquestioningly processed by the Werberat and unquestioningly actioned by the participating advertisers.'

<sup>133</sup> EDRI, in commenting on a draft of this document, stated 'that ignores the fact that, once ... it is confirmed as fulfilling the criteria of the VCP, advertising is withdrawn from the allegedly infringing environment, which will (and is intended to) hurt that environment and is quite obviously a sanction that is imposed as a direct result of the Werberat's decision'.

<sup>134</sup> Decision of the Austrian Supreme Court No 4 Ob 59/00f of 14 March 2000, and Decision of the Austrian Supreme Court No 4 Ob 64/00s of 14 March 2000.

<sup>135</sup> The Associations interviewed for this Chapter 2 are a sampling of those involved in the VCP.



Interviewed associations have explained that they have contributed actively to the insertion of Article 1.7 under the Ethics Code and Article 8 under the Rules of Procedure either by alerting the Werberat about their concerns related to the placement of advertising in Unlawful Advertising Environments or by collaborating directly in the drafting of the mentioned articles.

If we look at Article 1.7 of the Ethics Code and Article 8 of the Rules of Procedure, the main role of associations in this VCP seems to be to report to the Werberat the existence of what they consider Advertising Environments Breaching Copyright where advertising is placed. However, as explained by the Werberat in the context of this Chapter 2, in practice the role of associations goes beyond the mentioned actions as they have been the drivers of the VCP and they are the ones who know it well.

### 2.3. Role of Advertisers/Agencies

In cases where the Werberat considers a complaint raised by an association against an advertising placed in an Advertising Environment Breaching Copyright to be justified, in line with Article 8.3 of the Rules of Procedure, it issues a request to the Agency or Advertiser placing the advertising in the conflicting Environment to submit their opinion on the complaint, so that they have the opportunity to express their views on the matter.

The Werberat can address its requests to any Advertiser or Agency, regardless as to whether they are Members of the SASR or not.

One Advertiser involved in a complaint procedure raised by an association, pursuant to Articles 2.8 and 8 of the Rules of Procedure in connection with Article 1.7 of the Ethics Code, has participated in this Chapter 2. As this Advertiser explained, they worked closely with their Agency to address the Werberat's request related to Article 1.7 of the Ethics Code. They consider the VCP as a tool protecting brand safety.

### 2.4. Role of public authorities

The Ethics Code is a private initiative carried out by the Austrian advertising industry with no mandatory power and no governmental help. Public authorities neither took part in the drafting of the VCP nor in their implementation.

### 2.5. Role of civil society

One of the main aims of the Ethics Code is to protect consumers from browsing in Advertising Environments Breaching Copyright, as by doing so they could assume that those websites are providing services that are legal.

Nevertheless, as pointed out by the Werberat and by one association interviewed, consumer associations were not invited to contribute to the drafting of the VCP.

In relation to this Chapter 2, several Austrian consumer associations have been contacted in order to gather their opinion about the VCP. Although two consumer associations agreed to be interviewed for the purposes of this Chapter 2 (see Chapter 2: Annex 1), only one of these associations made comments on the intellectual property aspects of the Ethics Code. Neither association interviewed was initially aware that the Ethics Code had been amended in April 2014 to include Article 1.7.

The interviewed consumer association that made comments on the intellectual property aspects of the Ethics Code highlighted that they are sceptical generally regarding self-regulation as it may eventually harm the fundamental rights of certain groups of people. Nevertheless, they do not consider that this VCP affects the mentioned rights since the decisions of the Werberat are not binding and therefore it is voluntary for Advertisers to withdraw their advertising from the Advertising Environments. Having said that, rather than being considered as an instrument to fight against the infringement of intellectual property rights, the consumer association considers that the VCP should be regarded as an awareness tool to make Advertisers/Agencies aware of the situation.



## 3. Duties and procedures

This Section summarises the duties and procedures resulting both from Article 1.7 of the Ethics Code and the articles of the Rules of Procedure relating to Advertising Environments Breaching Copyright.

### 3.1. Scope of application of the VCP

#### 3.1.1. Territorial scope

The Werberat's activities are limited to the territory of the Federal Republic of Austria, as stated in Article 2.1 of the Rules of Procedure.

Bearing this in mind, as explained by the Werberat and by one association, the territorial criteria to be considered when it comes to submitting complaints before the Werberat against Advertising Environments Breaching Copyright in relation to Article 1.7 of the Ethics Code are:

- The Advertiser placing its advertising in such Environments has to be based in Austria, i.e., it has to be an Austrian company or an Austrian subsidiary of an international company; and
- The advertising placed in the Advertising Environment Breaching Copyright has to be directed to an Austrian audience, either exclusively or in addition to audiences of other jurisdictions<sup>136</sup>.

The Werberat and one of the interviewed associations have indicated that complaints can refer to Advertising Environments Breaching Copyright owned by entities that are not based in Austria. Otherwise, it would be easy for such Environments to escape the VCP, merely by getting incorporated in a foreign jurisdiction.

#### 3.1.2. Material scope

As provided for by Article 2.4 of the Rules of Procedure, the Werberat is not competent regarding the following advertising:

- Party political and election advertising.
- Publications that promote the arts and culture alone; insofar as goods, services, companies or events directly or indirectly related to this segment are exclusively advertised.
- Advertising of and for non-profit organisations.

Therefore, where an association raises a complaint before the Werberat concerning the placement of one of the mentioned categories of advertising in an Advertising Environment Breaching Copyright, such a complaint would be rejected by the Office.

#### 3.1.3. Subjective scope

As laid down in Article 3.3 of the Rules of Procedure and as previously mentioned in this Chapter 2, only associations can submit to the Werberat complaints against Advertising Environments Breaching Copyright.

### 3.2. Definition of Advertising Environments Breaching Copyright

As explained by the Werberat, they do not decide whether an Advertising Environment identified in the complaint infringes copyright. In practice they examine complaints received from associations to determine whether they fall

<sup>136</sup> It may be extracted from the *Pammer* CJEU Ruling, that the following criteria, inter alia, may determine that an advertising placed in an Advertising Environment Breaching Copyright is addressed to an Austrian audience: (i) use of German language; (ii) use of Austrian telephone numbers for contact purposes; or (iii) use of an '.at' domain name.

within the territorial, material and subjective scope of the VCP (see Section 3.3.2 of this Chapter 2 ('Preliminary examination of the complaint by the Office (Articles 8.1 and 8.2 of the Rules of Procedure)'). For example, the Werberat checks if the complaint has been submitted by an association, whether the advertiser concerned is based in Austria and the advertising is addressed to an Austrian audience.

In practice, associations are the ones that set forth whether an advertising environment infringes copyright. Amongst their day-to-day activities is the monitoring of websites to try to identify Advertising Environments Breaching Copyright. As explained by one of the interviewed associations, they internally manage an evidence sheet where they include for each Advertising Environment Breaching Copyright the evidence gathered.

One of the interviewed associations explained for the purposes of this Chapter 2 that for defining Advertising Environments Breaching Copyright they mainly base their assessment on the following parameters and/or tools:

- Factors drawn from case law<sup>137</sup>.
- Factors outlined in an INCOPRO report<sup>138</sup>.
- Rankings of the most popular websites in Austria<sup>139</sup>. These rankings help associations to prioritise their monitoring activities.
- The Google Transparency Report<sup>140</sup>. This is taken as a reference to determine the scale of copyright infringement and see how many right holders object to content that is made available on certain websites.

### 3.3. Complaint procedure before the Werberat

When the VCP was created, Article 8 was introduced under the Rules of Procedure to specifically regulate the procedure applicable to complaints related to Unlawful Advertising Environments, including Advertising Environments Breaching Copyright.

That being said, Article 8 of the Rules of Procedure contains certain cross-references to other pre-existing articles of the Rules of Procedure. Namely, such other articles of the Rules of Procedure that are applicable to the general complaint procedure system of the Werberat and that existed prior to the implementation of this VCP in April 2014 are the following:

- Article 9.2 of the Rules of Procedure.
- Article 11 of the Rules of Procedure.
- Article 15 of the Rules of Procedure.

In addition, Article 16 of the Rules of Procedure, which deals with the communication of the Werberat's decisions, refers to Article 8 of the Rules of Procedure and thus would also be applicable to the VCP.

According to Article 8 of the Rules of Procedure as well as the other articles of the Rules of Procedure that are applicable to the VCP, the complaint procedure governing Advertising Environments Breaching Copyright comprises the following phases:

- Submission of complaints by associations (Article 3.3. of the Rules of Procedure).
- Preliminary examination of the complaint by the Office (Articles 8.1 and 8.2 of the Rules of Procedure).

---

<sup>137</sup> e.g. Decision of the Austrian Supreme Court No 4 Ob 71/14s of 26 June 2014.

<sup>138</sup> See INCOPRO's report, Appendix A, *Full methodology*, Section *Factors for selecting sites* of the INCOPRO's report, <http://www.incopro.co.uk/wp-content/uploads/2015/05/Revenue-Sources-for-Copyright-Infringing-Sites-in-EU-March-2015.pdf>.

<sup>139</sup> e.g. <http://www.alexa.com/topsites/countries/AT>;  
[http://www.similarweb.com/country/category/austria/arts\\_and\\_entertainment/movies](http://www.similarweb.com/country/category/austria/arts_and_entertainment/movies).

<sup>140</sup> <https://www.google.com/transparencyreport/removals/copyright/?hl=en>.

- Request to Advertisers/Agencies to issue an opinion (Articles 8.3, sentence 1 and 8.4 of the Rules of Procedure).
- Notification to the owner of the Advertising Environment Breaching Copyright (Article 8.3, sentence 2 of the Rules of Procedure).
- Forward of the complaint to the Small Senate (Articles 8.5, 8.6 and 9.2 of the Rules of Procedure).
- Appeal by the Advertiser/Agency or the owner of the Advertising Environment Breaching Copyright before the Ethics Senate (Articles 8.7 and 15 of the Rules of Procedure).
- Communication of the Werberat's decision to Advertisers/Agencies, owners of Advertising Environments Breaching Copyright and associations (Article 16 of the Rules of Procedure).

### 3.3.1. Submission of complaints by associations (Article 3.3 of the Rules of Procedure)

As stated by two associations interviewed for the purposes of this Chapter 2, complaints regarding Advertising Environments that are considered to be breaching copyright can be submitted by associations at any time by filling out an online complaint form available at the Werberat website.

Although, as explained under Section 3.2 of this Chapter 2 ('Definition of Advertising Environments Breaching Copyright'), there is previous monitoring and analysis work done by associations to determine whether an Advertising Environment is obviously infringing copyright. When it comes to the online submission of the complaint, a coherent exposition of facts is sufficient (Article 8.2 of the Rules of Procedure).

Additionally, if associations wish they can upload screenshots of the Advertising Environment to the online complaint form, subject to their complaint.

### 3.3.2. Preliminary examination of the complaint by the Office (Articles 8.1 and 8.2 of the Rules of Procedure)

Once a complaint regarding an Advertising Environment Breaching Copyright is received, the Office assesses whether the complaint is justified (in German *begründet*). If considered necessary, the Office may contact the concrete association that has submitted the complaint for further information and clarification.

As explained by the Werberat for the purposes of Chapter 2, in practice it considers a complaint justified when it falls within the scope of application of the VCP, namely when it meets its territorial, material and subjective scope (see Section 3.1 of this Chapter 2 ('Scope of application of the VCP')): the Werberat does not analyse whether the Advertising Environment identified in the complaint effectively infringes copyright. It has been emphasised by the Werberat that it does not have competence to rule with legal consequence on the question of whether or not the Environment is infringing copyright and it relies on associations' opinions.

Interviewed for the purposes of this Chapter 2, one association explained that the Werberat so far has always considered justified the complaints the association has raised concerning Advertising Environments they identified as breaching copyright.

No specific deadline is envisaged by the Rules of Procedure concerning the Office's preliminary examination. As indicated by one association interviewed for the purposes of this Chapter 2, the Werberat generally conducts the preliminary examination in an efficient manner.

### 3.3.3. Request to Advertisers/Agencies to issue an opinion (Articles 8.3, sentence 1 and 8.4 of the Rules of Procedure)

Article 8.3 of the Rules of Procedure envisages that when the Office considers a complaint justified it issues a request to the Advertiser or the Agency asking for their opinion on the complaint within three working days. Although it is not established in the Rules of Procedure, according to one association interviewed for the purposes

of this Chapter 2, the Advertiser may request an extension of the mentioned deadline, which in fact has already happened in practice.

Two associations interviewed have explained that, in fact, the Office generally gets in touch with the Advertiser and such party will contact its Agency to try to understand how its advertising ended up in an Advertising Environment Breaching Copyright.

Two associations interviewed have highlighted that, in practice, if Advertisers have questions about the Office's request for opinion (e.g., why it has been considered that a specific Advertising Environment infringes copyright), the Werberat will come back to associations and ask them to communicate directly with the Advertiser concerned. This has happened once in practice. This direct interaction between Advertisers and associations is due to the fact that associations are the ones that decide to submit claims relating to Advertising Environments they consider to be in breach of copyright and, as pointed out, in practice the Werberat does not analyse whether such Environments effectively infringe the Austrian Copyright Law.

Article 8.4 of the Rules of Procedure provides that should the Advertiser agree to the discontinuation of the advertising campaign in the Advertising Environment Breaching Copyright, the Office will close the file and the complainant association will be informed of the decision; in line with Article 11 of the Rules of Procedure. Advertisers generally remove their advertising from Advertising Environments Breaching Copyright as such a placement may damage their image and sometimes even breach their internal ethical rules. The Werberat stated that Advertisers are generally grateful for being informed that their advertising is placed on Advertising Environments Breaching Copyright, as they are often unaware of the circumstances, mainly for the following reasons:

- Certain Advertisers manage their own blacklists about Advertising Environments Breaching Copyright but as new Advertising Environments are being created such blacklists are not always up-to-date.
- Advertisers do not always have a strict control of the digital supply chain.

As explained by the Werberat, among all the Advertisers contacted by the Office only one (i.e., an online gaming company) was initially reluctant to remove its advertising campaign, but it finally agreed to do so. In this respect, it is important to bear in mind that the choice to remove advertising from an Advertising Environment considered to be breaching copyright is based on a voluntary business decision, as the Werberat's requests are not legally binding. In fact, it has been pointed out by one association that what makes this VCP successful is its collaborative nature.

#### 3.3.4. Notification to the owner of the Advertising Environment Breaching Copyright (Article 8.3, sentence 2 of the Rules of Procedure)

In parallel to the request to issue an opinion addressed to Advertisers, the Office must also try to reach the owners of the Advertising Environment Breaching Copyright to inform them about the complaint (Article 8.3 of the Rules of Procedure).

However, as pointed out both by the Werberat and by two associations they are generally not able to comply with such notification in practice for the following reasons:

- Most of the owners of Advertising Environments Breaching Copyright are not based in Austria.
- Most of the Advertising Environments Breaching Copyright do not provide sufficient contact details.

As explained by the Werberat, to date no Advertising Environment Breaching Copyright has complained about the Werberat's requests for removal of advertising to Advertisers/Agencies. According to the Werberat, this is due to the fact that normally 'the activities of such Environments are dubious'.

### 3.3.5. Forward of the complaint to the Small Senate (Articles 8.5, 8.6 and 9.2 of the Rules of Procedure)

As per Article 8.5 of the Rules of Procedure, the complaint will be forwarded by the Office to the Small Senate with a request for comments within three working days in the following cases:

- The Advertiser/Agency considers the complaint unfounded in whole or in part and continues the advertising campaign; or
- The Advertiser/Agency does not issue a response to the Office's request within three working days.

In such cases, after having analysed the complaint and the arguments of the Advertiser and the owner of the Advertising Environment Breaching Copyright, if any, the Small Senate may decide to request the cessation of the advertising from the Advertising Environment Breaching Copyright. The cessation of the advertising campaign is totally voluntary for the same reasons explained above.

To date, based on the information provided by stakeholders interviewed, no complaints have reached the Small Senate given that all concerned Advertisers removed their advertising campaigns from Advertising Environments Breaching Copyright during the preliminary examination phase before the Office.

### 3.3.6. Appeal by the Advertiser/Agency or the owner of the Advertising Environment Breaching Copyright before the Ethics Senate (Articles 8.7 and 15 of the Rules of Procedure)

Where Advertisers/Agencies or the owner of the Advertising Environment Breaching Copyright do not agree with the Small Senate's cessation request, they may raise an appeal against it before the Ethics Senate, as provided for by Articles 8.7 and 15 of the Rules of Procedure.

Such an appeal has to be performed in writing and Advertisers or the owners of the Advertising Environments Breaching Copyright have to provide the Ethics Senate with additional information not presented previously in the procedure. As an example of what kind of additional information can be provided, Article 15.2 of the Rules of Procedure refers to market research data.

As informed by the Werberat and by associations interviewed, at the time of conducting this Chapter 2, in practice, no appeals regarding Article 1.7 of the Ethics Code have been submitted to the Ethics Senate by Advertisers/Agencies or owners of Advertising Environments Breaching Copyright.

### 3.3.7. Communication of the decision to Advertisers/Agencies, owners of Advertising Environments Breaching Copyright and Associations (Article 16 Rules of Procedure)

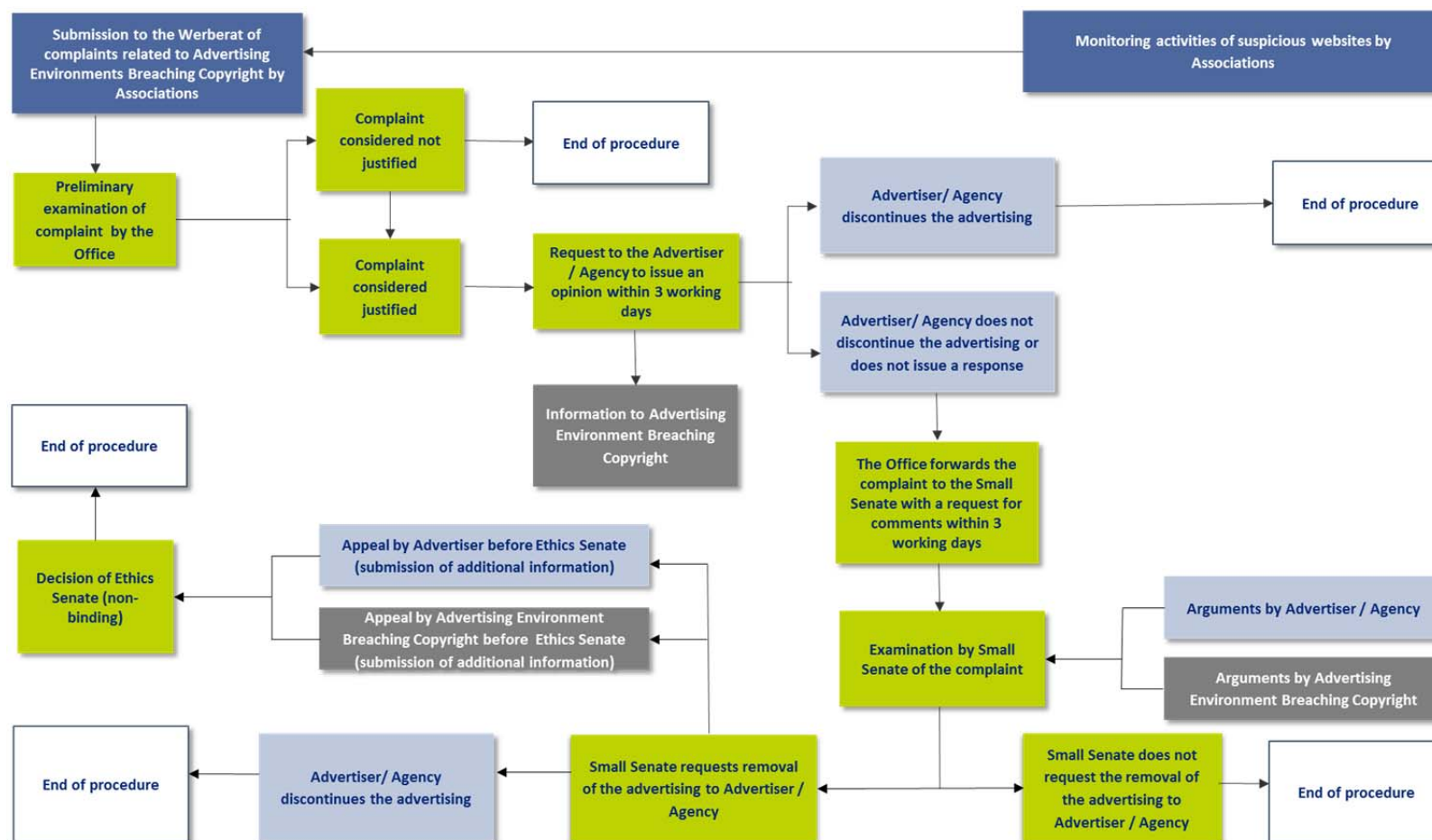
According to Article 16 of the Rules of Procedure, complaining associations and concerned Advertisers/Agencies and owners of Advertising Environments Breaching Copyright are to be notified by the Werberat about its decisions.

Additionally, the Werberat's decisions are published on the Werberat's website<sup>141</sup>.

---

<sup>141</sup> <http://www.werberat.at/verfahrenliste.aspx>.

### 3.3.8. VCP procedure flowchart





## 4. Coexistence of the measures set forth under the VCP with European Union and Austrian legal frameworks and related case law

Section 4 of this Chapter 2 ('Coexistence of the measures set forth under the VCP with the European Union and Austrian legal frameworks and related case law') summarises the European Union and Austrian legal frameworks and related case law that may have an impact on the practical application of the VCP.

The considerations included in this Section are based upon the following legal sources:

- Fundamental Rights in the European Union (Section 4.1. of this Chapter 2 ('Charter of fundamental rights')).
- European Union Directives (Section 4.2 of this Chapter 2 ('European Union directives')).
- Constitutional Prerequisites and Fundamental Rights in Austria (Section 4.3 of this Chapter 2 ('Constitutional prerequisites and fundamental rights in Austria')).
- Austrian Regulations (Section 4.4 of this Chapter 2 ('Austrian Regulations')).

### 4.1. Charter of Fundamental Rights

As further analysed under Section 4.5 of the Chapter 2 ('Analysis of the VCP in relation to the European Union and Austrian legal frameworks and case law'), the fundamental rights set out below, provided for by the Charter of Fundamental Rights<sup>142</sup>, may eventually have an impact on the duties envisaged by the VCP:

- Article 11, 'Freedom of expression and information'. This right includes, inter alia, freedom to receive information and ideas without interference by public authority and regardless of frontiers.
- Article 16, 'Freedom to conduct a business'. This right includes the freedom to undertake an economic or commercial activity and the freedom of contract.
- Article 17, 'Right to property'. This right stipulates that no one shall be deprived of his possessions except in the public interest and in cases and under conditions provided for by law, subject to fair compensation being paid in good time for their loss. Protection of intellectual property (including literary and artistic property, as well as patent and trade mark rights and associated rights) is explicitly covered by this right.

As far as other fundamental rights envisaged by the Charter of Fundamental Rights are concerned, such as, for example, the right to the protection of personal data (Article 8 of the Charter of Fundamental Rights, ('Protection of personal data')) and the right to an effective remedy and to a fair trial (Article 47 of the Charter of Fundamental Rights, ('Right to an effective remedy and to a fair trial')), it is doubtful that such rights may have an impact on this VCP for the reasons outlined in Section 4.5 of this Chapter 2 ('Analysis of the VCP in relation to the European Union and Austrian legal frameworks and case law').

### 4.2. European Union Directives

As the VCP intends to fight, inter alia, against infringement of the Austrian Copyright Law, the following provisions of the Infosoc Directive<sup>143</sup> are to some extent related given that they establish that right holders have the exclusive right of making available works to the public and they deal with the measures/sanctions applicable to the infringement of copyright:

---

<sup>142</sup> See complete wording in Annex 4 of this Chapter 2.

<sup>143</sup> See complete wording in Annex 4 of this Chapter 2.



- Article 3 of the Infosoc Directive. This article envisages that right holders have the exclusive right to authorise or to prohibit the making available to the public of their works from a place and at a time individually chosen by such public.
- Article 8 of the Infosoc Directive. This article envisages that the sanctions applicable to the infringement of copyright or related rights shall be effective, proportionate and dissuasive. Likewise, right holders shall be able to apply for injunctions against intermediaries whose services are used by a third party to infringe a copyright or related rights.

Contrasting with the views expressed in the remaining chapters of this study regarding other VCPs, Article 15 of the E-Commerce Directive would not be relevant in the case at issue as neither Article 1.7 of the Ethics Code nor the Rules of Procedure envisage any monitoring duty or any obligation to actively seek facts or circumstances indicating the infringement of copyright.

The Fundamental Rights mentioned under Section 4.1 of this Chapter 2 ('Charter of Fundamental Rights') and the aforementioned Directives, have been interpreted, inter alia, in the following cases<sup>144</sup>:

- Promusicae CJEU Ruling

This Ruling establishes that the protection of intellectual property rights is not of a higher order than other fundamental rights; meaning that the protection of intellectual property rights does not prevail over other rights, such as the freedom to conduct a business.

- Kino.to CJEU Ruling

Amongst others, this Ruling establishes that where several fundamental rights protected by the European Union legal order are at issue, such legal order and the interpretation thereof shall ensure a fair balance between the various rights at stake and shall avoid conflicts with other general principles of EU law, such as the principle of proportionality. Namely, in its Ruling the CJEU highlights the need to strike a balance between (1) copyright and related rights, which are intellectual property and are therefore protected by Article 17.2 of the Charter of Fundamental Rights, (2) the freedom to conduct a business, which economic agents enjoy under Article 16 of the Charter of Fundamental Rights and (3) the freedom of information of internet users, whose protection is ensured by Article 11 of the Charter of Fundamental Rights.

- Svensson CJEU Ruling

This Ruling establishes that the provision of clickable links to protected works constitutes an act of communication to the public. To the extent the links are directed at a 'new public', namely, a public that was not taken into account by copyright holders at the time of the initial communication, the authorisation of copyright holders would be required. This would be the case, for example, in relation to a protected work no longer available to the public on the website on which it was initially communicated or where it is henceforth available on that website but only to a restricted public, while being accessible on another website through a clickable link. In light of this, it may be considered that Advertising Environments Breaching Copyright make available protected works to a new public as they are addressed to a public that was not taken into account by the copyright holders, in which case the owners of such Environments would require copyright holders' consent to perform such a communication legally.

### 4.3. Constitutional prerequisites and fundamental rights in Austria

The following fundamental rights set forth by the Austrian State Basic Act of 1867 (*Staatsgrundgesetz*), which enjoys constitutional status in Austria<sup>145</sup>, may have an impact on certain measures envisaged by the VCP:

- Article 5 of the Austrian State Basic Act of 1867, *Right to property*
- Article 6 of the Austrian State Basic Act of 1867, *Freedom to conduct a business*
- Article 13 of the Austrian State Basic Act of 1867, *Freedom of expression*

<sup>144</sup> See detailed description in Annex 6 of this Chapter 2.

<sup>145</sup> See complete wording in Annex 5 of this Chapter 2.

Although these fundamental rights have been considered by Austrian courts, there are no decisions directly applicable to the VCP. Below are examples of relevant cases in other areas:

- Decision of the Austrian Constitutional Court No B622/1982 of 5 December 1983

This decision deals with the fixation of reasonable remuneration for a license based on Article 59a of the Austrian Copyright Law. The Austrian Collecting Society explained that the fixed remuneration was not reasonable as it reduced the authors' remuneration and it alleged that it constituted a violation of the right to property. The Austrian Constitutional Court ruled that the protection of copyright is effectively covered by the right to property but it considered that the remuneration at stake was reasonable and rejected the Austrian Collecting Society's claim.

- Decision of the Austrian Constitutional Court No G118/2015 of 3 July 2015

This decision deals with the distribution of electronic cigarettes. The Austrian Constitutional Court ruled that when it comes to electronic cigarettes the purposes of protection of health and youth are not as worthy as the freedom to conduct a business. Hence, the distribution of electronic cigarettes may not be restricted in a way whereby only certified tobacco dealers are allowed to sell such cigarettes.

#### 4.4. Austrian Regulations

The following provisions of the Austrian Regulations are related to the VCP<sup>146</sup> to the extent they deal with the protection of copyright and its enforcement:

- Article 18(1) of the Austrian Copyright Law. This article establishes that authors have the exclusive right to make their works available to the public.
- Article 81(1) and Article 81(1)(a) of the Austrian Copyright Law. These articles establish that a person who has suffered an infringement of any exclusive rights conferred by the Austrian Copyright Law, or who fears such an infringement, is entitled to bring proceedings for a restraining injunction.
- Article 82 of the Austrian Copyright Law. This article establishes that a person who has suffered an infringement of any exclusive rights conferred by the Austrian Copyright Law is entitled to file cease-and-desist actions.
- Article 85 of the Austrian Copyright Law. This article envisages the publication of court decisions related to cease-and-desist actions.
- Article 86 of the Austrian Copyright Law. This article deals with claims on equitable remuneration.
- Article 87 of the Austrian Copyright Law. This article deals with claims for damages and for the surrender of profits.
- Article 87a of the Austrian Copyright Law. This article deals with claims for rendering of accounts.
- Article 87b of the Austrian Copyright Law. This article deals with claims for information.
- Article 87c of the Austrian Copyright Law. This article deals with claims for interim injunctions.

In addition, Article 1330 of the Austrian Civil Code grants a right for the claiming of compensation by anybody that suffers damages or losses profit due to defamation.

The Austrian Regulations have been considered by Austrian courts, inter alia, in the following cases:

- Decision of the Austrian Supreme Court No 4 Ob 71/14s of 26 June 2014

On the basis of the Kino.to CJEU Ruling, the Austrian Supreme Court ruled that if the main purpose of a website is to make various protected works available to the public without the agreement of the relevant rightholders, the respective internet service provider can be ordered to block access to the website. But the reason why this ruling is important in relation to this VCP is because, unlike the CJEU, the Austrian Supreme Court clarified that such a

---

<sup>146</sup> See complete wording in Annex 5 of this Chapter 2.

blocking order only applies to websites that are in obvious violation of copyright laws and describes how to categorise a website as being in obvious violation of the Austrian Copyright Law. This ruling is used by associations, among other tools, to categorise Advertising Environments they consider to be in breach of copyright.

- Decision of the Austrian Supreme Court No 4 Ob 105/11m of 20 September 2011

A professional photographer filed an action against an operator of an internet search engine claiming that the search engine provides a publicly available preview of pictures without his consent. The legal issue at stake was whether the publication is to be regarded as a copyright infringement. The Austrian Supreme Court dismissed the claim and considered the preview as not infringing copyright given that the search engine did not save the pictures on a database but provided a hyperlink to the legally uploaded picture, i.e., to a copy of the protected work which was made available with the rightholder's consent. By combining this decision with the VCP, it may be extracted that websites providing hyperlinks to legally uploaded content made available with rightholders' consent would not qualify as Advertising Environments Breaching Copyright.

#### 4.5. Analysis of the VCP in relation to the European Union and Austrian legal frameworks and case law

In light of the European Union and the Austrian legal frameworks and related case law discussed in the preceding Sections of this Chapter 2, it cannot be totally excluded that perhaps certain procedures envisaged by the VCP may be eventually considered inconsistent with the right of Advertisers to conduct their business, this possibly even more so taking into consideration the *Promusicae* and the *Kino.to* CJEU Rulings. Therefore, under Section 4.5.1 of this Chapter 2 ('Coexistence of the VCP with the freedom to conduct business of Advertisers' and owners of Advertising Environments Breaching Copyright') the right of Advertisers and owners of Advertising Environments Breaching Copyright to conduct their business is reviewed in detail so as to determine whether it effectively impacts the VCP.

As far as other fundamental rights are concerned, such as those analysed under other chapters of this study (e.g., right to the protection of personal data; right to an effective remedy and to a fair trial; freedom of information), it is unlikely that they may have a detrimental impact on the VCP, as highlighted in Section 4.5.2 ('Coexistence of the VCP with the right to an effective remedy and to a fair trial of owners of Advertising Environments Breaching Copyright'), Section 4.5.3 ('Coexistence of the VCP with the right to the protection of personal data of the stakeholders involved in the VCP') and 4.5.4 ('Coexistence of the VCP with the freedom of internet users to receive information').

Finally, given that according to Article 1330 of the Austrian Civil Code anybody that suffers damages due to defamation may claim for compensation, under Section 4.5.5 of this Chapter 2 ('Resort by the owners of advertising environments allegedly breaching copyright to the Article 1330 of the Austrian Civil Code') it is analysed whether the owners of advertising environments may resort to such possibility.

##### 4.5.1. Coexistence of the VCP with the freedom to conduct business of Advertisers' and owners of Advertising Environments Breaching Copyright

The freedom to conduct a business is enshrined in Article 16 of the Charter of Fundamental Rights (*Freedom to conduct a business*) and in Article 6 of the Austrian State Basic Act of 1867 (*Freedom to conduct a business*).

This freedom includes, without limitation, the right for any business to be able to freely use within the limits of its liability for its own acts the economic, technical and financial resources available to it. It has been pointed out in the literature<sup>147</sup> that this freedom recognises the right to economic initiative its main function being to foster social, economic and political integration and to protect consumers.

---

<sup>147</sup> Andrea Usai. 'The Freedom to Conduct a Business in the EU, Its Limitations and Its Role in the European Legal Order: A New Engine for Deeper and Stronger Economic, Social, and Political Integration' ([https://www.germanlawjournal.com/pdfs/Vol14-No9/14.9.10\\_Usai\\_Business%20Freedom.pdf](https://www.germanlawjournal.com/pdfs/Vol14-No9/14.9.10_Usai_Business%20Freedom.pdf)).

In relation to the VCP, both Advertisers and owners of Advertising Environments Breaching Copyright being economic agents enjoy the freedom to conduct a business granted by the Charter of Fundamental Rights and by the Austrian State Basic Act of 1867 by means of which they have the freedom to choose, inter alia, where to place their advertising.

#### *4.5.1.1. Coexistence with the freedom to conduct a business of Advertisers*

The Werberat's requests to Advertisers to remove their advertising from Advertising Environments Breaching Copyright following an association's request may, to some extent, interfere with Advertisers' business activities. Indeed, the Werberat's requests may restrict the free use of Advertisers' resources since it may lead Advertisers to take measures that represent a cost for them and that may impact their activities. In reality, banning Advertisers from placing their advertising in an Advertising Environment Breaching Copyright may lead to a loss of audience for them.

However, as already mentioned previously in this Chapter 2, the Werberat's requests to remove advertising are not legally binding and Advertisers may freely decide whether or not to remove their advertising from Advertising Environments Breaching Copyright following the Werberat's cessation requests. Accordingly, the interference with Advertisers' activities identified above is limited due to the non-binding nature of the Werberat's decisions. Thus, it may be argued that in practice the Werberat's requests would effectively not impinge on Advertisers' freedom to conduct their business.

#### *4.5.1.2. Coexistence with the freedom to conduct a business of owners of Advertising Environments Breaching Copyright*

By means of the freedom to conduct a business, website owners have the liberty, inter alia, to sell advertising space to Advertisers.

The decrease in the placement of advertising on Advertising Environments considered to be in breach of copyright as a consequence of the VCP may, to some extent, interfere with the business activities of the website owners (it being justified or not). In reality, the Werberat's requests to Advertisers to remove their advertising from Advertising Environments Breaching Copyright may imply a loss of revenues for such Environments.

Even if it could be considered that this would endanger the existence of the website owner's business, it would have to be borne in mind that this freedom may be subject to limits and restrictions that have been recognised by the CJEU in various decisions since its judgment of 14/05/1974, C-4/73, Nold KG v Commission, EU:C:1974:51<sup>148</sup>. Limits to the freedom to conduct a business are accepted provided that the two following conditions are satisfied:

- The restriction must protect the general interest proportionately; and
- The restriction must not hinder the substance of the right.

As to the first condition, among the VPC's aims are (i) the protection of rightholders' intellectual property rights and (ii) the creation a safer environment for consumers so that they avoid Advertising Environments Breaching Copyright. The CJEU has found that consumer protection and the protection of intellectual property rights may be construed as a general interest that would justify restrictions to the freedom to conduct a business (see respectively CJEU judgments of 08/10/1986, C-234/85, Keller, EU:C:1986:377<sup>149</sup> and 30/07/1996, C-84/95, Bosphorus v Minister for Transport, Energy and Communications and Others, EU:C:1996:312<sup>150</sup>). As to the second condition, it cannot be considered that the restriction to place advertising on Advertising Environments Breaching Copyright would hinder the substance of the freedom to conduct business of the respective website owner given that advertising it is only one of the financing mechanisms of such owners.

In light of this, as the CJEU accepts certain limitations to the freedom to conduct a business that would be applicable in the case of the VCP, it cannot be considered that the freedom of owners of Advertising Environments Breaching Copyright to conduct their business would be breached.

<sup>148</sup> <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:61973CJ0004>.

<sup>149</sup> <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:61985CJ0234>.

<sup>150</sup> <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:61995CJ0084>.

#### 4.5.2. Coexistence of the VCP with the right to an effective remedy and to a fair trial of owners of Advertising Environments Breaching Copyright

The right to an effective remedy and to a fair trial is established by Article 47 of the Charter of Fundamental Rights (*Right to an effective remedy and to a fair trial*) as well as by Article 83(2) of the Austrian Constitution of 2 December 1867 (*Bundes-Verfassungsgesetz*).

This right seeks to provide effective recourse to any person who alleges that his/her rights have been violated and it comprises, inter alia, the following requirements: (i) decisions shall be issued by impartial and independent bodies, through equitable processes taking place within reasonable time frames; (ii) persons concerned shall be able to ascertain the reasons upon which decisions are based, either by reading the decisions themselves or by requesting and obtaining disclosure of those reasons; (iii) persons concerned shall be able to contest the grounds on which the decisions are based and to make submissions on the evidence relating to the decisions.

In relation to the VCP, Article 8 of the Rules of Procedure specifically provides for the implementation of safeguards towards owners of Advertising Environments Breaching Copyright, namely:

- Following the reception of a complaint from an association, the Werberat requests the Advertiser to issue an opinion and, in parallel, it also informs the owner of the Advertising Environment Breaching Copyright concerned on the reception of the claim (Article 8.3 of the Rules of Procedure).
- Owners of Advertising Environments Breaching Copyright may submit arguments before the Small Senate (Article 8.6 of the Rules of Procedure).
- In cases where the Small Senate would issue a cessation request to an Advertiser, the owner of the Advertising Environment Breaching Copyright concerned may file an appeal against such decision before the Ethics Senate (Article 8.7 of the Rules of Procedure).

Therefore, if we contrast the requirements comprised by the fundamental right analysed with the provisions of the VCP relating to Advertising Environments Breaching Copyright, it is unlikely that the VCP may breach the right to an effective remedy and to a fair trial of the owners of such advertising environments<sup>151</sup>.

#### 4.5.3. Coexistence of the VCP with the right to the protection of personal data of the stakeholders involved in the VCP

The right to the protection of personal data is envisaged by Article 8 of the Charter of Fundamental Rights (*Protection of personal data*) and by Article 1(1) of the Austrian Data Protection Law. This right generally serves to protect the self-determination right of an individual regarding the use of personal data related to him.

Although the processing of information related to legal persons is outside of the scope of the Data Protection Directive, Austria is amongst the countries that extend the right to the protection of data to information relating to legal persons. Indeed, Article 2 of the Austrian Data Protection Law defines 'data subjects' as follows: 'Any natural or legal person or group of natural persons not identical with the controller, whose data are processed'. This circumstance has also been stressed by the Austrian Supreme Court<sup>152</sup>.

In the case of the VCP, following the reception of a complaint made by an association, the Werberat tries to find out by its own means the contact details of Advertisers (e.g., contact section of their corporate website) and of owners of Advertising Environments Breaching Copyright (e.g., contact section of the Environment itself; existing public registers, such as 'Whois' databases) and gets in touch directly with them. The Werberat focuses on information that is publicly available. The following provisions of the Austrian Data Protection Law are to be considered as regards data publicly available:

---

<sup>151</sup> EDRI, in commenting on a draft of this document, stated 'it is problematic that website operators can only submit arguments before the Small Senate (i.e., if the Advertiser submits objections)'.

<sup>152</sup> For example, in its decision No 6 Ob 162/00t of 28 June 2000, the Austrian Supreme Court ruled that the economic data of a company are protected by the Austrian Data Protection Law.

- Article 1(1) of the Austrian Data Protection Law. It envisages that everybody shall have the right to secrecy for the personal data related to him/her insofar as he/she has an interest deserving such protection and such an interest is precluded when data cannot be subject to the right to secrecy due to their general availability.
- Article 8(2) of the Austrian Data Protection Law. It envisages that the use of legitimately published data shall not constitute an infringement of interests in secrecy deserving protection.

Accordingly, as the data used by the Werberat to contact Advertisers and the owners of Advertising Environments Breaching Copyright is data that has been legitimately published, the right to the protection of personal data would not be infringed due to the processing of such data.

Furthermore, none of the duties and procedures envisaged by the VCP — analysed under Section 3 of this Chapter 2 ('Duties and Procedures') — implies the exchange of personal data of persons/companies involved in complaints under Article 8 of the Rules of Procedure. In this sense, as already pointed out previously in this Chapter 2, one of the interviewed associations has highlighted that in practice if Advertisers have questions about the Office's request for opinion, the Werberat will come back to associations and will ask them to communicate directly with the Advertiser concerned, but in such cases it may be understood that the relevant association agrees to the disclosure of its personal data to the Advertiser.

Finally, although the publication of the Werberat's decisions on its website may involve the disclosure of the names of the Advertiser and the owner of the Advertising Environment Breaching Copyright, as such data is to be considered published data, then its protection would not be infringed in line with Articles 1(1) and 8(2) of the Austrian Data Protection Law.

Therefore, based on the previous considerations it can be understood that the right to the protection of personal data of the parties involved in the VCP could impact the VCP.

#### 4.5.4. Coexistence of the VCP with the freedom of internet users to receive information

The freedom to receive information is established by Article 11 of the Charter of Fundamental Rights (*Freedom of expression and information*) as well as by Article 13 of the Austrian State Basic Act of 1867 (*Staatsgrundgesetz*).

This freedom includes, inter alia, the right to receive information without interference.

Internet users enjoy the freedom to receive information granted by the Charter of Fundamental Rights and by the Austrian State Basic Act of 1867 by means of which they have the freedom to access the information available on the websites they visit.

Among others, it may be extracted from the Kino.to CJEU Ruling that the measures adopted to bring an end to a third party's online infringement of copyright or of a related right shall not prevent internet users to lawfully access information on the service provider's website.

In the case at issue, should an Advertiser decide to discontinue its advertising campaign from an Advertising Environment Breaching Copyright following the Werberat's request, this would not affect internet users' freedom to access the information available in the mentioned Advertising Environment, i.e., on the website, since this information would not be blocked as a consequence of the duties and procedures envisaged by the VCP.

Therefore, it can be considered that the VCP is not in breach of the freedom of internet users to receive information.



#### 4.5.5. Resort by the owners of Advertising Environments Breaching Copyright to the Article 1330 of the Austrian Civil Code<sup>153</sup>

According to Article 1330 of the Austrian Civil Code, a person that adversely affects another person's reputation (either natural or legal) by making untrue facts available to the public can be sued before Austrian civil courts by the affected person.

In the case of the VCP, as the Werberat's decisions are published on its website, in case an Advertising Environment would have been incorrectly categorised by an association as an Advertising Environment Breaching Copyright the owner of such environment could also claim for compensation or for revocation of the Werberat's decision before Austrian courts on the basis of Article 1330 of the Austrian Civil Code as the publication of the Werberat's decision would be based on untrue facts and could affect its reputation.

However, based on the interviews conducted with associations and with the Werberat for the purposes of this Chapter 2 it seems that in practice it is unlikely that the owners of Advertising Environments Breaching Copyright could file an action against the Werberat before civil courts, pursuant to Article 1330 of the Austrian Civil Code, given that before filing their complaints with the Werberat, associations exhaustively review Advertising Environments to make sure they are actually infringing the Austrian Copyright Law. Although the risk exists that an association would incorrectly categorise an Advertising Environment as an Advertising Environment Breaching Copyright, it is reasonable to understand that such risk would be relatively low taking into account that associations are experts on such matters. In fact, as explained by the Werberat, to date none of the owners of Advertising Environments Breaching Copyright that have been subject to a complaint under Article 8 of the Rules of Procedure have claimed for compensation/revocation of the Werberat's decision, pursuant to Article 1330 of the Austrian Civil Code.

#### 4.5.6. Summary of findings relating to the coexistence of the VCP with the European Union and Austrian legal frameworks and case law

This Section summarises the findings made under Section 4 of this Chapter 2 ('Coexistence of the measures set forth under the VCP with European Union and Austrian legal frameworks and related case law') regarding the compatibility of the VCP with European Union and Austrian legal frameworks and case law.

##### 4.5.5.1. *Coexistence of the VCP with fundamental rights*

The following conclusions have been reached concerning the coexistence of the VCP with certain fundamental rights:

- Freedom to conduct a business of Advertisers and owners of Advertising Environments Breaching Copyright
  - Advertisers

---

<sup>153</sup> EDRI, in commenting on a draft of this document, has pointed out that even if they '[...] agree that defamation law might be an unlikely resort for affected website operators, we could also imagine more realistic means of redress namely: contractual liability of the advertiser for unjust contract termination, or tort liability of the right holder (for unfair business practices).' The alternative options suggested by EDRI have not been analysed in this Chapter as they are outside of its scope.



Although the Werberat's requests to remove advertising addressed to Advertisers following associations' complaints may eventually be seen as restricting the free use of Advertisers' resources, as they may lead Advertisers to take measures that represent a cost for them and that may impact their activities, as the Werberat's requests are not legally binding in practice it may be argued that such requests may effectively not impinge on Advertisers' freedom to conduct their business.

- Owners of Advertising Environments Breaching Copyright

Even if it could be considered that the loss of revenues by owners of Advertising Environments Breaching Copyright as a consequence of the VCP may possibly impact on their freedom to conduct a business, the CJEU accepts certain limitations to such a right that would be applicable to the situation at issue.

- Right to an effective remedy and to a fair trial of owners of Advertising Environments Breaching Copyright

It is unlikely that the right to an effective remedy and to a fair trial of the owners of Advertising Environments Breaching Copyright could impact the VCP given that Article 8 of the Rules of Procedure provides for the implementation of safeguards towards such owners (e.g., they may issue their opinion or submit claims against the Werberat's decisions).

- Right to the protection of personal data of the stakeholders involved in the VCP

It is unlikely that the right to the protection of personal data of Advertisers and owners of Advertising Environments Breaching Copyright could impact the VCP given that the categories of data related to them processed in connection with this VCP are data legitimately published. As far as associations are concerned, it may be understood that they agree to the disclosure of personal data related to them to Advertisers.

- Freedom of internet users to receive information

The VCP is not in breach of the right of internet users to access information. Indeed, although Advertisers may eventually remove their advertising from an Advertising Environment Breaching Copyright, the information of such Environment could still be accessed by internet users as it would not be blocked as a consequence of the duties and procedures envisaged by the VCP.

#### *4.5.5.2. Resort by the owners of Advertising Environments Breaching Copyright to Article 1330 of the Austrian Civil Code*

In such cases where an Advertising Environment would have been incorrectly categorised as an Advertising Environment Breaching Copyright, the owner of such Environment could claim for compensation or for revocation of the Werberat's decision before Austrian courts on the basis of Article 1330 of the Austrian Civil Code.

However, based on the interviews conducted with Associations and with the Werberat, it seems that in practice it is unlikely that the owners of Advertising Environments Breaching Copyright could file an action against the Werberat before civil courts, pursuant to Article 1330 of the Austrian Civil Code.

## 5. Technologies

As the Rules of Procedure establish in Article 3.3, only associations may file complaints against Advertising Environments Breaching Copyright. Such complaints have to be performed through the online complaint form available at the Werberat website. However, such an online complaint submission mechanism already existed before the implementation of the VCP in April 2014, as it was designed for the submission to the Werberat of complaints related to the overall Ethics Code.

In addition, according to the information obtained during the interviews, parties use emails for communicating and exchanging information.

## 6. Costs

Associations do not have to pay any administration fees to the Werberat in relation to the VCP.

Furthermore, as far as their monitoring activities are concerned, although they may involve certain costs (e.g., one association interviewed has indicated that at some point they hired the monitoring services of a vendor), such costs are not strictly related to the VCP but rather to the associations' daily business.

As far as the Werberat is concerned, the VCP does not entail any special costs for them, as explained during the interviews conducted for the purposes of this Chapter 2.

## 7. Education

So far, the following events have taken place in relation to the VCP:

- The Werberat organised a press conference to present the VCP after its implementation in April 2014.
- The VCP was presented by the Werberat at the 2014 Safer Internet Day, organised at European Union level.

In addition, the Werberat website publishes news related to the VCP, its background, its objectives<sup>154</sup> and also the Werberat's decisions in the context of Article 1.7 of the Ethics Code, so that interested parties may have access to it.

As indicated by stakeholders interviewed for this Chapter 2, educational activities relating to this VCP mainly focus on Advertisers/Agencies' awareness as their participation in the VCP is key to achieving its main objective: the removal of advertising from Advertising Environments Breaching Copyright.

Educational activities are not specifically addressed to associations since they participated in the creation of the VCP and they are therefore aware of it.

Finally, as far as consumers are concerned, one association interviewed explained that they prefer not to carry out specific educational activities addressed to this category of stakeholders as, in their opinion, there is a risk that consumers could become aware of Advertising Environments Breaching Copyright that they were not otherwise aware of and could thus access illegal content offered through them.

---

<sup>154</sup> [http://www.werberat.at/news\\_154.aspx](http://www.werberat.at/news_154.aspx).

## 8. Effectiveness

Prior to the official implementation of the VCP, between December 2013 and February 2014 the Werberat conducted an information campaign addressed to Advertisers and it supplied sixty of the most important Advertisers with screenshots of their advertising in Unlawful Advertising Environments. All notified Advertisers decided to remove such advertising from the mentioned Environments, which included Advertising Environments Breaching Copyright.

After the official implementation of the VCP, all the Advertisers contacted removed their advertising upon the request of the Werberat.

At the time the primary research for this Chapter 2 was undertaken (June 2016), the following statistics regarding Unlawful Advertising Environments were publicly available on the Werberat's website<sup>155</sup>:

	Total number of complaints filed relating to 1.7 of the ethics code
2014	11
2015	5

As put forth by the Werberat for the purposes of this Chapter 2, of the total complaints the following are specifically related to Advertising Environments Breaching Copyright:

Year	Number of complaints related to advertising environments breaching copyright
2014	9
2015	1

<sup>155</sup> <http://www.werberat.at/statistik.aspx>.

## Chapter 2: Annex 1

### Interviewed stakeholders

Rightholder Associations	Intermediaries	Civil Society
VAP (Anti-piracy Association of the Film Industry)	Werberat	Arbeiterkammer- Konsumentenschutz (Consumers' area in the Austrian Chamber of Labour)
IFPI Austria (International Federation of the Phonographic Industry)		VIBE (Association for internet users in Austria)
FAMA (Trade Association for Film and Music)		
GEBERIT – Company that has withdrawn its advertising from Advertising Environments Breaching Copyright in the context of Article 1.7 of the Ethics Code		

## Chapter 2: Annex 2

### Article 1.7 of the Ethics Code (*Unlawful Advertising Environments*)

**Austrian Advertising Council** valid from 1 April 2014

The self-regulatory body of the Austrian advertising industry

#### ADVERTISING INDUSTRY CODE OF ETHICS

In Austria, as is the case in nearly all European countries, a dual system of restrictions on advertising is in place, which consists of legal regulations on the one hand, and voluntary guidelines on the other. The advertising industry's code of ethics constitutes a core component of the Austrian system for the protection of consumers from abuse of advertising. Self-disciplinary mechanisms of the advertising industry are used for monitoring and early correction of aberrations and undesirable developments, complementing the relevant legal provisions. The self-regulatory guidelines of the advertising industry for a country must correspond to the scope of statutory advertising rules. In jurisdictions with progressive legal regulatory systems for advertising and consumer protection, which is extensive in Austria, the self-regulatory framework for advertising tends to shift to areas of ethics and morality that are subject to social development (at an ever-increasing pace). These areas cannot be legally regulated since they are constantly changing and evolving; they represent a culturally specific elusive phenomenon, which necessitates advertising self-regulation with a good sense of judgement. The advertising industry code of ethics, i.e., the totality of self-regulatory policies that the Austrian advertising industry has voluntarily imposed on its work, is divided into two parts. The first part, 'Basic rules of conduct', mainly consists of directives on the aforementioned sensitive areas, and represents the 'core' of the advertising industry code of ethics. The second part, 'Special rules of conduct', governs areas that have come to be of particular relevance nationally or internationally as part of our borderless communication society, and therefore require special arrangements.

[...]

#### 1.7 UNLAWFUL ADVERTISING ENVIRONMENTS

##### *Preamble*

Following the increasing importance of advertising placements in web media (banner advertising, internet spots and the like), the question of the ethical evaluation of the advertising environment used is gaining in prevalence.

Advertising on advertising carriers with a primary purpose and mode of operation obviously in violation of the applicable laws in effect in the territory of the Federal Republic of Austria (cf. illustrative list in the following paragraph) is contrary to the general advertising principles. A responsible advertising sector strives not to place advertising campaigns in such an advertising environment. This is particularly true in the online world.

Advertising carriers with a primary purpose and mode of operation obviously in violation of the applicable laws in effect in the territory of the Federal Republic of Austria, are especially those with the following primary purpose and/or mode of operation.

- Breach of the Data Protection Act Austria
- Violation of Rights under the Copyright Act Austria
- Breach of the (NS) Prohibition Act Austria of 1947
- Violation of the Pornography Act Austria and/or the provisions of the Criminal Code relating to offences against sexual integrity and self-determination
- Violation of the provisions of the Criminal Code relating to offences against the public peace (especially dissemination of terrorist and/or hateful content)
- Violation of the Law on War Materials and/or the Arms Acts Austria
- Violation of the Addictive Substances Act Austria.



## Chapter 2: Annex 3

### Rules of Procedure of the Werberat

**Version:** 26 January 2015

#### *Article 1 Entitlement to appeal*

- (1) Any person is entitled to submit complaints about advertising with the Austrian Advertising Council.
- (2) The Austrian Advertising Council may also initiate proceedings.

#### *Article 2 Jurisdiction of the Austrian Advertising Council*

- (1) The activities of the Austrian Advertising Council cover the entire territory of the Federal Republic of Austria.
- (2) The jurisdiction of the Austrian Advertising Council is limited to the area of commercial advertising.
- (3) The Austrian Advertising Council is responsible
  - a) for advertising and promotional activities of all companies operating in Austria, which are published in Austria in all types of media. The prerequisite is for an advertising campaign to be addressed to the Austrian population. Promotional activities also encompass measures that affect the presentation of any company, insofar as they are directed at the general public or specific persons, and go beyond internal corporate communications.
  - b) for professional communication to inform citizens ('public information') through public bodies of the Federation and the State (extended jurisdiction).
- (4) The Austrian Advertising Council is not responsible
  - a) for party political and election advertising
  - b) for publications that promote the arts and culture alone; insofar as goods, services, companies or events directly or indirectly related to this segment are exclusively advertised, as well as
  - c) for advertising of and for non-profit organisations.
- (5) In commercial representations and statements that violate the law against unfair competition (UWG), the Austrian Advertising Council acts as a contact, but is not deemed competent to act. The Austrian Advertising Council is a member of the association for the protection against unfair competition, and reserves the right to forward any such complaints to the Protection Association.
- (6) If any complainant asserts claims alleging that a competitor is in breach of statutory provisions, the Austrian Advertising Council may request that such complainant assert such rights individually. If the advertising campaign may take a decisive impact on end consumers, the Austrian Advertising Council reserves the right to forward the complaint to the competent authorities and law enforcement officials.
- (7) The Austrian Advertising Council may conduct preliminary testing of publicity in the scope of the service 'Copy Advice', which specifically excludes an evaluation under competition law. There is no legal right to a preliminary evaluation.
- (8) The Austrian Advertising Council may evaluate the compatibility of the placement of advertising in an Advertising Environment as per Article 1.7 of the Code of Ethics of the Austrian advertising industry at the request of any association within the meaning of Article 3 (3). The evaluation of individual contents (editorial content of a medium, user-generated content) in an Advertising Environment that is generally deemed safe is excluded. The detailed procedure is described in Article 8.

### *Article 3 Form of complaint*

(1) Complaints are to be directed to the Austrian Advertising Council in writing, specifying the applicant and an accurate statement of the circumstances (under reference to the advertising industry Code of Ethics), as well as submission and/or reference to the exact type of means of advertising (e.g., visual display, brochure, TV spot, poster, banner ads or online viral etc.), and reference to the medium (e.g., title, station, name, URL of website):

‘Gesellschaft zur Selbstkontrolle der Werbewirtschaft’

Wiedner Hauptstrasse 57/III/6

A-1040 Wien

Phone: +43 (0)5 90 900-3577

Fax: +43 (0)5 90 900-285

Email: [office@werberat.at](mailto:office@werberat.at) internet: <http://www.werberat.at/>

(2) All consumers are entitled to register complaints on the homepage of the Austrian Advertising Council. For this purpose, an online, publicly available complaint option is available under [www.werberat.at](http://www.werberat.at).

(3) Any complaints due to the placement of advertising on illegal advertising carriers may only be submitted by associations whose main purpose is the prevention of illegal practices on advertising carriers (e.g., the internet). The complaint must be justified in writing, and the accuracy of statements must be warranted.

(4) Telephone complaints are processed if the applicant is clearly identifiable.

(5) Anonymous complaints are generally not processed.

### *Article 4 Confidentiality of the complaint*

(1) The identity of the complainant will be kept confidential.

### *Article 5 Costs*

(1) Proceedings before the Austrian Advertising Council are free of charge.

### *Article 6 Receipt of complaints*

(1) Following an appeal to the Austrian Advertising Council, the office is to establish contact with the complainant without delay.

(2) The Austrian Advertising Council is required to clarify the circumstances under investigation as far as possible. Accordingly, the office will investigate the complaint in terms of competence and relevance. For this purpose, the Advertising Council may consult third parties for expertise or legal advice.

(3) If competence and relevance apply, complaints are ranked according to their time of receipt, and alternately forwarded to Senate 1, 2 or 3 of the decision-making body of the office for processing. Essential detail: complaints are checked first by the Austrian Advertising Council in terms of their relevance and competence in order of receipt, and are immediately allocated to the next free group, once relevance and competence have been established.

(4) In the presence of competence and relevance, the office will verify the completeness of the information. The office is authorised to obtain the information necessary for this purpose.

### *Article 7 Rejection of complaints without proceedings*

(1) The office of the Austrian Advertising Council will reject any application without further proceedings, if:

- a) the Council is not competent, or
- b) the issue is subject to ordinary criminal administrative proceedings at the time of referral to the Austrian Advertising Council, or

- c) civil proceedings pending in civil or criminal courts of law, or if criminal prosecution is under consideration.
- d) Complaints will also be rejected if the necessary documents for further processing have not been submitted by the applicant in full, and are not furnished upon further request.

### *Article 8 Complaints relating to the Advertising Environment*

- (1) Complaints regarding an Advertising Environment (e.g., websites, online platforms) may be processed by the office of the Advertising Council in the scope of a preliminary examination.
- (2) The assessment takes place on the basis of Article 1.7 of the Code of Ethics of the Austrian advertising industry and on the basis of coherent exposition of facts by the complainant association.
- (3) If the complaint is considered justified by the office, the office of the Austrian Advertising Council will issue a request to the client of the campaign and/or the responsible Agency to issue an opinion on the complaint within three working days. The office of the Austrian Advertising Council is to notify the owner of the Advertising Environment if possible.
- (4) If the client and/or the responsible agency agree to the discontinuation of the advertising campaign in the Advertising Environment at issue, the complaint case is to be concluded. All stakeholders will be notified as per Article 11.
- (5) If the Advertisers and/or responsible Agency consider the appeal unfounded in whole or in part, and they do not intend to discontinue the advertising campaign accordingly, or if they have not issued a response within three working days, the complaint is forwarded to the Small Senate (Article 9(2)) without delay with a request for comment (three working days).
- (6) The Small Senate may, after examination of the complaint and any arguments of the Advertiser or the advertising carrier, decide to request removal of the advert.
- (7) The client/s of the campaign and/or the agency, as well as the operator of the advertising carrier, may raise objections against the request for removal, in accordance with Article 15.

### *Article 9 Manifestly unfounded complaints*

- (1) Complaints may be classified as manifestly unfounded in the scope of preliminary examination. In this case, the complaint is dismissed without further proceedings.
- (2) For purposes of screening, a Small Senate is set up. This committee consists of four periodically changing members of the Austrian Advertising Council, the speaker of the Austrian Advertising Council, as well as a board member of the association. Said period is limited to half a year.
- (3) The Small Senate will be sent complaints by the office that are manifestly unfounded in their opinion for preliminary examination. The assessment takes place based on the code of ethics of the advertising industry.
- (4) For a final decision of the Small Senate, a response of at least two-thirds of its members (four out of six) is required. Otherwise, the complaint must be immediately forwarded to the Austrian Advertising Council for further examination, in accordance with Article 9 et seq.
- (5) The office of the Austrian Advertising Council is to notify the board of the association, the complainant, the respondent (Advertisers) and/or the responsible Agency, as well as the advertising carrier of the matter.
- (6) The applicant may object against dismissal of the complaint only by specific reference to an article of the advertising industry Code of Ethics that was previously not cited in the complaint. In this case, the board is to reconsider the complaint, in accordance with Article 9.
- (7) Manifestly unfounded complaints, where no proceedings were initiated, are not included in the statistics of the Austrian Advertising Council.

### *Article 10 Complaints that are not manifestly unfounded — opinion of affected parties*

(1) Upon receipt of a complaint that is not obviously unfounded, the office of the Austrian Advertising Council will request the client of the campaign and/or the responsible Agency to issue an opinion on the complaint within three working days.

(2) The office of the Austrian Advertising Council may notify the media the complaint refers to of the matter as well.

### *Article 11 Performance by modification of advertising*

(1) If the client and/or the responsible Agency agree to modification or discontinuation of the disputed advertising campaign, the office of the Austrian Advertising Council will notify the complainant, as well as the advertising carrier in cases of Article 10, paragraph 2.

(2) The office of the Austrian Advertising Council is entitled to terminate the present complaint without direct referral to the Austrian Advertising Council, under Article 11, paragraph 1. All members of the Austrian Advertising Council and the board of the association must be notified in writing without delay.

### *Article 12 Submission to the Austrian Advertising Council*

(1) If the Advertisers and/or responsible Agency consider the appeal unfounded in whole or in part, and they do not intend to modify or discontinue the advertising campaign accordingly, or if they have not issued a response within the deadline defined by the Austrian Advertising Council (Article 10, paragraph 1), the complaint is forwarded to the Austrian Advertising Council with a request for comment without delay (three working days).

(2) For this purpose, the complaint is sent to the competent Austrian Advertising Council Senate according to Article 6, paragraph 3, along with the offending adverts/spots by the office, as well as the opinion of the company where applicable. Transmission of information will take place by email.

(3) The members of the Austrian Advertising Council are requested to submit their comments to the office via the online assessment tool within a period of three working days.

(4) Decision-making takes place by simple majority of valid votes cast (at least six votes) of the members of the Austrian Advertising Council. The chairman of the Austrian Advertising Council shall have the casting vote.

### *Article 13 Decision*

(1) The Austrian Advertising Council generally decides by way of three decision categories:

1. No reason to intervene
2. Awareness — request to be more sensitive when designing advertising campaigns or individual content in the future
3. Request for an immediate halt to the campaign or immediate change of content.

(2) Decisions are made on the basis of valid votes cast by the members according to the following distribution of votes:

- 'No intervention' if at least 50 per cent of votes are in favour,
- 'Request for immediate cessation' only if more than 50 per cent vote in favour (absolute majority, i.e., 50 per cent of votes cast + 1),
- in all other cases, category two 'Awareness' applies.

The spokesperson of the Austrian Advertising Council shall have the casting vote.

(3) Aggregation rules for the categories 'Cessation' for 'ambivalent' cases are defined as follows: (unclear cases occur if 'Cessation' receives most votes, but does not reach absolute majority)

Step 1: in the first step, it is decided if cessation is requested on the basis of votes cast. Cessation may only take place if an absolute majority is reached.

If most votes were cast in category 'Cessation', but no absolute majority was achieved, Step 2 follows.

Step 2: the votes on 'Cessation' and 'Awareness' are added, and compared to the votes for 'No reason to intervene'. If there is a majority of added votes for 'Cessation' and 'Awareness', the decision is for 'Awareness'. If, however, 'No intervention' has more votes than 'Stop' and 'Awareness' together, then the decision is 'No intervention'.

(4) The office of the Austrian Advertising Council is to aggregate comments of individual advertising council members, evaluate them in accordance with Article 12, paragraph 1 et seq., and arrive at a decision.

(5) Members of the advertising council must take the following into account in their decision:

- a. the legal provisions
- b. the Austrian advertising industry Code of Ethics, as well as the Rules of Procedure of the Advertising Council
- c. the conduct of advertising practice of the International Chamber of Commerce (ICC codes).

### **Article 14 Complaint**

(1) If the Austrian Advertising Council issues a complaint on the advertising campaign, the client/s and/or the Agency of the campaign are notified in writing to modify or discontinue the advertising campaign immediately.

(2) The complaint, as well as, in cases of Article 10, paragraph 2, the advertising carrier will be informed of the decision of the Advertising Council in writing.

(3) In case of cessation decisions of the Advertising Council, the office is to decide whether any economic risk applies in issuing such notice in consultation with the President or the Vice-President of the Council.

- a) If the office cannot identify any risk, the board is notified of the cessation decision.
- b) In case of foreseeable risk, the board is to take a decision as follows: The board is to decide with a two-thirds majority of the valid votes cast in accordance with Articles of association, § 10. This decision is without suspensive effect. Otherwise, the complaint is again examined under Article 11 et seq.

### **Article 15 Appeals**

(1) The client/s and/or the agency of the campaign may appeal against the 'cessation request' in accordance with Article 13, paragraph 1 (within two working days).

(2) The cessation request is the only valid reason for appeal. The appeal is to be issued to the Austrian Advertising Council in writing by way of submission of additional information not presented to date (e.g., market research data).

(3) The Ethics Senate of the company of self-regulation of the advertising industry, which is to be established, decides upon such appeals. Until the establishment of the Ethics Senate Article 11 applies for the decision. Article 12 and Article 13 shall apply *mutatis mutandis*.

### **Article 16 Communication of decision**

(1) The applicant and the client/s and/or the agency of the campaign, as well as the advertising carrier in cases under Article 8, are to be notified of the decision of the Austrian Advertising Council.

(2) In addition, the decision is published on the Austrian Advertising Council website under <http://www.werberat.at/>.

(3) In particular, the media and the public may also be informed of the decision of the Austrian Advertising Council.

(4) In case of competence of the Austrian Advertising Council in accordance with Article 2, paragraph 4, lit. b, the spokesperson for the Austrian Advertising Council may issue a statement on the occasion after obtaining the consent of the President of the association, which is to include a reference to the lack of competence, and may entail the Austrian Advertising Council distancing itself from the advertising campaign.

Such distancing is to be formulated taking into account the lack of competence, so as to ensure that it will not be understood as a condemnation of the advertising campaign under the Austrian Advertising Council.

## Chapter 2: Annex 4

### European Union legal framework

#### Charter of Fundamental Rights

- Article 11: Freedom of expression and information.
  - '1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers [...]'.
- Article 16: Freedom to conduct a business.
  - 'The freedom to conduct a business in accordance with Union law and national laws and practices is recognised.'
- Article 17: Right to property.
  - '2. Intellectual Property shall be protected'.
- Article 47: Right to an effective remedy and to a fair trial.
  - '1. Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article 2. Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented.'

#### European Union Directives

- Article 3 of the Infosoc Directive.
  - '(2) Member States shall provide for the exclusive right to authorise or prohibit the making available to the public, by wire or wireless means, in such a way that members of the public may access them from a place and at a time individually chosen by them: (a) for performers, of fixations of their performances; (b) for phonogram producers, of their phonograms; (c) for the producers of the first fixations of films, of the original and copies of their films; (d) for broadcasting organisations, of fixations of their broadcasts, whether these broadcasts are transmitted by wire or over the air, including by cable or satellite.'
- Article 8 of the Infosoc Directive.
  - '1. Member States shall provide appropriate sanctions and remedies in respect of infringements of the rights and obligations set out in this Directive and shall take all the measures necessary to ensure that those sanctions and remedies are applied. The sanctions thus provided for shall be effective, proportionate and dissuasive. 2. Each Member State shall take the measures necessary to ensure that rightholders whose interests are affected by an infringing activity carried out on its territory can bring an action for damages and/or apply for an injunction and, where appropriate, for the seizure of infringing material as well as of devices, products or components referred to in Article 6(2). 3. Member States shall ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.'

## Chapter 2: Annex 5

### Austrian legal framework

#### Constitutional prerequisites and fundamental rights in Austria

- Austrian Constitution.
  - Article 83.2. Right to an effective remedy and to a fair trial. 'No one shall be deprived of his lawful judge'.
- Austrian State Basic Act of 1867.
  - Article 5. 'The property is inviolable. No one may be deprived of his or her possessions, except in the cases and under the conditions provided for by law.'
  - Article 6. 'Every citizen can take in every place of the national territory domicile and residence, acquire property of any kind and freely dispose of the same feature, and exercise every line of business according to the law.'

#### Austrian Regulations

- Austrian Civil Code.
  - Article 1330. '(1) Anybody who, due to defamation, suffered real damage or loss of profit may claim compensation. The same applies if anyone is disseminating facts which jeopardise someone's reputation, gains or livelihood, the untruth of which was known or must have been known to him. In this case there is also a right to claim a revocation and the publication thereof.'
- Austrian Copyright Act.
  - Article 18a(1). 'The author has the exclusive right to make the work available to the public, by wire or wireless means, in such a way which allows members of the public to access it from a place and at a time individually chosen by them.'
  - Article 81(1) and 81(1)(a). '(1) A person who has suffered an infringement of any exclusive rights conferred by this Law, or who fears such an infringement, shall be entitled to bring proceedings for a restraining injunction. Legal proceedings may also be brought against the proprietor of a business if the infringement is committed in the course of the activities of his business by one of his employees or by a person acting under his control, or if there is a danger that such an infringement will be committed; Paragraph 81(1a) shall apply mutatis mutandis. (1a) if the person who has committed such an infringement, or by whom there is a danger of such an infringement being committed, uses the services of an intermediary for that purpose, the intermediary shall also be liable to an injunction under subparagraph (1).'
  - Article 82. '(1) If the rights to exclusion based on this law of any person are infringed, then that person can demand that the illegal situation be remedied; § 81 Section 1a applies correspondingly. (2) The injured party can demand especially that the reproductions produced or distributed in violation of the provisions of this law and those intended for illegal distribution be destroyed and that the instruments intended exclusively or predominantly for illegal reproduction (moulds, pieces, discs, film strips and similar) be disabled. (3) If the infringing products or infringing instruments designated in Section 2 contain parts, unmodified existence of which and the use of which by the defendant does not infringe on the plaintiff's right to exclusion, then the court must designate these parts in the ruling ordering the destruction or disabling. During enforcement, these parts, to the extent possible, must be preserved from the destruction or disabling if the obliged party pays in advance the associated costs. If it is evident in the enforcement proceedings, that the disabling of infringing instruments would require disproportionately great expenditures, and if these expenditures are not paid in advance by the obliged party, then the enforcement court orders, according to the agreement of the parties, the destruction of



these infringing instruments. (4) If the circumstance in violation of the law can be remedied in another way than that designated in Section 2, with no or with less destruction of value, then the injured party can only seek measures of this sort. In specific, parts cannot be destroyed merely because the statement of origin is missing or does not correspond to the law. (5) Instead of destruction of infringing products or disabling of infringing instruments, the injured party can demand that the infringing products or infringing instruments can be ceded to him by their owner in exchange for an appropriate compensation that does not exceed the manufacture costs. (6) The claim for remediation is made against the owner of the products that are subject to the measures serving to remedy the illegal circumstance. The claim can be lodged during the duration of the infringed right as long as this sort of products are in existence.'

- Article 85. '(1) If a claim is lodged for injunction or remediation or determination of the existence of non-existence of an right of exclusion based on this law or of the authorship (§ 19), then at the request of the prevailing party the court must grant authorisation to publish the ruling within a certain period at the costs of the opponent, if the prevailing party has a justified interest in this. The court must determine the type of publication. (2) The publication includes the verdict. At the request of the prevailing party, the court can however determine a content of the publication that differs from the verdict in its scope or wording or amends it. This request must be made at the latest four weeks after the entry into force of the ruling. If the request is made only after the conclusion of the oral hearings, then the court of first instance must rule on this by a resolution after the entry into force. (3) The court of first instance must determine the costs of publication at the request of the prevailing party and charge the opponent with compensation of these. (4) The publication on the basis of final ruling or another enforceable execution title must be made by the media entrepreneur without unnecessary delay.'
- Article 86. '(1) If anyone, without authorisation, a) disseminates the performance of a work of literature or of music in violation of § 66, Section 1 and 5, stores it on visual or audio storage media or copies these or distributes it in violation of § 66, Section 1 and 5 or § 69, Section 2, b) broadcasts by broadcast media, publicly reproduces or makes available to the public the performance of a work of literature or music in violation of § 66, Section 7, 69 Section 2, §§ 70, 71 or 71a, c) uses an image or an audio storage medium in a manner reserved for the producer according to §§ 74 or 76, d) uses a radio broadcast in a manner reserved to the radio entrepreneur according to § 76a, e) uses a database in a manner reserved for the producer according to § 76d, then he must make an appropriate payment, even if he is not responsible, to the injured party whose consent he would have had to procure. (2) There is no claim to this sort of payment, however, if a broadcast, a public reproduction, or an act of making available to the public is only illegal due to the fact that it has been undertaken with the aid of image- or audio storage devices or broadcasts, which according to § 50, Section 2, § 53, Section 2, § 56, Section 3, § 56b, Section 2, § 56c Section 3, no 2, § 56d, Section 1, no 2, § 66, Section 7, § 69, Section 2, §§ 70, 71, 74, 76 or 76a, Section 2 and 3 may not be used for this purpose, and if this characteristic of the image- or audio storage device or broadcast has been unknown to the user at no fault of his own. (3) If anyone uses a press release in violation of § 79, then he has to pay an appropriate payment to the news agency, even if he is not at fault.
- Article 87a. 'If anyone is obliged according to this law to make appropriate payment or appropriate remuneration, or an appropriate part of this sort of payment in compensation for damages, surrender of profits or remediation, then he must render accounts to the entitled party and have the accuracy of these accounts audited by a professional. If this results in a larger amount than from the rendering of accounts, then the costs of the audit must be paid by the party owing payment. If anyone is obliged to render accounts, then he must also provide information to the entitled party concerning all further circumstance necessary for prosecution. (2) If anyone is liable as guarantor and payer according to § 42b, Section 3, no 1, then he must also state to the entitled party the name of the person from whom he has purchased the storage material or the reproduction device, to the extent that he does not pay the remuneration. (3) Sections 1 and 2 also apply correspondingly to whomever is released from liability according to § 42b, Section 3, no 1.'
- Article 87b. '(1) If anyone distributes parts within Germany, whose right to distribution is expired due to marketing in a member country of the European Community or in a treaty country of the European

Economic Area (§ 16, Section 3), then he must provide to the entitled party on request correct and complete information on the manufacturer, content, country of origin and quantity of distributed pieces. Anyone who has the right to distribute parts in Germany at the moment of expiry has a right to information. (2) If the right to exclusion based on this law of any party has been infringed, then this party can demand information on the origin and the distribution channel of the infringing merchandise and services, as long as this would not be disproportionate in comparison to the severity of the infringement and would not violate legal obligations to confidentiality; the obligation to provide information corresponds to the infringer and to the persons who for commercial purposes 1) Have had infringing merchandise in their possession, 2) Have made use of infringing services, 3) Have provided services used for infringement of rights. (2a) The obligation to provide information according to Section 2 involves, to the extent it applies, 1) The names and addresses of manufacturers, salespersons, suppliers and other in previous possession of the merchandise or services, in addition to the commercial customer and points of sale for which they were intended, 2) The amounts of the manufactured, delivered, received or ordered merchandise and the prices, which were paid for the merchandise or services. (3) Intermediaries, according to the sense of § 81, Section 1a, must provide information to the injured party upon written and sufficiently justified request, about the identity of the infringing party (name and address) and also the information necessary for the determination of the infringing party. The justification must include especially sufficiently specific statements about the facts on which the suspicion of infringement of rights is based. The injured party must compensate the intermediary for the reasonable costs of providing information. (4) Art market professionals who have participated in a sale subject to resale right according to the sense of § 16b, Section 2, must provide to the entitled party on request correct and complete information that could be necessary to secure the payment of this sale. The claim expires if the information is not requested within a period of three years after the resale.'

- Article 87c. '(1) In relation with claims to cease and desist, for remediation, appropriate payment, compensation for damages and surrender of profits according to this law, interim injunctions may be issued both for securing the claim and for securing the evidence. (2) For securing the claims to appropriate payment, compensation for damages and surrender of profits, interim injunctions can be issued in the case of infringements of rights committed for commercial gain, if it is probable that the performance of these claims is endangered. (3) For securing of claims to cease and desist and for remediation, interim injunctions can be issued, even if the prerequisites stipulated in § 381 for the enforcement order are not met. (4) Interim injunctions according to Section 1 must be issued upon request by the endangered party without prior hearing of the opponent, if a delay would cause irremediable damage for the endangered party, or if there is a danger that evidence will be destroyed.'

## Chapter 2: Annex 6

### CJEU Case Law

PROMUSICAE CJEU RULING (29 JANUARY 2008)	
Parties	<ul style="list-style-type: none"> <li>▪ Productores de Música de España (hereinafter, <b>PROMUSICAE</b>)</li> <li>▪ Telefónica de España, S.A.U. (hereinafter, <b>TELEFONICA</b>).</li> </ul>
Facts	<ul style="list-style-type: none"> <li>▪ PROMUSICAE is a Spanish non-profit-making organisation of producers and publishers of musical and audio-visual recordings.</li> <li>▪ TELEFONICA is a Spanish commercial company whose activities include the provision of internet access services.</li> <li>▪ PROMUSICAE asked for TELEFONICA to be ordered to disclose the identities and physical addresses of certain persons to whom it provided internet access services and whose IP address and date and time of connection were known. According to PROMUSICAE, those persons used a file exchange program (peer-to-peer) and provided access in shared files of personal computers to phonograms in which the members of PROMUSICAE held the exploitation rights.</li> <li>▪ The Spanish judge ordered the preliminary measures requested by PROMUSICAE. TELEFONICA appealed against that order, arguing that under the Spanish Law implementing the E-Commerce Directive, the communication of data required by PROMUSICAE was authorised only in a criminal investigation or for the purpose of safeguarding public security and national defence, not in civil proceedings including for preliminary measures.</li> <li>▪ PROMUSICAE argued that the Spanish law implementing the E-Commerce Directive had to be interpreted in accordance with various provisions of the E-Commerce Directive, the InfoSoc Directive and the Enforcement Directive and with Articles 17.2 (<i>Right to Property</i>) and 47 (<i>Right to an effective remedy and to a fair trial</i>) of the Charter of Fundamental Rights. Such provisions did not allow a Member State to limit solely to the purposes expressly mentioned in that law the obligations to communicate the data in question.</li> </ul>
Preliminary Ruling	By its questions, the national court asked essentially whether Community law, in particular the E-Commerce Directive, the InfoSoc Directive and the Enforcement Directive read also in the light of Articles 17 ( <i>Right to Property</i> ) and 47 ( <i>Right to an effective remedy and to a fair trial</i> ) of the Charter of Fundamental Rights, must be interpreted as requiring Member States to lay down, in order to ensure effective protection of copyright, an obligation to communicate personal data in the context of civil proceedings.
CJEU Decision	<ul style="list-style-type: none"> <li>▪ The CJEU has established that the E-Commerce Directive, the InfoSoc Directive, the Electronic Communications Directive, the Enforcement Directive and the E-Commerce Directive do not require Member States to impose an obligation to communicate personal data in order to ensure effective protection of copyright in the context of civil proceedings.</li> <li>▪ However, according to the CJEU, European law requires that, when incorporating those Directives into national law, Member States must take care to rely on an interpretation of them which allows a fair balance to be struck between the various fundamental rights protected by the EU legal order, namely, between the protection of personal data on the one hand and the protection of property (including intellectual property) and the right to an effective remedy on the other hand.</li> <li>▪ The mechanisms allowing those different rights and interests to be balanced are</li> </ul>

PROMUSICAE CJEU RULING (29 JANUARY 2008)	
	<p>contained in the E-Commerce Directive, in that it provides for rules which determine in what circumstances and to what extent the processing of personal data is lawful and what safeguards must be provided for, and in the E-Commerce Directive, the InfoSoc Directive and the Enforcement Directive which reserve the cases in which the measures adopted to protect the rights they regulate affect the protection of personal data. They further result from the adoption by Member States of national provisions transposing those Directives and their application by national authorities.</p> <ul style="list-style-type: none"> <li>Furthermore, when implementing those Directives, the Authorities and Courts of the Member States must not only interpret their national laws in a manner consistent with those Directives but also make sure that they do not rely on an interpretation of them which would be in conflict with the fundamental rights mentioned above or with the other general principles of EU law, such as the principle of proportionality.</li> </ul>
SVENSSON CJEU RULING (13 FEBRUARY 2014)	
Parties	<ul style="list-style-type: none"> <li>Nils Svensson</li> <li>Sten Sjögren</li> <li>Madelaine Sahlman</li> <li>Pia Gadd</li> </ul> <p>(hereinafter, jointly referred to as the <b>Applicants</b>)</p> <ul style="list-style-type: none"> <li>Retriever Sverige AB. (hereinafter, <b>RETRIEVER</b>).</li> </ul>
Facts	<ul style="list-style-type: none"> <li>The Applicants, all journalists, are the authors of press articles that were published in the <i>Göteborgs-Posten</i> newspaper and on the <i>Göteborgs-Posten</i> website.</li> <li>RETRIEVER is a Swedish company that operates a website that provides its clients with lists of clickable Internet links to articles published by other websites. The articles linked by RETRIEVER's website were freely accessible on the <i>Göteborgs-Posten</i> newspaper's website.</li> <li>The Applicants brought an action against RETRIEVER before the Stockholm District Court (<i>Stockholms tingsrätt</i>) in order to obtain compensation on the ground that RETRIEVER had made use, without their authorisation, of certain articles written by them by making them available to its clients.</li> <li>By judgment of 11 June 2010, the Stockholm District Court rejected the Applicants' action. The Applicants then brought an appeal against this judgment before the Svea Court of Appeal (<i>Svea hovrätt</i>). The Applicants claimed before this court, inter alia, that RETRIEVER had infringed their exclusive exploitation right to make their respective works available to the public, in that as a result of the services offered on its website, RETRIEVER's clients had access to the Applicants' works.</li> <li>RETRIEVER opposed alleging that the provision of lists of internet links to works communicated to the public on other websites does not constitute an act liable to affect the copyright in those works. It did not carry out any transmission of any protected work as its services are limited to indicating to its clients the websites on which the works that are of interest to them could be found.</li> </ul>
Preliminary Ruling	<p>By its questions, the national court decided to refer to the CJEU for a preliminary ruling asking, inter alia:</p> <ul style="list-style-type: none"> <li>Whether Article 3.1 of the Infosoc Directive must be interpreted as meaning that the</li> </ul>

SVENSSON CJEU RULING (13 FEBRUARY 2014)	
	<p>provision on a website of clickable links to protected works available on another website constitutes an act of communication to the public as referred to in that provision, where, on that other site, the works concerned are freely accessible.</p> <ul style="list-style-type: none"> <li>▪ Whether it could be possible for a Member State to give wider protection to authors' exclusive right by enabling communication to the public to cover a greater range of acts than provided for in Article 3.1 of the Infosoc Directive.</li> </ul>
CJEU Decision	<ul style="list-style-type: none"> <li>▪ The CJEU has established that, as per Article 3.1 of the Infosoc Directive, in a case where all the users of another website to whom the works at issue have been communicated by means of a clickable link could access those works directly on the website on which they were initially communicated, without the involvement of the manager of that other website, the users of the site managed by the latter must be deemed to be potential recipients of the initial communication and, therefore, as being part of the public taken into account by the copyright holders when they authorised the initial communication. Therefore, since there is no new public, the authorisation of the copyright holders is not required for a communication to the public.</li> <li>▪ The CJEU also stated that, if the Member States were to be afforded the possibility of laying down that the concept of communication to the public includes a wider range of activities than those referred to in Article 3.1 of the Infosoc Directive, the functioning of the internal market would be bound to be adversely affected. Therefore, the mentioned article must be interpreted as precluding a Member State from giving wider protection to copyright holders by laying down that the concept of communication to the public includes a wider range of activities than those referred to in that provision.</li> </ul>

KINO.TO CJEU RULING (27 MARCH 2014)	
Parties	<ul style="list-style-type: none"> <li>UPC Telekabel Wien GmbH (hereinafter, <b>TELEKABEL</b>)</li> <li>Constantin Film Verleih GmbH</li> <li>Wega Filmproduktionsgesellschaft mbH</li> </ul> <p>(hereinafter, jointly referred to as the <b>Production Companies</b>).</p>
Facts	<ul style="list-style-type: none"> <li>TELEKABEL is an Austrian internet service provider.</li> <li>The Production Companies are an Austrian and a German film production companies.</li> <li>Having established that a website was offering, without their agreement, either a download or 'streaming' of some of the films that the Production Companies had produced, the Production Companies referred the matter to the court responsible for hearing applications for interim measures with a view to obtaining, on the basis of Article 81(1)(a) of the Austrian Copyright Act an order enjoining TELEKABEL to block the access of its customers to the website at issue (i.e., kino.to), inasmuch as that site makes available to the public without their consent cinematographic works over which they hold a right related to copyright.</li> <li>By order of 13 May 2011, the Commercial Court of Vienna (<i>Handelsgericht Wien</i>) prohibited TELEKABEL from providing its customers with access to <i>kino.to</i> by blocking that website's domain name and current IP address and any other IP addresses of that website of which TELEKABEL might be aware.</li> <li>TELEKABEL appealed to the Austrian Supreme Court (<i>Oberster Gerichtshof</i>) and alleged, inter alia, that its services could not be considered to be used to infringe a copyright or related right within the meaning of Article 8.3 of the Infosoc Directive because it did not have any business relationship with the operators of the website at issue and it was not established that its own customers acted unlawfully. In any event, TELEKABEL claimed that the various blocking measures that may be introduced can all be technically circumvented and that some of them are excessively costly, which would be contrary to the rights envisaged in the Charter of Fundamental Rights.</li> </ul>
Preliminary Ruling	<p>The national court decided to refer to the CJEU for a preliminary ruling asking, inter alia:</p> <ul style="list-style-type: none"> <li>Whether it is compatible with Union law, in particular with the necessary balance between the parties' fundamental rights, to prohibit in general terms an internet access provider from allowing its customers access to a certain website (thus without ordering specific measures) as long as the material available on that website is provided exclusively or predominantly without the rightholder's consent, if the access provider can avoid incurring coercive penalties for breach of the prohibition by showing that it had nevertheless taken all reasonable measures?</li> <li>If the answer to the previous question is in the negative: Whether it is compatible with Union law, in particular with the necessary balance between the parties' fundamental rights, to require an internet access provider to take specific measures to make it more difficult for its customers to access a website containing material that is made available unlawfully if those measures require not inconsiderable costs and can easily be circumvented without any special technical knowledge?</li> </ul>
CJEU Decision	<ul style="list-style-type: none"> <li>The CJEU has established that where several fundamental rights are at issue, the Member States must, when transposing a directive, ensure that they rely on an interpretation of the directive which allows a fair balance to be struck between the applicable fundamental rights protected by the European Union legal order.</li> </ul>

#### KINO.TO CJEU RULING (27 MARCH 2014)

- Furthermore, when implementing the measures transposing that directive, the authorities and courts of the Member States must not only interpret their national law in a manner consistent with that directive but also ensure that they do not rely on an interpretation of it that would be in conflict with those fundamental rights or with the other general principles of EU law, such as the principle of proportionality.
- In the case at issue, the CJEU observed that an injunction such as that at issue in the main proceedings, taken on the basis of Article 8.3 of the Infosoc Directive, makes it necessary to strike a balance, primarily, between (i) copyrights and related rights, which are intellectual property and are therefore protected under Article 17.2 of the Charter of Fundamental Rights, (ii) the freedom to conduct a business, which economic agents such as internet service providers enjoy under Article 16 of the Charter of Fundamental Rights, and (iii) the freedom of information of internet users, whose protection is ensured by Article 11 of the Charter of Fundamental Rights.



## **CHAPTER 3: UK GOOD PRACTICE PRINCIPLES FOR THE TRADING OF DIGITAL DISPLAY ADVERTISING**



## Chapter 3: Glossary of terms

For the purposes of this Chapter 3, the following definitions apply:

- **Charter of Fundamental Rights**: the Charter of Fundamental Rights of the European Union<sup>156</sup>.
- **CV tool**: as defined by the GPPs, is the content verification technology product or service that may block or report the serving of display advertising onto destinations that have been defined as inappropriate to the advertising campaign by the advertiser or the agency.
- **Data Protection Directive**: the Directive of 24 October 1995 on Data Protection<sup>157</sup>. At the moment of the drafting of this Study, the Data Protection Directive was in force. This Directive **has been repealed** by the General Data Protection Regulation on May 2016.
- **Display Advertising**: as defined by the GPPs, is the display of visual files including images, flash and video provided by buyers to sellers on a digital media property (or other connected application) when an internet user visits the digital media property.
- **DTSG**: the Digital Trading Standards Group, the standards group within JICWEBS aimed at protecting brand safety and preventing advertising misplacement.
- **CJEU**: the Court of Justice of the European Union.
- **Enforcement Directive**: the Directive of 29 April 2004 on the Enforcement of Intellectual Property Rights<sup>158</sup>.
- **European Union Directives**: collectively, the Enforcement Directive, the InfoSoc Directive and the Data Protection Directive.
- **GPPs**: the good practice principles for the trading of digital display advertising drafted by DTSG and adopted by JICWEBS<sup>159</sup>.
- **HRA**: the UK Human Rights Act of 1998 which incorporated in UK legislation the articles and rights of the European Convention of Human Rights<sup>160</sup>.
- **IAB UK**: the Internet Advertising Bureau UK, a trade association related to online advertising<sup>161</sup>.
- **IASH**: the Internet Advertising Sales House, a group created by JICWEBS in order to help advertisers regarding the placement of their advertising.
- **InfoSoc Directive**: the Directive of 22 May 2001 on Information Society<sup>162</sup>.
- **Inventory**: the space on a website which is used for placing advertising.
- **IPO**: the UK Intellectual Property Office, a public body promoting the protection of intellectual property rights in the UK<sup>163</sup>.
- **IWL**: the Infringing Website List created by PIPCU to identify likely infringing websites<sup>164</sup>.

<sup>156</sup> Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, pp. 391-407.

<sup>157</sup> Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, pp. 31-50.

<sup>158</sup> Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, OJ L 157 of 30.04.2004.

<sup>159</sup> The Good Practice Principles are provided in Annex 1 of this Chapter 3.

<sup>160</sup> <http://www.legislation.gov.uk/ukpga/1998/42/contents>.

<sup>161</sup> <https://www.iabuk.net/>.

<sup>162</sup> Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167, 22.06.2001 pp. 10-19.

<sup>163</sup> <https://www.gov.uk/government/organisations/intellectual-property-office>.

<sup>164</sup> <https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/pipcu/Pages/Operation-creative.aspx>.

- **JICWEBS**: the Joint Industry Committee for Web Standards, an organisation created by the UK media industry<sup>165</sup>.
- **Kino.to CJEU Ruling**: the judgment of 27/03/2014, C-314/12, UPC Telekabel Wien, EU:C:2014:192<sup>166</sup>.
- **Likely Infringing Website**: a digital media property likely infringing intellectual property rights including, trade marks, design rights, copyrights and rights related to copyright.
- **PIPCU**: the Police Intellectual Property Crime Unit, a special unit created within the City of London Police dedicated exclusively to fighting infringements of intellectual property rights<sup>167</sup>.
- **Progress Report**: Report issued in February 2015 by DTSG to summarise the progress of the GPPs.
- **Promusicae CJEU Ruling**: the judgment of 29/01/2008, C-275/06, Promusicae, EU:C:2008:54<sup>168</sup>.
- **Svensson CJEU Ruling**: the judgment of 13/02/2014, C-466/12, Svensson and Others, EU:C:2014:76<sup>169</sup>.
- **UK**: the United Kingdom.
- **UK Copyright, Designs and Patents Act**: the Act of the Parliament of the UK of 1988 on Copyright, Designs and Patents<sup>170</sup>.
- **UK Data Protection Act**: the Act of the Parliament of the UK of 1998 on Data Protection<sup>171</sup>.
- **UK Registered Designs Act**: the Act of the Parliament of the UK of 1949 on Registered Designs<sup>172</sup>.
- **UK Regulations**: collectively, the UK Copyright, Designs and Patents Act, the UK Trade Marks Act, the UK Registered Designs Act and the UK Data Protection Act.
- **UK Trade Marks Act**: the Act of the Parliament of the UK of 1994 on Trade Marks<sup>173</sup>.
- **VCP**: Means 'voluntary collaboration practices' developed by industry, public bodies and/or third parties such as non-governmental organisations and then adhered to by the respective industry in addressing infringements of trade mark rights, design rights, copyright and rights related to copyright over the internet. Here, with regard to the present Chapter 3 'VCP' shall comprise in particular the GPPs.
- **Verification Provider**: the independent and registered auditor in charge of investigating and becoming aware that every signatory of the GPPs complies with them.

<sup>165</sup> <http://www.iicwebs.org/>.

<sup>166</sup> <http://curia.europa.eu/juris/document/document.jsf?jsessionid=9ea7d0f130d5682c6360d7a642ab82679809c8f7b53e.e34KaxilC3eQc4OLaxqMbN4ObNmPe0?text=&docid=149924&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=141830>.

<sup>167</sup> <https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/pipcu/pages/default.aspx>.

<sup>168</sup> <http://curia.europa.eu/juris/liste.jsf?language=en&num=C-275/06>.

<sup>169</sup> <http://curia.europa.eu/juris/liste.jsf?num=C-466/12>.

<sup>170</sup> <http://www.legislation.gov.uk/ukpga/1988/48/contents>.

<sup>171</sup> <http://www.legislation.gov.uk/ukpga/1998/29/contents>.

<sup>172</sup> <http://www.legislation.gov.uk/ukpga/Geo6/12-13-14/88/contents>.

<sup>173</sup> <http://www.legislation.gov.uk/ukpga/1994/26/contents>.

## Chapter 3: Structure and content

This Chapter 3 analyses in depth the application of the good practice principles (GPPs), by assessing the following elements:

- Role of the parties involved in the implementation of the GPPs.
- Analysis of the duties and procedures prescribed by the GPPs.
- Coexistence of the measures established under the GPPs with European Union and the UK legal frameworks and related case law.
- Role of technologies used in implementing the duties and procedures envisaged by the GPPs.
- Costs assumed by the parties involved in the implementation of the GPPs.
- Role of educational activities of the parties involved in the promotion of the GPPs.
- Effectiveness of the measures established by the GPPs.

This Chapter 3 initially involved exhaustive desk research to identify the stakeholders involved in the GPPs. A sample of them were then contacted and some agreed to be interviewed for the purposes of this Chapter 3, whilst others declined the invitation to participate.

The statements contained in the Chapter 3 on the stakeholders' position regarding the GPPs and their day-to-day procedure are based on the feedback and supporting documentation provided by those stakeholders that agreed to participate in this Chapter 3.

Although the GPPs do not contain a specific definition of advertising misplacement and they refer to online advertising misplacement in general, which could include the placement of display advertising in media properties offering inappropriate or illegal content of any type (e.g., pornographic content, content showing violence, terrorist related content), this Chapter 3 focuses exclusively on the placement of display advertising on 'likely infringing websites', that is media properties likely infringing intellectual property rights, including, trade marks, design rights, copyrights and rights related to copyright.

## 1. Introduction

The good practice principles (GPPs) outline six (6) commitments for all businesses involved in the buying, selling or facilitating of display advertising and their main aim is to set out good practice for reducing the amount of advertising that appears on websites that offer illegal content by introducing transparency to the market. Indeed, as stated by IAB UK, the GPPs provide those in the display advertising chain with a framework that clarifies rights and responsibilities within the increasingly complex process that is advertising trading<sup>174</sup>.

The GPPs evolve the principles of the IASH system, an initiative launched in 2005 with the aim of minimising the misplacement of display advertising. IASH comprised twenty seven (27) advertising networks<sup>175</sup> within the UK, whose compliance was independently verified, and it was designed for the advertising network and sales house model<sup>176</sup>. Under its code of conduct dated June 2011, IASH provided the main stakeholders involved in the trading of display advertising at that time with good practices regarding the types of inventory which could or could not be traded. Moreover, when buying display advertising in the UK, buyers were encouraged to work with businesses whose compliance with the IASH code of conduct had been independently verified.

Due to the development of the display advertising market, the IASH code of conduct turned out not to be flexible enough to allow its application to new trading models and technologies which have led to a more automated system of delivering and targeting advertising. As a consequence, in 2011 the IASH and its code of conduct were revoked with the intention of creating a new system to cover the latest industry developments.

In December 2013 the GPPs drafted by DTSG were published after having been reviewed and approved by JICWEBS. The GPPs are built upon the aims of the IASH code of conduct and replace it with standards of practice to reduce the risk of unsafe advertising online in line with both current and future technology and trading methods.

In February 2015, the progress report issued by DTSG outlined that signatories of the GPPs represented over two thirds (2/3) of the applicable UK display advertising market by the end of 2014 and that it was expected that this will grow to between eighty per cent (80 %) and ninety per cent (90 %) by the end of 2015. In this regard, IAB UK when interviewed for the purposes of this Chapter 3 has indicated that one (1) of the strengths of the GPPs is that they have the full support of the online advertising industry.

The GPPs were updated by DTSG in June 2015 to address reporting and timing issues, which were not envisaged by its initial version. As mentioned by JICWEBS, as the whole industry is constantly evolving, the idea is to keep the GPPs up-to-date and to improve them through feedback from industry.

As far as the placing of advertising on likely infringing websites is concerned, the IWL launched by PIPCU through the Operation Creative campaign since 2013 has had a strong impact on the GPPs. The IWL provides a list of likely infringing websites; it can be used by advertising businesses as an inappropriate schedule within their trading agreements, in line with the requirements envisaged by the GPPs.

The GPPs are divided into the following main parts:

- Section 1 – UK GPPs: This section contains (i) an explanation regarding the background of the GPPs, (ii) a definition of digital advertising trading and (iii) the six (6) commitments forming the GPPs.
- Section 2 – Compliance and Enforcement: This section contains (i) JICWEBS' requirements for selecting verification providers, (ii) the review of signatory's policies by verification providers, (iii) reporting issues<sup>177</sup> and (iv) timing issues<sup>178</sup>.
- Appendix 1 – Definitions: This appendix contains a list of definitions of the most relevant stakeholders acting in the display advertising arena.

<sup>174</sup> <http://www.iabuk.net/blog/the-iab-believes-in-brand-safety-online>.

<sup>175</sup> IAB, December 2013, 'Factsheet: Minimising the risk of advertising misplacement', page 1 <http://www.iabuk.net/sites/default/files/IAB%20Factsheet%20-%20Minimising%20the%20risk%20of%20ad%20misplacement.pdf>.

<sup>176</sup> A detailed explanation on the evolution of the trading of display advertising can be found in Annex 2 of this Chapter 3.

<sup>177</sup> Included following the amendment of the Good Practice Principles in 2015.

<sup>178</sup> Included following the amendment of the Good Practice Principles in 2015.

The GPPs' objectives are as follows, as explained by the different stakeholders interviewed for the purposes of this Chapter 3:

- Reducing significantly the risk of the misplacement of display advertising.
- Protecting brands, by preventing damages to advertisers caused by associations with inappropriate content.
- Protecting the integrity of digital advertising.
- Fighting against inappropriate or illegal online content or services, including content or services breaching intellectual property rights, by preventing websites offering such content/services from benefitting from advertising revenues.
- Creating a safer environment for consumers so that they avoid websites containing inappropriate or illegal content of any type.

The GPPs are a voluntary system of self-regulation to which signatories may freely adhere. Being a private arrangement, the GPPs leave their signatories free to implement the corresponding measures for voluntary cooperation in order to fight against advertising misplacement.

As explained by JICWEBS when interviewed for the purposes of this Chapter 3, the GPPs are an industry self-regulation tool that is meant to be a framework for increasing transparency and trust between trading parties rather than an instrument for imposing obligations. JICWEBS stressed the fact that the GPPs are an optional and voluntary code of best practice that coexists in parallel with the legal framework without impacting it. According to JICWEBS, the voluntary nature of the GPPs implies the following benefits:

- The GPPs are flexible and therefore they can be evolved.
- Partners are encouraged to work together, transparently and for their benefit.
- Application of the GPPs does not rely on legal enforcement, which is costly and time consuming.

As far as the IPO is concerned, the fact that the GPPs are a voluntary scheme introduced by the industry rather than being enforced by public authorities helps to make it more readily acceptable.

Finally, according to the feedback provided by an association of rightholders interviewed, voluntary codes of conduct such as the GPPs are very helpful. To their mind, inter alia, they have given rightholders a better understanding of how the online advertising industry works and they have helped advertisers to take the infringement of intellectual property rights more seriously. However, the mentioned association of rightholders has stressed that the problem of self-regulatory instruments such as the GPPs is that they are based entirely on goodwill and since they are not subject to regulatory control they do not completely guarantee that their signatories will comply with the obligations foreseen by them.

## 2. Stakeholders and third parties

The GPPs have been adopted under the umbrella of JICWEBS, a joint industry committee made up of trade bodies from the UK media industry. They were drafted by DTSG, the JICWEBS' standards group in charge of brand safety and they were ratified and approved by JICWEBS.

Buyers, sellers and facilitators<sup>179</sup> operating in the digital advertising market can be signatories of the GPPs. They need to be audited by verification providers, who will check whether they meet the GPPs' standards. Subsequent to approval from the verification providers, JICWEBS may award signatories with the GPPs' compliance seal and compliance certificate.

In contrast to the other VCPs examined in this study, rightholders do not play an active role in the GPPs but they may benefit from them given that the GPPs may lead to the reduction of the advertising revenues achieved by likely infringing websites and to better protection of the rightholder's brand image.

Neither public authorities nor civil society participate actively in the GPPs and they were not involved in their drafting.

This Section of Chapter 3 explains in detail the specific roles regarding the GPPs played by JICWEBS, DTSG, the GPPs' signatories, verification providers and rightholders and why public authorities and civil society do not participate in it.

### 2.1. Role of JICWEBS and DTSG

#### 2.1.1. JICWEBS

The UK media industry created JICWEBS as a joint industry committee whose main objective is to promote and to enhance best practices relating to the trading of online advertising as well as industry standards.

JICWEBS' members represent sellers, buyers and facilitators from the following UK industry bodies:

- Internet Society of British Advertisers<sup>180</sup>.
- IAB UK.
- Institute of Practitioners in Advertising<sup>181</sup>.
- Association of Online Publishers<sup>182</sup>.
- News Media Association<sup>183</sup>.

JICWEBS is composed of various standards groups through which it seeks guidance and recommendations from the advertising industry. Each of these standards groups focusses on a specific topic relating to the trading of online advertising and proposes principles to JICWEBS for consideration. The members of JICWEBS' standards groups encompass all areas of the online advertising system to ensure that all interests are represented. At the date of drafting this Chapter 3, the following standards groups are operative within JICWEBS:

- Digital Content Measurement Group. Deals with audio visual measurement.
- DTSG. Deals with brand safety.
- Internet Technical Group. Deals with industry raised technical issues.

---

<sup>179</sup> A detailed explanation on the evolution of the trading of display advertising can be found in Annex 2 of this Chapter 3.

<sup>180</sup> <http://www.isba.org.uk/>.

<sup>181</sup> <http://www.ipa.co.uk/>.

<sup>182</sup> <http://www.ukaop.org/>.

<sup>183</sup> <http://www.newsmediauk.org/>.



When the idea of drafting the GPPs was proposed, JICWEBS' main role was to engage with all parts of the industry in order to build consensus to make sure the GPPs were signed by the industry, as explained by JICWEBS for the purposes of this Chapter 3. In other words, JICWEBS was responsible for getting agreements on the GPPs so that everybody supported the initiative.

In November 2013, when the DTSG proposed the GPPs to JICWEBS, JICWEBS reviewed them and, with some changes, adopted them as the industry agreed standards.

Presently JICWEBS is in charge of performing the following tasks regarding the GPPs:

- Hosting the GPPs.
- Approving verification providers that will verify compliance by signatories with the GPPs.
- Conducting independent reviews and appeals.
- Reviewing the signatories' submissions and issuance of the DTSG seal and certificate of compliance.
- Publishing the list of signatories of the GPPs through its website.

### 2.1.2. Role of DTSG

Among JICWEBS' standards groups, DTSG is the one that deals with brand safety and that reports and makes proposals to JICWEBS on this matter. It was created in 2012 with the aim of building on the accomplishments of the IASH and to reflect the evolving digital display market.

It is made up of representatives from across the digital advertising market, including buyers, sellers and facilitators.

DTSG's main purposes are the following:

- To protect brand safety.
- To diminish the risk of misplacement of display advertising.
- To secure a safer environment for the placement of display advertising.

In compliance with its main purpose, in November 2013 DTSG proposed the GPPs to JICWEBS as a set of industry wide standards aimed at reducing the risk of misplacement of display advertising. DTSG also updated the GPPs in June 2015 to take into account reporting and timing considerations.

## 2.2. Role of signatories

As indicated by Section 1.1. of the GPPs ('Introduction'), the GPPs cover commitments for all businesses involved in the buying, selling or facilitating of display advertising. Also, the progress report highlights the fact that the GPPs involve a broad cross-section of the different trading models today<sup>184</sup>.

Accordingly, any business pertaining to the three (3) following general categories of players involved in the trading of online advertising may become a signatory of the GPPs<sup>185</sup>:

- Sellers. As defined by Appendix 1 of the GPPs, sellers are businesses that sell directly or that are responsible for placing display advertising on digital media properties. This category of signatory includes, without limitation, publishers<sup>186</sup>, supply side platforms or advertising networks.
- Buyers. As defined by Appendix 1 of the GPPs, buyers are businesses that buy display advertising from sellers. This category of signatory includes, without limitation, advertisers or agencies, ad trading desks, sales houses or demand side platforms.

<sup>184</sup> Progress report, page 9. <http://www.jicwebs.org/agreed-principles/latest-news/170-minimising-the-risk-of-digital-display-advertising-misplacement>.

<sup>185</sup> The list of the current signatories of the GPPs can be found in Annex 2 of this Chapter 3.

<sup>186</sup> Website providing content for internet users.

- **Facilitators.** As defined by Appendix 1 of the GPPs, facilitators are businesses that provide a technology platform with the primary purposes of brokering for compensation, the placement of display advertising between buyers and sellers. This category of signatory includes, without limitation, advertising exchanges.

For the avoidance of doubt, sellers, buyers and facilitators involved in the trading of online advertising do not have to previously become members of an association represented in JICWEBS to become signatories of the GPPs.

In general terms, the GPPs signatories' role consists of implementing advertising misplacement minimisation policies covering their online trading activities and to have these policies verified by verification providers.

The duties relating to signatories envisaged by the GPPs are structured as follows:

- Common duties applicable to all categories of signatories (e.g., to implement methods for minimising advertising misplacement; to have advertising misplacement policies verified by verification providers).
- Common duties applicable only to buyers and sellers (e.g., to understand any contractual consequences should they fail to monitor the process or to respond appropriately to advertising misplacement via take down).
- Duties applicable exclusively to sellers (e.g., to confirm the specific provisions they apply to minimise the risk of advertising misplacement; to explain the processes that form the basis of specific provisions and/or the reasonable endeavours).

As far as facilitators are concerned, although they are bound by the duties applicable to all categories of signatories, the GPPs do not foresee additional duties that would apply specifically to them and not to the other categories of signatories. Only Note B of the GPPs refers explicitly to them as it provides that facilitators shall abide by the criteria selected by buyers and sellers for minimising advertising misplacement in the interface that they provide to their users.

## 2.3. Role of Verification Providers

Signatories of the GPPs are subject to an independent audit to demonstrate that they meet the standards laid down by the GPPs.

Verification providers carry out an independent assessment and issue a report on whether signatories have implemented the policies for minimising advertising misplacement in compliance with the GPPs. In practice, the verification procedure does not extend to testing the effectiveness of any processes or controls, being limited to ascertain whether signatories have implemented policies for minimising advertising misplacement rather than verifying whether the policies are actually effective.

Generally, verification providers tailor their services to the specific business of each category of signatory and the documentation they have in place with their trading partners.

The criteria employed by JICWEBS for the selection of verification providers are provided for under Section 2.1 of the GPPs ('Selection of Verification Provider'). Accordingly, verification providers should be registered auditors and members of either:

- The Institute of Chartered Accountants in England and Wales.
- The Institute of Chartered Accountants of Scotland.
- The Institute of Chartered Accountants in Ireland.
- The Association of Chartered Certified Accountants.

In exceptional circumstances, signatories of the GPPs may apply to JICWEBS in order that they may use a verification provider who is not a member of one (1) of the aforementioned bodies setting out the exceptional condition of such a request and provided that the verification provider (i) is independent of and/or not owned by a signatory, DTSG business or relevant trade association and (ii) maintains business operations in the UK. As explained by JICWEBS, to the date there have been no applications to use verification providers not belonging to the mentioned bodies.

Thus far, the organisations below have been approved by JICWEBS as verification providers to carry out independent verification in relation to the GPPs:

- ABC.
- BPA Worldwide.
- ePrivacy GmbH.

Verification providers are subject to annual review by JICWEBS.

Documentation regarding certification requirements and the review decisions relating to verification providers are made public.

## 2.4. Role of rightholders

As confirmed by JICWEBS, one (1) of the aims of the GPPs is to reduce the placement of display advertising on likely infringing websites, as explained under Section 1 of this Chapter 3 ('Introduction'). Therefore, despite the fact that the GPPs themselves do not specifically contain a definition of 'advertising misplacement', according to the feedback provided by JICWEBS and other interviewed stakeholders it could be understood that display advertising carried out on likely infringing websites is among the activities that could be considered, inter alia, as advertising misplacement under the GPPs.

As such, from an intellectual property perspective, rightholders in the context of the GPPs are entities holding any intellectual property rights, including trade mark rights, design rights, copyright and rights related to copyright, whose rights may be infringed by likely infringing websites.

As explained by an association of rightholders interviewed for the purposes of this Chapter 3, they participated together with other rightholders and certain advertisers in a consultation process carried out by DTSG prior to the drafting of the GPPs.

However, as confirmed by another association of rightholders interviewed for this Chapter 3, currently rightholders do not directly play an active role in it, although they obviously benefit from it given that the GPPs may lead to a reduction in the revenues of likely infringing websites and to better protection of the rightholder's brand image.

## 2.5. Role of public authorities

The GPPs are a private initiative carried out by the advertising industry with no mandatory power and no governmental involvement.

Although PIPCU participated in a consultation process relating to the GPPs organised by JICWEBS prior to the drafting of the GPPs, neither PIPCU nor other public authorities were involved specifically in the drafting of the GPPs and nowadays they are not involved in its implementation.

In contrast, public authorities play an essential role regarding the IWL, an initiative that runs in parallel to the GPPs. The list is held by PIPCU, a national police unit within the City of London Police, which is operationally independent and was launched in September 2013 by the UK Intellectual Property Office, a public body dealing with the protection of intellectual property rights in the UK. Further information on the IWL is provided under Section 3.2 of this Chapter 3 ('Definition of Likely Infringing Websites').

## 2.6. Role of civil society

Although one (1) of the main objectives of the GPPs when minimising advertising misplacement is to protect brand reputation so consumers do not make a wrong association between illegal content on a website and the advertising campaign of a well-known brand displayed on the latter, the fact is that no consumer association has been involved in the drafting and application of the GPPs, as explained by JICWEBS interviewed for the purposes of this Chapter 3.

In relation to this Chapter 3, several UK consumer associations have been contacted in order to gather their opinion about the GPPs and all of them stated that they were not involved in the enforcement of intellectual property rights and therefore were not able to contribute.

## 3. Duties and procedures

This Section summarises the duties and procedures resulting from the GPPs.

### 3.1. Scope of application of the GPPs

#### 3.1.1. Territorial scope

Section 1.1 of the GPPs ('Introduction') establishes that the GPPs apply to businesses with UK presence, targeting UK audiences or users.

The FAQs relating to DTSG<sup>187</sup> confirm this scope, despite the fact that many advertising trading businesses operate at scale and therefore will also apply good practice globally and in line with other initiatives.

#### 3.1.2. Material scope

No restriction is established by the GPPs as to the categories of advertising that may be subject to them. Therefore, the GPPs apply to the misplacement of any kind of advertising, without limitation.

Furthermore, the GPPs contain commitments for all the businesses involved in the buying, selling or facilitating of display advertising that have subscribed to JICWEBS and have signed the GPPs. As already mentioned under Section 2.2 of this Chapter 3 ('Role of signatories'), the three (3) categories of players are very broad and may include a large variety of business models (e.g., publishers, supply side platforms, advertising exchanges, sales houses, advertising networks, demand side platforms, independent trading desks, agency trading desks). Notwithstanding the foregoing, facilitators providing stand alone advertising serving services are excluded from the scope of application of the GPPs, as explicitly established under Section 1.1 of the GPPs ('Introduction'). As explained by JICWEBS, these facilitators are publishers that sell their own inventory without allowing other third parties to do so.

### 3.2. Definition of Likely Infringing Websites

Identifying likely infringing websites is difficult for the digital advertising industry. Moreover, advertising businesses had different interpretations of what constituted a likely infringing website and therefore there was no accepted authoritative definition, so they were unable to instruct their trading partners accordingly<sup>188</sup>.

All the stakeholders interviewed for the purposes of this Chapter 3, including, without limitation, JICWEBS, the IPO, IAB UK and an association of rightholders stated that in relation to the GPPs, since the summer of 2014 it is easier to define in practice likely infringing websites as this circumstance is now determined by PIPCU's IWL. Indeed, although the GPPs and the IWL are two (2) different initiatives, they run in parallel and signatories of the GPPs are encouraged to use the IWL as a blacklist of websites or an inappropriate schedule where display advertising should not be placed.

Regarding the origin of the IWL, JICWEBS has explained that before the GPPs were published rightholders asked them to set forth a list outlining likely infringing websites with the aim of enabling all the players of the online marketing industry to stop trading with those websites. For instance, the advertising industry had difficulty in identifying likely infringing websites because of a lack of common understanding of what a likely infringing website actually was, how it behaved or what it looked like. As JICWEBS was not prepared to draft such a list on likely

---

<sup>187</sup> <http://www.jicwebs.org/digital-trading-standards-group-good-practice-principles/dtsg-information-and-forms/166-digital-trading-standards-group-faqs>.

<sup>188</sup> IAB, 2 September 2015, 'Factsheet: Copyright and Brand Safety' <http://www.iabuk.net/sites/default/files/UPDATED%20IAB%20Factsheet%20September%202015%20-%20Copyright%20and%20Brand%20Safety.pdf>.

infringing websites, given that they are not legal experts<sup>189</sup>, JICWEBS encouraged (i) rightholders to work with the City of London Police to elaborate the mentioned list and (ii) the advertising industry to be aware of the list.

Following JICWEBS' suggestion, PIPCU was launched in September 2013. It is a unit within the City of London Police, operationally independent and funded by the IPO. Its purpose is to protect UK industries from intellectual property infringements taking place in the online world.

In the summer of 2014, as a consequence of the collaboration between rightholders, the advertising industry trade bodies and PIPCU, the IWL was created as an online register of likely infringing websites accessible by the advertising industry. The PIPCU's IWL contains an up-to-date list of likely infringing websites identified by the creative industries and verified by PIPCU, so that advertisers, agencies and other intermediaries can cease advertising placement on these websites.

The IWL was subject to a three (3) months pilot period within which a total of sixty one (61) likely infringing websites which were evidenced as obtaining benefits from online advertising were involved. The procedure for identifying such websites during the pilot programme has afterwards been adopted by the definitive IWL.

Access to the IWL is totally voluntary. Therefore, the advertising industry is neither obliged to access it nor legally required to prevent the placement of advertising on the websites that are included in it. However, as explained by all stakeholders interviewed for the purposes of this Chapter 3, in practice the IWL is widely used by the advertising industry.

As indicated by PIPCU, the process which leads to the inclusion of a likely infringing website under the IWL is the following:

- Rightholders identify and report to PIPCU websites that they believe are likely infringing websites, providing detailed evidence indicating how these websites are involved in intellectual property rights infringements.
- Thereafter, officers from PIPCU evaluate the reported websites and check whether they may be considered likely infringing websites. The specific procedure applied to this end is confidential, as confirmed by the IPO for the purposes of this Chapter 3.
- When it has been confirmed by PIPCU that a website is a likely infringing website, PIPCU contacts the operator of the website, who is given the opportunity to engage with the police and to correct its behaviour, if any, and to begin operating legitimately.
- In cases where the operator would not be willing to engage with PIPCU, other options may be used, such as contacting the domain registrar in order to seek suspension of the likely infringing website and ensure the inclusion thereof in the IWL.

IAB UK has stressed the fact that the advertising industry cannot make the decision as to what websites are likely infringing websites. The IWL provides an authoritative list of likely infringing websites. IAB UK believes the GPPs provide a platform for the UK's digital advertising industry to help tackle the infringement of intellectual property rights by enabling the use of the IWL<sup>190</sup>.

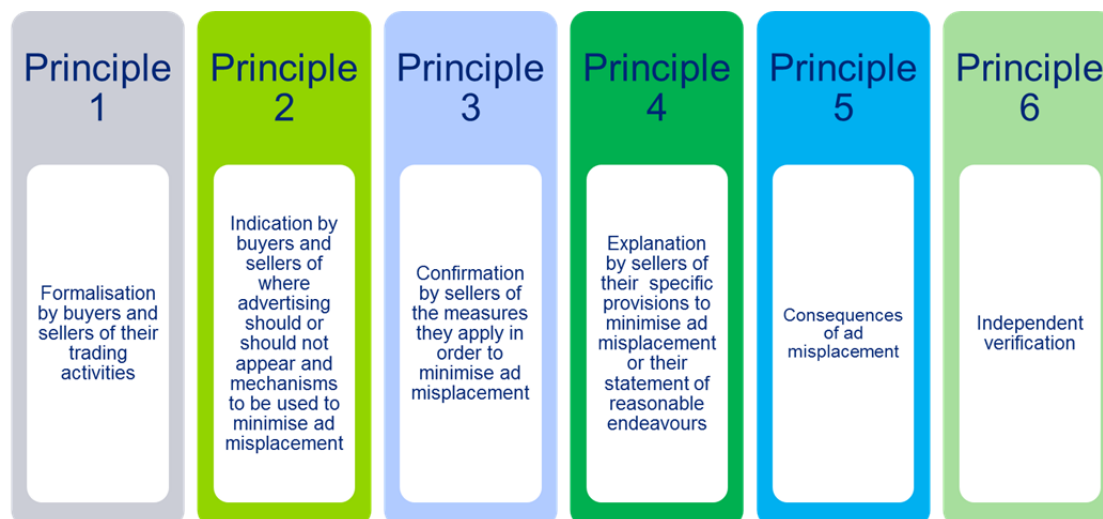
---

<sup>189</sup> The GPPs expressly state under their Note C that neither DTSG nor JICWEBS will draw up, maintain or approve any suggested criteria or scheduling or any form of inappropriate destinations.

<sup>190</sup> <http://www.iabuk.net/blog/the-iab-believes-in-brand-safety-online#11PdMy35Y2OI2ITP>.

### 3.3. The GPPs

This Section analyses the six (6) following principles that form the GPPs as well as the compliance and enforcement procedures relating to it:



#### 3.3.1. Principles addressed to the signatories

Section 1.3 of the GPPs ('The Principles') establishes that signatories have to comply with the six (6) following principles or commitments:

- Principle 1 – Formalisation by buyers and sellers of their trading activities.

Through this first principle, signatories to the GPPs commit themselves to establish and to enforce clear contractual terms for the buying and selling of display advertising.

The transaction between a buyer and a seller has to be performed through one (1) of the following means:

- A so-called primary agreement. A sample primary agreement is available on JICWEBS' website<sup>191</sup>.
- A contract including specific terms and policies that cover substantive points regarding the methods for minimising advertising misplacement.

As it may be understood from signatories' certificates available on JICWEBS' website<sup>192</sup>, in practice trading transactions are governed through different types of contractual instruments, such as, without limitation, services agreements or the so-called 'insertion orders'. Those instruments contain references to terms and conditions for display advertising (either directly or indirectly, by providing the URL where they are located) and both constitute the entire agreement for display advertising transactions.

- Principle 2 - Indication by buyers and sellers of where advertising should or should not appear and mechanisms to be used to minimise advertising misplacement.

Through this second principle, buyers and sellers commit themselves to specifically refer to their intention as to where advertising should or should not appear either (i) under the primary agreement subscribed to by them or (ii) under the specific terms and conditions relating to advertising misplacement included in the contract to be entered into by them.

<sup>191</sup> <http://www.jicwebs.org/images/Sample%20Primary%20Agreement.pdf>.

<sup>192</sup> <http://www.jicwebs.org/digital-trading-standards-group-good-practice-principles/dtsg-information-and-forms/151-dtsgsignatories>.



To ensure compliance thereof, they have to use one (1) or both of the following means:

- Appropriate/inappropriate schedules.

These schedules have to be agreed between buyers and sellers pursuant to the primary agreement or the specific terms and conditions that are applicable to their relationship.

They have to outline the URLs or applications that are considered appropriate or inappropriate. As already explained under Section 3.2 of this Chapter 3 ('Definition of Likely Infringing Websites'), regarding likely infringing websites, the IWL is frequently used as an inappropriate schedule for the purposes of this second principle.

In cases where the parties subscribe to a primary agreement, the sample primary agreement that is available on JICWEBS' website envisages that they have to state in it the policy for appropriate and/or inappropriate schedules and to explain how this is agreed by the recipient, pre-delivery of advertising.

- A CV tool independently certified to JICWEBS' standards<sup>193</sup>.

CV tools are technological instruments which may be used by signatories of the GPPs to assess a website's content resolving if it is appropriate or inappropriate for an advertiser.

In cases where the parties subscribe to a primary agreement, the sample primary agreement that is available on JICWEBS' website envisages that they have to specify in it which tool they intend to use and whether it has been certified by an independent third party to JICWEBS' standards. Furthermore, an explanation of the configuration and use of the CV tool is required, for example, if it blocks and/or monitors advertising delivery and if it applies to all advertising campaigns or only to specific ones.

Indirectly, this second principle also contains a duty addressed to facilitators, as it is indicated under its Note B that facilitators' user interfaces have to be consistent with the criteria chosen by sellers and buyers concerning the placement of the underlying advertising.

Additionally, Note C of the GPPs - which is also linked to this second principle - expressly states that neither JICWEBS nor DTSG have any role in suggesting or approving any criteria, scheduling or deciding any form of inappropriate destinations. It is envisaged that such criteria have to be established by buyers. They may be included in the primary agreements buyers enter into with sellers or in other industry information, as required by buyers, provided it is accompanied by a disclaimer excluding the responsibility of JICWEBS and DTSG with regard to such sources or information.

As it may be understood from signatories' certificates available on JICWEBS' website<sup>194</sup>, in practice targeting instructions which may include appropriate and inappropriate schedules and/or specify the use of CV tools are either established directly in the contractual instruments governing trading parties' relationship or agreed specifically on a campaign by campaign basis.

- Principle 3 – Confirmation by sellers of the measures they apply in order to minimise advertising misplacement.

Through this third principle, sellers commit themselves to confirm to buyers the specific provisions that they apply to minimise the risk of advertising misplacement, regardless of whether they source inventory directly or indirectly.

In cases where sellers do not provide the aforementioned specific provisions, at least they have to carry out a statement of reasonable endeavours.

As it may be understood from signatories' certificates available on JICWEBS' website<sup>195</sup>, in practice most sellers have internally adopted brand safety policies to comply with this principle, a copy of which is provided to buyers and is available on their websites.

<sup>193</sup> A more detailed explanation relating to CV tools is included as Annex 4 to this Chapter 3.

<sup>194</sup> <http://www.jicwebs.org/digital-trading-standards-group-good-practice-principles/dtsg-information-and-forms/151-dtsgsignatories>.

<sup>195</sup> <http://www.jicwebs.org/digital-trading-standards-group-good-practice-principles/dtsg-information-and-forms/151-dtsgsignatories>.

- Principle 4 – Explanation by sellers of their specific provisions to minimise advertising misplacement or their statement of reasonable endeavours.

This fourth principle is closely related to the third one. It establishes that in addition to the confirmation by sellers of the specific provisions they apply for minimising advertising misplacement or the provision of the statement of reasonable endeavours, sellers commit themselves to be able to provide an explanation to buyers on the process or processes supporting such measures.

As it may be understood from signatories' certificates available in JICWEBS' website<sup>196</sup>, in practice this explanation is generally included by sellers under their internal brand safety policies.

- Principle 5 – Consequences of advertising misplacement.

Through this fifth principle, buyers and sellers, in the event of a failure in the monitoring of the advertising misplacing process, commit themselves to (i) understand the contractual consequences of the event and (ii) to take down the advertising misplaced.

As it may be understood from signatories' certificates available on JICWEBS' website<sup>197</sup>, in practice sellers' internal brand safety policies generally establish that the removal of misplaced advertising has to take place in a short period of time (i.e., normally it ranges between certain business hours and one (1) working day). In certain cases, sellers require buyers to provide them with supporting documentation evidencing the misplacement (e.g., screenshots). Normally, it is established that the consequences of advertising misplacement are evaluated and agreed with buyers on a case by case basis prior to the occurrence of a misplacement (e.g., under specific insertion orders negotiated with each buyer).

- Principle 6 – Independent verification.

Through this sixth principle, signatories commit themselves to have their advertising misplacement minimisation policies and procedures verified by a Verification Provider approved by JICWEBS.

Such verification procedures have to be performed within six (6) months of the signatory joining the GPPs and thereafter every year.

The functioning, timing and reporting linked to the verification procedure provided for by this sixth principle are detailed by Section 2 of the GPPs ('Compliance and Enforcement'), analysed in the following Section of this Chapter 3.

### 3.3.2. Compliance and enforcement

As stated previously in this Chapter 3, signatories of the GPPs have to implement policies and processes to minimise the risk of advertising misplacement. According to the sixth principle of the GPPs and as developed in its Section 2 ('Compliance and Enforcement'), these policies and processes have to be verified by an independent third party in charge of confirming that both comply with the requirements established by the GPPs.

This Section analyses in detail the procedure to be followed by buyers, sellers and facilitators in order to adhere to the GPPs and to receive the corresponding seal and certification of fulfilment, which may be summarised as follows:



<sup>196</sup> <http://www.jicwebs.org/digital-trading-standards-group-good-practice-principles/dtsg-information-and-forms/151-dtsgsignatories>.

<sup>197</sup> <http://www.jicwebs.org/digital-trading-standards-group-good-practice-principles/dtsg-information-and-forms/151-dtsgsignatories>.

### 3.2.2.1. Adherence to the GPPs

Buyers, sellers and facilitators that wish to apply for certification of their business activities against JICWEBS' GPPs have to adhere to the GPPs as formal signatories. To that end, they have to pay an annual fee.

### 3.2.2.2. Independent policy verification process

The verification process to be undergone by signatories is described under Section 2.2 of the GPPs ('Independent Policy Verification Process') as well as in JICWEBS' so-called 'Guide to Verification'<sup>198</sup>.

In order to prove their compliance with the GPPs, signatories have to provide verification providers with all information which might be important regarding their advertising misplacement policies. According to Section 2.2 of the GPPs ('Independent Policy Verification Process') and JICWEBS' 'Guide to Verification' this information may include:

- Contract terms and policies relating to the transactions of advertising.
- A statement of reasonable endeavours applied to minimise the risk of advertising misplacement.
- Internal policies, procedures and controls relating to the placement of advertising, such as the details regarding the use of CV tools and appropriate/inappropriate schedules, names and training of personnel with enforcement responsibility and details of the enforcement process.

As an example, the verification process carried out by ABC, one (1) of JICWEBS' approved verification providers, includes the following steps:

- Signatories have to send a confirmation form to ABC which schedules its verification work. The form covers the details of the signatory and its product, the relevant staff members of the signatory to be contacted (including the contact details), verification fees and signatories' signature confirming consent for ABC to proceed with the verification process.
- ABC's audit team sends to signatories a declaration form for them to complete.
- Signatories have to return the complete declaration form to ABC with attachments/evidence.
- ABC arranges a meeting in the signatories' offices and, in advance of the meeting, sets out what will be covered in terms of paperwork, policies and/or a walk-through of relevant systems and procedures.
- After the meeting, there may be further e-mail correspondence or calls for ABC to complete its review.
- ABC sends signatories a management letter outlining its findings and recommendations, if any.
- Signatories have to provide ABC with evidence that recommendations made by ABC have been implemented.

At the end of the verification process, verification providers provide a written report of their findings to the respective signatory and, if they determine that the latter's policies are compliant with the GPPs, a verification submission form has to be sent to JICWEBS to consider if a certificate and seal will be issued.

It is clarified at the end of Section 2.2 of the GPPs ('Independent Policy Verification Process') concerning effectiveness of the verification process that the verification does not test the effectiveness of any processes, procedures or controls for advertising misplacement but is limited solely to check whether signatories have implemented policies for minimising advertising misplacement in compliance with the GPPs. Therefore, as indicated by JICWEBS interviewed for the purposes of this Chapter 3, the compliance certificate obtained by a signatory only verifies its policies regarding minimising advertising misplacement, but not its effectiveness.

---

<sup>198</sup> [http://www.abc.org.uk/Documents/Guides/Guide%20To%20DTSG%20Verification\\_Final\\_January2014.pdf](http://www.abc.org.uk/Documents/Guides/Guide%20To%20DTSG%20Verification_Final_January2014.pdf).

### 3.2.2.3. Reporting

Section 2.3 of the GPPs ('Reporting'), contains a description of the procedure for the results of the independent verification procedure to be submitted to JICWEBS (verification submission procedure) as well as the certificates and seals granted by JICWEBS to signatories that have successfully completed the verification procedure.

To initiate the reporting procedure, signatories and verification providers have to jointly complete and submit a verification submission form to JICWEBS. However, it does not have to be physically signed by signatories if, instead, they instruct verification providers to submit it to JICWEBS. In this case, a copy of the signatory's instruction (which could be an e-mail) along with the verification submission form should be submitted to JICWEBS. It is established by JICWEBS that the instruction has to include the following statement: 'I confirm that the corporate information and description of compliance with the GPPs on the attached JICWEBS/DTSG Submission Form is factually accurate and agree to my verification provider submitting the form to JICWEBS'.

A standard verification submission form is available on JICWEBS' website<sup>199</sup>. This standard form is structured in three (3) parts:

- Corporate information relating to the signatory subject to the verification as well as to the verification process itself (i.e., company name and UK address; URL; main contact and e-mail address; business/brand verified; business type; month of verification and signed date) and corporate information relating to the Verification Provider (i.e., company name and UK address; URL and main contact and e-mail address).
- Statement of Verification Provider. Through this statement, the Verification Provider acknowledges signatories' compliance with the GPPs.
- Findings. This section has to include a description of the fulfilment by the signatory of each of the six (6) commitments provided for by the GPPs, backed with the corresponding information, documentation, policies and processes. As indicated by Section 2.3.1 of the GPPs ('Verification submission'), as a minimum the information provided has to be in the form of a summary and/or extracts from relevant documents along with easily accessible links to the documents themselves.

It is specified on JICWEBS' website that the form has to be sent both in Word and PDF format to the following e-mail address of JICWEBS: [info@jicwebs.org](mailto:info@jicwebs.org).

Upon receipt of a verification submission form, JICWEBS reviews it and, subject to the approval thereof, it issues to signatories:

- A seal of compliance. The seal references the relevant Verification Provider. This is normally in the form of the Verification Provider's logo incorporated into the seal. However, if the signatory wishes, the Verification Provider may, instead of the logo, either state the company name or use the statement 'JICWEBS approved VP'<sup>200</sup>. Generally, seals look as follows:



<sup>199</sup> <http://www.jicwebs.org/digital-trading-standards-group-good-practice-principles/dtsg-information-and-forms/163-dtsg-verification-submission-form>.

<sup>200</sup> <http://www.jicwebs.org/digital-trading-standards-group-good-practice-principles/dtsg-information-and-forms/167-use-of-verification-provider-s-name-and-logo>.

- A certificate of compliance. The certificate comprises the following items:
  - Seal.
  - Signatory's name and address.
  - Signatory's logo (optional).
  - Business/brand verified.
  - Service provided.
  - Month of verification.
  - Compliance findings against the GPPs.
  - Verification Provider's name and address.
  - Statement of the Verification Provider.

Although not expressly provided for by the GPPs, JICWEBS has explained for the purposes of this Chapter 3 that in cases where signatories are not awarded with the seal and the certificate they have the right to appeal such a decision.

Certificates and seals of compliance with the GPPs are publicly available on JICWEBS' website<sup>201</sup>.

#### 3.2.2.4. *Timing*

Section 2.4 of the GPPs ('Timing'), deals with the relevant timeframes to be considered relating to the GPPs. Thus, it establishes the following timing considerations:

- Seals.
  - First seal. The term for signatories to obtain the first seal is fixed at six (6) months from their adherence to the GPPs<sup>202</sup>.
  - Subsequent seals. Subsequent seals have to be issued before the expiration of the current seal. However, if a subsequent submission is made earlier, the new seal can be valid for twelve (12) months provided that the month of verification is within the timeframe indicated below under 'verification work'<sup>203</sup>.
- Verification submission. The submission to JICWEBS of the verification form made jointly by a signatory and a Verification Provider has to take place at least (2) weeks prior to the end of the month in which the seal has to be issued.

In the event the signatory estimates that it will not be able to comply with the aforementioned term, the signatory has to formally request to JICWEBS an extension of this period, explaining the reasons of the delay and suggesting a revised date. Subsequent to this, JICWEBS should inform the signatory about its resolution.

In cases where JICWEBS grants the signatory with a delayed submission date, the signatory will be de-listed from the GPPs when the normal expected seal issue date has passed and re-listed once the seal is issued by JICWEBS.

- Verification work. The verification work has to be completed not earlier than four (4) months before the month in which the seal is issued<sup>204</sup>.

<sup>201</sup> <http://www.jicwebs.org/digital-trading-standards-group-good-practice-principles/dtsg-information-and-forms/151-dtsgsignatories>.

<sup>202</sup> E.g., in cases where adherence would have taken place in May 2015, the first seal should be issued by JICWEBS by end November 2015.

<sup>203</sup> E.g., in cases where the current seal would be valid until July 2015, if verification work is done in March 2015 and submission is made in April 2015, then the new seal would be valid until July 2016.

<sup>204</sup> E.g., if the verification work has been completed in March 2015, then the seal must be issued no later than July 2015.

## 4. Coexistence of the measures set forth under the GPPs with European Union and the UK legal frameworks and related case law

Section 4 of this Chapter 3 ('Coexistence of the measures set forth under the GPPs with the European Union and UK legal frameworks and related case law') summarises the European Union and UK legal frameworks and related case law that may have an impact on the practical application of the GPPs.

The considerations included in this Section are based upon the following legal sources:

- Fundamental rights in the European Union (Section 4.1 of this Chapter 3 ('Charter of Fundamental Rights')).
- European Union Directives (Section 4.2 of this Chapter 3 ('European Union Directives')).
- Fundamental rights in the UK (Section 4.3 of this Chapter 3 ('Fundamental rights in the UK'))<sup>205</sup>.
- UK Regulations (Section 4.4 of this Chapter 3 ('UK Regulations')).

### 4.1. Charter of Fundamental Rights

As a preliminary comment, it must be taken into consideration that in the negotiations of the Lisbon Treaty<sup>206</sup>, the UK secured a protocol to the Treaty<sup>207</sup> relating to the application of the Charter of Fundamental Rights. Namely, this protocol in its Article 1.1 states that the 'Charter does not extend the ability of the Court of Justice of the European Union or any court or tribunal of [...] the United Kingdom, to find that the laws, regulations or administrative provisions, practices or actions of [...] the United Kingdom are inconsistent with the fundamental rights, freedoms and principles it reaffirms'.

Having said that, confusion exists about the applicability of the Charter of Fundamental Rights to the UK<sup>208</sup>. On the one hand, certain sectors believe that the mentioned protocol implies an opt-out that excludes the application of the Charter of Fundamental Rights to the UK and, on the other hand, others understand that the protocol has a mere interpretative nature and that it has limited or no legal effect at all.

Given that it may not be ruled out that the Charter of Fundamental Rights applies to the UK, it has been considered necessary to analyse, as further developed under Section 4.5 of Chapter 3 ('Analysis of the GPPs in relation to the European Union and UK legal frameworks and case law'), whether certain fundamental rights provided for by the Charter of Fundamental Rights may have an impact on certain duties envisaged by the GPPs.

In this context, in cases where the Charter of Fundamental Rights would be considered applicable in the UK, the following fundamental rights established by the mentioned Charter may eventually have an impact on the GPPs<sup>209</sup>:

- Article 8: 'Protection of personal data'. This right generally serves to protect the self-determination right of an individual regarding the use of personal data related to themselves.
- Article 16: 'Freedom to conduct a business'. This right includes the freedom to undertake an economic or commercial activity and the freedom of contract.

<sup>205</sup> Unlike where it has been highlighted in the remaining Chapters of this study regarding other VCPs, no constitutional provisions are analysed herein due to the absence of a written constitution in the UK.

<sup>206</sup> Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, OJ C 306, 17.12.2007, pp. 1–271.

<sup>207</sup> Protocol (No 30) to the Treaty of Lisbon on the application of the Charter of Fundamental Rights of the European Union to Poland and to the United Kingdom, OJ C 306, 17.12.2007, pp. 1–271.

<sup>208</sup> See, for example, the document entitled 'The application of the EU Charter of Fundamental Rights in the UK: a state of confusion', issued by the House of Commons' European Scrutiny Committee (26 March 2014).

<sup>209</sup> See complete wording in Annex 5 of this Chapter 3.



- Article 17: 'Right to property'. This right stipulates that no one shall be deprived of their possessions except in the public interest and in cases and under conditions provided for by law, subject to fair compensation being paid in good time for their loss. Protection of intellectual property (including literary and artistic property, as well as patent and trade mark rights and associated rights) is explicitly covered by this right.
- Article 47: 'Right to an effective remedy and to a fair trial'. This right establishes that everyone whose rights and freedoms guaranteed by the law are violated has the right to an effective remedy before a tribunal. It includes the right to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law.

## 4.2. European Union Directives

As the GPPs intend to fight, inter alia, against the infringement of intellectual property rights, the following provisions of the European Union Directives<sup>210</sup> are to some extent related to it given that they establish that rightholders have the exclusive right of making available works to the public and they deal with the measures/sanctions applicable to the infringement of intellectual property rights:

- Article 3 of the Infosoc Directive. This Article envisages that rightholders have the exclusive right to authorise or to prohibit the making available to the public of their works from a place and at a time individually chosen by that public.
- Article 8 of the InfoSoc Directive. This Article envisages that the sanctions applicable to the infringement of copyright or related rights be effective, proportionate and dissuasive. Likewise rightholders should be able to apply for injunctions against intermediaries whose services are used by a third party to infringe a copyright or related rights.
- Article 3 of the Enforcement Directive. This Article envisages that the measures and remedies aimed at ensuring the enforcement of intellectual property rights be fair, equitable, not unnecessarily complicated or costly, or entail unreasonable time-limits or unwarranted delays, they should also be effective, proportionate, dissuasive, and applied in such a manner as to avoid the creation of barriers to legitimate trade and to provide for safeguards against their abuse.
- Article 9.1 of the Enforcement Directive. This Article envisages that upon the request of rightholders in the event of alleged infringements of intellectual property rights, judicial authorities may issue a number of measures.
- Article 15 of the Enforcement Directive. This Article envisages that in legal proceedings instituted for infringement of intellectual property rights judicial authorities may order at the request of the applicant and at the expense of the infringer appropriate measures for the dissemination of the information concerning the decision.
- Article 17.a of the Enforcement Directive. This Article promotes the development by trade or by professional associations or organisations of codes of conduct aimed at contributing towards the enforcement of intellectual property rights.

In addition, from a data protection perspective, Article 2.a of the Data Protection Directive has to be considered given that it provides a definition of what is to be considered personal data.

In contrast with the views expressed in other remaining chapters of this study regarding other VCPs (for example, regarding the French Charter for the Fight against the Sale of Counterfeit Goods on the Internet between Intellectual Property Rightholders and e-Commerce Platforms), Article 15 of the E-Commerce Directive would not be relevant in the case at issue given that no intermediaries providing information society services, such as hosting services providers, are involved in the GPPs. Although the GPPs envisage the use of CV tools and/or appropriate/inappropriate schedules, which indirectly imply certain monitoring duties, these duties are addressed

<sup>210</sup> See complete wording in Annex 5 of this Chapter 3.



to the parties intervening in the trading of display advertising and not to intermediaries providing information society services.

The fundamental rights mentioned under Section 4.1 of this Chapter 3 ('Charter of Fundamental Rights') and the aforementioned Directives, have been interpreted, inter alia, in the following cases<sup>211</sup>:

- Promusicae CJEU Ruling

This Ruling establishes that the protection of intellectual property rights is not of a higher order than other fundamental rights; meaning that the protection of intellectual property rights does not prevail over other rights, such as the freedom to conduct a business.

- Kino.to CJEU Ruling

Amongst others, this Ruling establishes that where several fundamental rights protected by the European Union legal order are at issue, such legal order and the interpretation thereof shall ensure a fair balance between the various rights at stake and shall avoid conflicts with other general principles of EU law, such as the principle of proportionality. Namely, in its Ruling the CJEU highlights the need to strike a balance between (a) copyrights and related rights, which are intellectual property and are therefore protected by Article 17.2 of the Charter of Fundamental Rights, (2) the freedom to conduct a business, which economic agents enjoy under Article 16 of the Charter of Fundamental Rights and (3) the freedom of information of internet users, whose protection is ensured by Article 11 of the Charter of Fundamental Rights.

- Svensson CJEU Ruling

This Ruling establishes that the provision of clickable links to protected works constitutes an act of communication to the public. To the extent the links are directed at a 'new public', namely, a public that was not taken into account by copyright holders at the time of the initial communication, the authorisation of copyright holders would be required. This would be the case, for example, in relation to a protected work no longer available to the public on the website on which it was initially communicated or where it is henceforth available on that website but only to a restricted public, while being accessible on another website through a clickable link. In light of this, it may be considered that intellectual property infringing websites make available protected works to a new public as they are addressed to a public that was not taken into account by the copyright holders, in which case the owners of websites would require copyright holders' consent to perform such a communication legally.

### 4.3. Fundamental rights in the UK

Certain fundamental rights set forth by the HRA<sup>212</sup>, which implements in the UK the European Convention on Human Rights<sup>213</sup>, may have an impact on the measures envisaged by the GPPs.

The HRA places an obligation on public authorities to act at all times in a way which is compatible with the Convention Rights as set out in the European Convention on Human Rights (Introductory Text, Article 6 ('Acts of Public Authorities')). The limitation of the HRA's applicability to 'public authorities' does, however, mean that private parties are generally not able to take proceedings against each other on the basis of Convention grounds alone. Therefore it would appear that the HRA only applies to actions brought against public authorities with which a vertical relationship can be shown. However, the House of Lords, in its decision of 6 May 2004 under Case *Campbell v Mirror Group Newspapers Ltd* found that while the HRA cannot create new causes of action between individuals, 'if there is a relevant cause of action, the court as a public authority must act compatibly with both parties' Convention rights'. In addition, the HRA states that Courts must interpret primary and secondary legislation in a way which is compatible with Convention rights (Introductory Text, Article 3 ('Interpretation of

---

<sup>211</sup> See detailed description in Annex 7 of this Chapter 3.

<sup>212</sup> See complete wording in Annex 6 of this Chapter 3. The House of Lords, in its decision of 6 May 2004 under case *Campbell v Mirror Group Newspapers Ltd* found that while the HRA cannot create new causes of action between individuals, 'if there is a relevant cause of action, the court as a public authority must act compatibly with both parties' Convention rights'. Therefore, it is to be understood that the HRA, which implements in the UK the European Convention on Human Rights, is also applicable to private disputes.

<sup>213</sup> [http://www.echr.coe.int/Documents/Convention\\_ENG.pdf](http://www.echr.coe.int/Documents/Convention_ENG.pdf).

legislation')). Even though the common law is not specified in this section, a judge presiding over a dispute between private parties is often encouraged to interpret a rule of common law in accordance with Convention rights. Therefore, it may be understood that the HRA, which implements in the UK the European Convention on Human Rights, is also in some ways applicable to private disputes.

That being said, the following fundamental rights established by the HRA may be affected by the GPPs:

- Right to the protection of property (Schedule 1, Part II, Article 1 ('Protection of property')).
- Right to an effective remedy and to a fair trial (Schedule 1, Part I, Article 6 ('Right to a fair trial'))<sup>214</sup>.

Furthermore, the freedom to conduct a business may also have an impact on the GPPs. As has been highlighted by the European Union Fundamental Rights Agency<sup>215</sup>, UK statutory law makes no explicit reference to the freedom to conduct business. Despite this, as the mentioned agency indicates, related rights are firmly rooted in the UK legal system, namely:

- The right of property (Schedule 1, Part II, Article 1 of the HRA ('Protection of property')), which has already been mentioned above.
- The freedom of contract, which stems from the UK the Companies Act of 2006<sup>216</sup>, the Competition Act of 1998<sup>217</sup> and the Enterprise Act of 2002<sup>218</sup>.

Regarding the right to the protection of personal data, which may also ultimately impact the GPPs, the HRA makes no explicit reference to it, but it is related to the right to respect for private and family life, set forth by Schedule 1, Part I, Article 8 of the HRA ('Right to respect for private and family life'). In addition, the UK has extended the law relating to breach of confidence, developed under the HRA, to protect privacy rights.

Although these fundamental rights have been considered by UK courts, there are no decisions directly applicable to the GPPs. Below are examples of relevant cases in other areas:

- Decision of the High Court of 17 July 2014 under Case *Comic Enterprise Ltd. V Twentieth Century Fox Film Corp*

Under this decision, which deals with the infringement of the claimant's trade mark by a media company, the High Court weighed up competing fundamental rights, including the fundamental right to property of the claimant.

- Decision of the High Court of 2 March 2015 under Case *Warner-Lambert Co LLC v Actavis Group PTC EHF*

This decision deals with the patent protection for a second medical use of a drug. The National Health Service in England was ordered to issue guidance to clinical commissioning groups in relation to prescribing and dispensing that drug so as to ensure that it should only be prescribed for a specific treatment and that generic versions thereof could only be prescribed for the treatment of other conditions. The freedom to conduct a business is specifically mentioned in the context of which fundamental rights are engaged by the matter at hand. The Court concluded that the order made is proportionate and will not create barriers to legitimate trade.

- Decision of the House of Lords of 6 May 2004 under Case *Campbell v Mirror Group Newspapers Ltd*

In this decision the UK's Highest Court stated that the requirement to give effect to Article 8 of the European Convention on Human Rights ('Right to respect for private and family life')<sup>219</sup> had led to the formation of a new cause of action that was described as wrongful disclosure/misuse of private information.

<sup>214</sup> Although the right to an effective remedy is not expressly mentioned by this Article, it would appear to fall within its remit.

<sup>215</sup> European Union Agency for Fundamental Rights 'Freedom to conduct a business: exploring the dimensions of a fundamental right', August 2015 ([http://fra.europa.eu/sites/default/files/fra\\_uploads/fra-2015-freedom-conduct-business\\_en.pdf](http://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-freedom-conduct-business_en.pdf)).

<sup>216</sup> [http://www.legislation.gov.uk/ukpga/2006/46/pdfs/ukpga\\_20060046\\_en.pdf](http://www.legislation.gov.uk/ukpga/2006/46/pdfs/ukpga_20060046_en.pdf).

<sup>217</sup> <http://www.legislation.gov.uk/ukpga/1998/41/contents>.

<sup>218</sup> <http://www.legislation.gov.uk/ukpga/2002/40/contents>.

<sup>219</sup> [http://www.echr.coe.int/Documents/Convention\\_ENG.pdf](http://www.echr.coe.int/Documents/Convention_ENG.pdf).

## 4.4. UK Regulations

*Inter alia*, the following provisions of UK Regulations are related to the GPPs<sup>220</sup>, to the extent that they deal with the protection of intellectual property rights and their enforcement:

- Section 16 of the UK Copyright, Designs and Patents Act. This section deals with the rights restricted by copyright in a work, which include the communication of the work to the public.
- Section 20 of the UK Copyright, Designs and Patents Act. This section deals with the infringement of copyright by communication to the public.
- Section 96 of the UK Copyright, Designs and Patents Act. This section refers in general to infringement actions available to copyright owners.
- Section 97 of the UK Copyright, Designs and Patents Act. This section deals with damages in infringement actions.
- Section 97.a of the UK Copyright, Designs and Patents Act. This section deals with injunctions against service providers that have actual knowledge of another person using their service to infringe copyright.
- Section 107 of the UK Copyright, Designs and Patents Act. This section deals with criminal liability for making or dealing with infringing articles.
- Section 226 of the UK Copyright, Designs and Patents Act. This section deals with the primary infringement of design rights.
- Section 227 of the UK Copyright, Designs and Patents Act. This section deals with the secondary infringement of unregistered design rights.
- Section 229 of the UK Copyright, Designs and Patents Act. This section deals with the rights and remedies of unregistered design right owners.
- Section 7 of the UK Registered Designs Act. This section deals with the rights conferred by registered designs.
- Section 7A of the UK Registered Designs Act. This section deals with the infringement of registered designs.
- Section 24A of the UK Registered Designs Act. This section deals with the infringement actions available to registered design owners and the relief that may be ordered by the court.
- Section 9 of the UK Trade Marks Act. This section deals with the rights conferred by registered trade marks.
- Section 10 of the UK Trade Marks Act. This section deals with the infringement of registered trade marks.
- Section 14 of the UK Trade Marks Act. This section deals with the infringement actions available to trade mark owners and the relief that may be ordered by the court.
- Section 15 of the UK Trade Marks Act. This section deals with orders for erasure, removal or obliteration from any goods, material or articles infringing trade mark rights.
- Section 16 of the UK Trade Marks Act. This section deals with orders for delivery up of goods, material or articles infringing trade mark rights.

Furthermore, in relation to the protection of personal data, Section 1 of the UK Data Protection Act ('Basic interpretative provisions') would be relevant as it contains a definition of 'personal data'.

---

<sup>220</sup> See complete wording in Annex 6 of this Chapter 3.

As explained by the IPO for the purposes of this Chapter 3, to date there have not been any judicial decisions in the UK relating to the GPPs or to the IWL. However, the IPO has stressed that although not linked to VCPs, UK Courts have made a number of general rulings that impact on rightholders' efforts in blocking access to websites that host copyright and trade mark infringing content including, inter alia, in the following cases:

- Decision of the High Court of Justice of 23 October 2014 under Case *1967 Ltd & Ors v British Sky Broadcasting Ltd & Ors*

In this decision the High Court of Justice granted an injunction to a number of record companies by issuing a blocking order against certain internet services providers. Specifically, they were asked to take measures to block and/or impede access to twenty one (21) websites which provided access to commercially available music without authorisation from copyright owners. The reason why this ruling is important in relation to the GPPs is because the High Court clarified that the target websites were infringing copyright based mainly on the following criteria: (i) they indexed torrent files; (ii) they provided an organised directory of content which users could search and browse; (iii) having selected the content, users could download it either from the target websites or other websites to which target websites provided links. According to the High Court, the role of the target websites was not passive as they intervened in an active and highly material way so as to enable users to access and download content in an easy and convenient way. Furthermore, as was the case in the Svensson CJEU ruling, the High Court considered that the target websites were communicating the content to a new public which had not been considered by rightholders when they authorised the original communication.

- Decision of the High Court of 17 October 2014 under Case *Cartier International AG & Ors v British Sky Broadcasting Limited*

In this decision the High Court ruled on blocking orders targeted at websites infringing trade marks by selling counterfeit goods. The High Court identified four cumulative conditions for a blocking order to be granted, namely: (i) internet services providers have to be 'intermediaries' under Article 11 of the Enforcement Directive; (ii) users/operators of the website must be infringing the trade mark; (iii) users/operators had to be using internet services providers' services to infringe and (iv) the internet services providers had to have actual knowledge of the infringement. With respect to condition (ii), the High Court ruled that there would be a trade mark infringement in such cases where target websites would advertise or offer goods to UK consumers by using identical signs in respect of identical goods without the consent of the relevant rightholder provided such activities would be liable adversely to affect the original function of the trade marks.

#### 4.5. Analysis of the GPPs in relation to the European Union and the UK legal frameworks and case law

In light of the European Union and the UK legal frameworks and related case law discussed in the preceding Sections of this Chapter 3, it appears that certain duties envisaged by the GPPs may be considered inconsistent with certain fundamental rights, as mentioned below.

Pursuant to the *Promusicae* and to the *Kino.to* CJEU Rulings the protection of intellectual property rights should not be understood as being of a higher interest than other fundamental rights. Therefore, during the subsequent analysis the impact of the following fundamental rights on the GPPs will be reviewed in detail:

- Freedom to conduct a business of owners of likely infringing websites and signatories of the GPPs.
- Right to an effective remedy and to a fair trial of owners of likely infringing websites.
- Right to the protection of personal data of the signatories involved in the GPPs and of the owners of likely infringing websites.

#### 4.5.1. Coexistence of the GPPs with the freedom to conduct a business of owners of likely infringing websites and of signatories of the GPPs

The freedom to conduct a business is enshrined in Article 16 of the Charter of Fundamental Rights ('Freedom to conduct a business'). UK statutory law makes no explicit reference to it but as previously indicated it is covered by the right to property envisaged by Schedule 1, Part II, Article 1 of the HRA ('Protection of property') and by the freedom to contract which may be inferred from the Companies Act of 2006<sup>221</sup>, the Competition Act of 1998<sup>222</sup> and the Enterprise Act of 2002<sup>223</sup>.

This freedom includes, without limitation, the right for any business to be able to freely use within the limits of its liability for its own acts the economic, technical and financial resources available to it. It has been pointed out in the literature<sup>224</sup> that this freedom recognises the right to economic initiative, its main function being to foster social, economic and political integration and to protect consumers.

In relation to the GPPs, both signatories to the GPPs as well as owners of likely infringing websites are economic agents and, therefore, enjoy the freedom to conduct a business granted by the Charter of Fundamental Rights and by the HRA, the Companies Act of 2006<sup>225</sup>, the Competition Act of 1998<sup>226</sup> and the Enterprise Act of 2002<sup>227</sup>.

##### 4.5.1.1. Coexistence of the GPPs with the freedom to conduct a business of owners of likely infringing websites

By means of the freedom to conduct a business, owners of likely infringing websites have the liberty, inter alia, to sell their inventory to advertisers.

The decrease in the placement of advertising on likely infringing websites as a consequence of the duties set forth by the GPPs may, to some extent, interfere with the business activities of the owners of likely infringing websites (it being justified or not). In reality, encouraging signatories not to place advertising on likely infringing websites may imply a loss of revenues for such websites.

Even if it could be considered that this would endanger the existence of the owners of likely infringing websites' business, it would have to be born in mind that this freedom may be subject to limits and restrictions that have been recognised by the CJEU in various decisions since its ruling of 14/05/1974, C-4/73, Nold, EU:C:1974:51<sup>228</sup>. Limits to the freedom to conduct a business are accepted provided that two following conditions are satisfied:

- The restriction must protect the general interest proportionately; and
- The restriction must not hinder the substance of the right.

As to the first condition, among the GPPs' aims are (i) the protection of rightholders' intellectual property rights and (ii) the creation a safer environment for consumers so that they avoid likely infringing websites. In this sense, the CJEU has found that consumer protection and the protection of intellectual property rights may be construed as a general interest that would justify restrictions to the freedom to conduct a business (see respectively CJEU

<sup>221</sup> [http://www.legislation.gov.uk/ukpga/2006/46/pdfs/ukpga\\_20060046\\_en.pdf](http://www.legislation.gov.uk/ukpga/2006/46/pdfs/ukpga_20060046_en.pdf).

<sup>222</sup> <http://www.legislation.gov.uk/ukpga/1998/41/contents>.

<sup>223</sup> <http://www.legislation.gov.uk/ukpga/2002/40/contents>.

<sup>224</sup> Andrea Usai, 'The Freedom to Conduct a Business in the EU, Its Limitations and Its Role in the European Legal Order: A New Engine for Deeper and Stronger Economic, Social, and Political Integration' ([https://www.germanlawjournal.com/pdfs/Vol14-No9/14.9.10\\_Usai\\_Business%20Freedom.pdf](https://www.germanlawjournal.com/pdfs/Vol14-No9/14.9.10_Usai_Business%20Freedom.pdf)).

<sup>225</sup> [http://www.legislation.gov.uk/ukpga/2006/46/pdfs/ukpga\\_20060046\\_en.pdf](http://www.legislation.gov.uk/ukpga/2006/46/pdfs/ukpga_20060046_en.pdf).

<sup>226</sup> <http://www.legislation.gov.uk/ukpga/1998/41/contents>.

<sup>227</sup> <http://www.legislation.gov.uk/ukpga/2002/40/contents>.

<sup>228</sup> <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:61973CJ0004>.

rulings of 8/10/1986, C-234/85, Keller, EU:C:1986:377<sup>229</sup> and 30/07/1996, C-84/95, Bosphorus, EU:C:1996:312<sup>230</sup>). As to the second

---

<sup>229</sup> <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:61985CJ0234>.

<sup>230</sup> <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:61995CJ0084>.

condition, it cannot be understood that the restriction to place advertising on likely infringing websites would hinder the substance of the freedom to conduct business of owners of likely infringing websites.

In light of the foregoing, as the CJEU accepts certain limitations to the freedom to conduct a business that would be applicable in the case of the GPPs, in practice it can not be considered that the freedom of owners of likely infringing websites to conduct their business would be breached.

That being said, given that the Charter of Fundamental Rights might not apply in the UK, there is some uncertainty as to how the aforementioned CJEU case law would be applicable to the freedom to conduct a business as inferred under UK law.

#### *4.5.1.2. Coexistence of the GPPs with the freedom to conduct a business of signatories of the GPPs*

By means of the freedom to conduct a business the signatories of the GPPs have the liberty, inter alia, to choose how to deal with their counterparts in the trade of display advertising and where to place such display advertising.

Given that the GPPs are not legally binding as they are a voluntary system of self-regulation to which signatories may freely adhere, there is no interference of the duties foreseen by the GPPs with signatories' activities. Thus, in practice the GPPs do not impinge on signatories' freedom to conduct their business.

#### **4.5.2. Coexistence of the GPPs with the right to an effective remedy and to a fair trial of owners of likely infringing websites**

The right to an effective remedy and to a fair trial is established by Article 47 of the Charter of Fundamental Rights ('Right to an effective remedy and to a fair trial') as well as by Schedule 1, Part I, Article 6 of the HRA ('Right to a fair trial')<sup>231</sup>. This right seeks to provide effective recourse to any person who alleges that his/her rights have been violated.

As explained by the CJEU in, for example, its ruling of 22/12/2010, C-279/09, DEB, EU:C:2010:811<sup>232</sup>, although Article 47 of the Charter of Fundamental Rights ('Right to an effective remedy and to a fair trial') uses the word 'person', the right to an effective remedy and to a fair trial may also cover legal persons, which would be the case of signatories.

In relation to the GPPs, the six commitments they establish may impact the owners of likely infringing websites based on the two following circumstances:

- The aim of the GPPs is to prevent the placement of display advertising on likely infringing websites. To that end they establish a range of preventive measures to be adopted by buyers, sellers and facilitators.
- If advertising is placed in practice on a likely infringing website, despite the preventive measures foreseen by the GPPs, signatories have to remove the advertising at stake.

A possible safeguard that could have been stipulated by the GPPs in favour of the owners of likely infringing websites would be the provision of a procedure allowing the owners to defend their position if signatories decide not to place advertising on their website.

Therefore, if we contrast the content of the right to an effective remedy and to a fair trial with the absence of safeguards under the GPPs towards owners of likely infringing websites, there may be a risk that the GPPs violate the mentioned right.

That being said, in practice most signatories of the GPPs refer to the IWL to determine whether or not a website likely infringes intellectual property rights, as explained by all the stakeholders interviewed for the purposes of this Chapter 3. As already clarified previously under Section 3.2 of this

<sup>231</sup> Although the right to an effective remedy is not expressly mentioned by this Article, it would appear to fall within its remit.

<sup>232</sup> <http://curia.europa.eu/juris/document/document.jsf?text=&docid=83452&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=131344>.



Chapter 3 ('Definition of likely infringing websites'), prior to the inclusion of a website in the IWL, PIPCU contacts the operator of such a website to give them the opportunity to comment on such a decision and to collaborate with PIPCU.

Consequently, in practice the two following scenarios are to be considered:

- Signatories including in their 'blacklists' likely infringing websites listed in the IWL.

In fact, as already explained, this is almost always the case. Therefore it could be understood that in this case the right to an effective remedy and to a fair trial of owners of likely infringing websites would have already been safeguarded by PIPCU before listing them in the IWL.

- Signatories that would include in their 'blacklists' likely infringing websites which are not listed in the IWL.

In practice signatories do not generally fall within this scenario, as the IWL is widely used, therefore the risk of the violation of the right to an effective remedy and to a fair trial of owners of likely infringing websites is low.

#### 4.5.3. Coexistence of the GPPs with the right to the protection of personal data of the signatories involved in the GPPs and of the owners of likely infringing websites

The right to the protection of personal data is envisaged by Article 8 of the Charter of Fundamental Rights ('Protection of personal data'), by the right to respect for private and family life set forth in the HRA (Schedule 1, Part I, Article 8 ('Right to respect for private and family life')), by the law relating to breach of confidence and by the UK Data Protection Act. This right generally serves to protect the self-determination right of an individual regarding the use of personal data related to them.

The processing of information related to legal persons is outside of the scope of the Data Protection Directive as well as of the UK Data Protection Act, whose Section 1 ('Basic interpretative provisions') defines 'personal data' as data which relate to a living individual.

None of the duties and procedures envisaged by the GPPs - analysed under Section 3 of this Chapter 3 ('Duties and Procedures') - imply the processing of personal data related to natural persons:

- Signatories involved in the GPPs.

Signatories involved in the GPPs are legal persons. Their contact details are the only information relating to them that may be processed in the context of the GPPs either by other signatories or by JICWEBS and verification providers. By applying to become signatories of the GPPs, it could be understood that they agree to the processing of such data.

- Owners of likely infringing websites.

The GPPs do not foresee the processing of any personal data relating to the owners of likely infringing websites. The only information that is processed concerning likely infringing websites is the URL of such websites, which is included under signatories' appropriate/inappropriate schedules or processed by the CV tools used by them.

Therefore, the right to the protection of personal data of the signatories involved in the GPPs or of owners of likely infringing websites would not impact the GPPs.

#### 4.5.4. Summary of findings relating to the compatibility of the GPPs with the European Union and UK legal frameworks and case law

This Section summarises the findings made under Section 4.5 of this Chapter 3 ('Coexistence of the measures set forth under the GPPs with European Union and UK legal frameworks and related case law') regarding the compatibility of the GPPs with European Union and UK legal frameworks and case law.

The following conclusions have been reached concerning the coexistence of the GPPs with certain fundamental rights:

- **Freedom to conduct a business of owners of likely infringing websites and of signatories of the GPPs**

- Owners of likely infringing websites' freedom to conduct a business.

Even if it could be considered that the loss of revenues by owners of likely infringing websites as a consequence of the duties established by the GPPs may possibly impact on their freedom to conduct a business, the CJEU accepts certain limitations to such a right that would be applicable to the situation at issue.

- Signatories' freedom to conduct a business.

Given that the GPPs are not legally binding in practice, such commitments do not impinge on signatories' freedom to conduct their business.

- **Right to an effective remedy and to a fair trial of owners of likely infringing websites**

The risk that the right of the owner of the likely infringing websites' to an effective remedy and to a fair trial may impact the GPPs is low. In practice most signatories use the IWL to determine whether or not a website likely infringes intellectual property rights and although the GPPs do not contain any safeguards in favour of owners of likely infringing websites, the latter are contacted by PIPCU before being included in the IWL to give them the opportunity to collaborate with them and/or to defend themselves.

- **Right to the protection of personal data of the signatories involved in the GPPs and of the owners of Likely Infringing websites**

The right to the protection of personal data of signatories of the GPPs and of owners of likely infringing websites does not impact the GPPs given that the GPPs do not imply the processing of personal data related to natural persons but information/contact details of legal persons, if any.

## 5. Technologies

The second principle established by the GPPs in its Section 1.3 ('The Principles') sets forth that signatories have to select from one (1) of the following means to detect advertising misplacement:

- CV tools. As explained under Annex 4 of this Chapter 3 ('CV tools'), CV tools are technological instruments which may be used by signatories of the GPPs to assess a website's content resolving if it is appropriate or inappropriate for an advertiser. They are able to recognise which content might be inappropriate for an advertiser despite the fact that another advertiser deems it appropriate. They are developed either internally by signatories or externally through third party services providers.
- Appropriate/inappropriate schedules. In practice, these appropriate/inappropriate schedules, or whitelists and blacklists, are supported by technological means that are developed either internally by signatories or externally through third party services providers.

Various interviewed stakeholders have explained that both CV tools and appropriate/inappropriate schedules existed before the adoption of the GPPs but now, their level of technical sophistication is increasing.

## 6. Costs

The signatories of the GPPs have to pay an annual fee due to their adherence to the GPPs. Adherence fees amount to £943<sup>233</sup> and they cover JICWEBS' supervisory role and its support in relation to the GPPs, namely:

- To host the GPPs.
- To approve verification providers.
- To conduct independent reviews and appeals.
- To review the signatories' submissions.
- To issue the GPPs seal of compliance and the relevant certificate.
- To publish the list of signatories through its website.

Moreover, the verification process to be undergone by signatories is also subject to a fee which varies depending on the Verification Provider they engage. For example, in JICWEBS' so-called 'Guide to Verification'<sup>234</sup> it is foreseen that ABC's related fees start at £2,839 (VAT not included) and that they are scaled depending on the size of the signatory (based on annual UK display advertising revenue).

Additional expenses may arise for the signatories of the GPPs as a consequence of the compliance with the commitments it envisages. For example, they will have (i) to acquire a CV tool and/or (ii) to develop internally appropriate/inappropriate schedules or to subcontract it with third party services providers.

---

<sup>233</sup> <http://www.jicwebs.org/images/JICWEBS%20product%20owner%20subscribers.pdf>.

<sup>234</sup> [http://www.abc.org.uk/Documents/Guides/Guide%20To%20DTSG%20Verification\\_Final\\_January2014.pdf](http://www.abc.org.uk/Documents/Guides/Guide%20To%20DTSG%20Verification_Final_January2014.pdf).

## 7. Education

Since the publication of the GPPs, JICWEBS, DTSG and the digital advertising trade industry have carried out activities to promote awareness of it, including the importance to signing it and implementing the commitments envisaged therein. The mentioned educational activities mainly focus on industry's awareness.

JICWEBS' website has a specific section devoted to the GPPs<sup>235</sup> where a huge amount of documentation and information relating to the GPPs may be found so that interested parties may have access to it, namely:

- JICWEBS subscriber information.
- FAQs.
- GPPs signatories.
- Verification providers.
- Registration form.
- Verification submission form.
- GPPs.
- Sample primary agreement.
- Use of Verification Provider's name and logo.
- Principles applicable to CV tools.

Apart from the mentioned section specifically dealing with the GPPs, JICWEBS regularly publishes on its website press releases relating to it<sup>236</sup>.

Among the industry, IAB UK is very active in promoting awareness on the GPPs. Inter alia, they have published several guidelines and information addressed to buyers, sellers and facilitators in order to provide them with complete information on the GPPs. Such educational activities are generally carried out by IAB UK through the following means: factsheets<sup>237</sup>, press releases<sup>238</sup> and blog entries<sup>239</sup>. Additionally, IAB has organised various events highlighting the problem of advertising misplacement and promoting the GPPs. One of these events, entitled 'Trusted ad trading and you in 2015', took place on February 2015 and it was hosted jointly by IAB UK and JICWEBS.

Interviewed for the purposes of this Chapter 3, IAB UK has explained that since the publication of the GPPs digital advertising trade bodies have hosted various general information sessions dealing with it. At the beginning, those 'town halls' aimed to educate the market on the DTSG, the GPPs and the signing up process. Now, they focus on updating the industry on upcoming plans and to facilitate feedback and opinion on the GPPs.

Furthermore, the industry is not alone in carrying out educational activities relating to the GPPs. Rightholders also play an important role in such activities. As explained by an association of rightholders in the context of this Chapter 3, its members have spoken at a number of industry events about the GPPs and the association has produced flyers outlining what the GPPs are.

Finally, as highlighted under point 3 ('Ongoing stakeholder dialogue') of the section 'Next steps' of the progress report, JICWEBS, DTSG and industry are devoted towards the dialogue for the development and improvement of

---

<sup>235</sup> <http://www.jicwebs.org/agreed-principles/digital-trading-standards-group-good-practice-principles>.

<sup>236</sup> E.g., <http://www.jicwebs.org/agreed-principles/latest-news/170-minimising-the-risk-of-digital-display-advertising-misplacement>,  
<http://www.jicwebs.org/current-priorities/brand-safety-online/161-dtsg-seal-press-release>,  
<http://www.jicwebs.org/component/content/article/2-content/154-dtsg-launches-uk-good-practice-principles>.

<sup>237</sup> E.g., <http://www.iabuk.net/sites/default/files/IAB%20Factsheet%20-%20Minimising%20the%20risk%20of%20ad%20misplacement.pdf>.

<sup>238</sup> E.g., <http://www.iabuk.net/about/press/archive/dtsg-report-shows-progress-of-digital-ad-industry-in-improving-brand-safety>.

<sup>239</sup> E.g., <http://www.iabuk.net/blog/the-iab-believes-in-brand-safety-online>.

the GPPs and, for this purpose, an ongoing dialogue between rightholders, PIPCU, the UK government and the EU Commission is taking place.

## 8. Effectiveness

An assessment on the application of the GPPs was made by JICWEBS under the progress report it issued on 24 February 2015, i.e., one year and two months after the publication of the GPPs.

The progress report contains the following main information concerning the effectiveness of the GPPs by February 2015:

- When the GPPs were adopted, thirty 37 advertising businesses were founder signatories, covering a significant proportion of the market.
- 28 advertising businesses have been awarded seals by JICWEBS confirming they meet standards aimed at reducing the risk of online advertising being served next to inappropriate or illegal content. A further 12 are progressing towards this same accreditation.
- Signatories represented over two thirds (2/3) of applicable UK display advertising market by the end of 2014 and it was expected that this will grow to between eighty per cent (80 %) and ninety per cent (90 %) by the end of 2015.

IAB UK when interviewed for the purposes of this Chapter 3 has indicated that it is expected that a new progress report relating to the GPPs including updated figures will be published early 2016.

In parallel, in August 2015 PIPCU stated that since the introduction of the IWL there has been a seventy three per cent (73 %) reduction in the appearance of advertising from the UK's top advertising spending companies on intellectual property infringing websites. For instance, the automotive, food and drink and real estate sectors' advertising has almost entirely stopped appearing on pirate sites<sup>240</sup>. These results impact positively the GPPs given that, as indicated previously in this Chapter 3, the latter are a platform to use the IWL as an inappropriate websites schedule.

---

<sup>240</sup> <https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/pipcu/pipcu-news/Pages/Operation-Creative-sees-73-per-cent-drop-in-top-UK-advertising-on-illegal-sites.aspx>.



## Chapter 3: Annex 1

### 1. GPPs (June 2015)

#### 1.1. Introduction

The UK\* Good Practice Principles ('the Principles') have been drafted by a cross-industry group called the Digital Trading Standards Group (DTSG)\*\* for review and adoption by [www.jicwebs.org](http://www.jicwebs.org). The intention of the Principles is to significantly reduce the risk of the misplacement of display advertising on digital media properties, uphold brand safety and protect the integrity of digital advertising. The work of the DTSG also reflects a common goal: that digital display advertising should not support inappropriate or illegal content or services.

The Principles cover commitments for all businesses involved in the buying, selling or facilitating of display advertising (see definitions in Appendix 1). These Principles, however, do not apply to Facilitators providing standalone ad serving services. The Principles aspire to evolve the objectives of the UK Internet Advertising Sales House (IASH) code in line with current and future technology and trading methods.

\*Business with the UK presence, targeting UK audience/users.

\*\*The DTSG is made up of representatives of the following parts of the digital display trading ecosystem: advertisers, agencies, agency trading desks (ATDs), demand side platforms (DSPs), advertising networks, sales houses, advertising exchanges, supply side platforms (SSPs) and publishers. See Appendix 1.

#### 1.2. What is digital advertising trading?

Digital display advertising – adverts that are displayed on digital media properties or other connected applications - commands a large share of media spend and helps to fund content, services and applications at little or no cost to consumers. Digital ad trading is the term given to the buying and selling of display media. The way in which digital display media is bought and sold has dramatically changed over the last 10 years and, as the market matures, so does the way in which this media is traded.

A video explaining how online display advertising works and the different businesses in the trading ecosystem is available at:

[www.iabuk.net/video/the-evolution-of-online-display-advertising](http://www.iabuk.net/video/the-evolution-of-online-display-advertising)

#### 1.3. The Principles

1. The buyers and sellers of digital display advertising shall ensure that the transaction is one pursuant to either (a) a primary agreement or (b) the specific terms and policies within an agreed or signed contract. An example of a primary agreement can be found at [www.jicwebs.org](http://www.jicwebs.org). See Note A.
2. A primary agreement, or the specific terms and policies within an agreed or signed contract, should include the buyers and sellers' intention as to where the advertising should (or should not) appear. See Note A.

The buyers and sellers should select from one or both of the following means to minimise ad misplacement:

- A. Independently-certified (to JICWEBS standards) Content Verification (CV) tool (criteria agreed between the Buyer and Seller pre-delivery); or
- B. Appropriate/Inappropriate schedules (criteria agreed between the Buyer and Seller pre-delivery).

See Notes B and C.

3. Sellers should confirm the specific provisions applied to minimise the risk of ad misplacement, irrespective of whether inventory is sourced directly or indirectly. In the absence of specific provisions, then as a minimum, a statement of reasonable endeavours is required.

4. Sellers should be able to explain the process(es) that form the basis of specific provisions and/or the reasonable endeavours.
5. Both buyers and sellers should understand any contractual consequences should they fail to monitor this process and respond appropriately to ad misplacement via take down.
6. Following a commitment to these Principles, each Signatory will have their ad misplacement minimisation policies independently verified by a JICWEBS-approved provider within six months and thereafter every year. Further details of this process are set out in the compliance and enforcement paper accompanying these Principles.

Notes:

- A. Principles 1 and 2 can be incorporated into agreed or signed contract terms and policies as long as they cover the substantive points regarding the methods for minimising 'ad misplacement'. An example of a primary agreement can be found at [www.jicwebs.org](http://www.jicwebs.org).
- B. A Facilitator will abide by any such criteria selected by the Buyer and/or Seller in the user interface provided by that Facilitator.
- C. No suggested criteria or scheduling, nor any form of 'inappropriate' destinations will be drawn up, maintained or approved by the DTSG or JICWEBS in relation to these Principles. The designation of such information is a matter solely for the Buyer to determine. Sources used may be referenced in a primary agreement or other industry information as required by the buyers but with a clear disclaimer that such sources and information are not the responsibility of the DTSG or JICWEBS.

## 2. Compliance and Enforcement

Following a commitment to the Principles, each Signatory will have their ad misplacement minimisation policies independently verified by a JICWEBS\*-approved provider ('Verification Provider') within six months and thereafter every year.

This paper, accompanying the Principles, sets out how this process will work and the requirements for (i) selecting a Verification Provider and (ii) the review of a Signatory's policies by a Verification Provider. The DTSG may evolve the detail and depth required from independent verification, as the Principles themselves evolve, and according to the DTSG Terms of Reference.

### 2.1. Selection of Verification Provider

A Signatory must choose and use a Verification Provider\*\* that is a registered auditor and member of either The Institute of Chartered Accountants in England and Wales (ICAEW), The Institute of Chartered Accountants of Scotland (ICAS), The Institute of Chartered Accountants in Ireland (ICAI) or The Association of Chartered Certified Accountants (ACCA). In exceptional circumstances a Signatory may apply to JICWEBS to use a provider who is not a member of one of the above bodies, setting out the exceptional circumstances for consideration.

These exceptional circumstances will be in addition to the following criteria:

- A. Be independent of and/or not owned by any Signatory, DTSG business or relevant individual Trade Association; and
- B. Maintain business operations in the UK.

JICWEBS will consider the application of verification providers in a timely manner and will not unreasonably withhold its approval thereof. All providers will be subject to annual review by JICWEBS and will submit compliance certificates and copies of relevant supporting material to JICWEBS, which will act as a central depository for this process.

JICWEBS will publicly disclose all its certification requirements and its review decisions regarding verification providers submitted for approval.

## 2.2. Independent Policy Verification Process

The Verification Provider will check the Signatory's compliance with the Principles. The Signatory must provide the Verification Provider with relevant information regarding the ad misplacement policies in force, and supplement such information by email or telephone correspondence as required.

Relevant written information may include:

- A. Contract terms and policies relating to the transactions of ads;
- B. A statement of reasonable endeavours applied to minimise the risk of ad misplacement,
- C. Internal policies, procedures and controls relating to the placement of ads, such as the:
  - i. details regarding the use of CV tools and appropriate/inappropriate schedules;
  - ii. names and training of personnel with enforcement responsibility; and
  - iii. enforcement process.

The Verification Provider must provide the Signatory, with a written report of its findings and, if it determines that the Signatory's policies are compliant with the Principles, a Verification Submission form should be sent to JICWEBS to consider if a certificate and seal will be issued.

Please note: Independent Verification is limited solely to whether the Signatory has implemented policies for minimising ad misplacement in compliance with the Principles. It does not extend to testing the effectiveness of any processes, procedures or controls for ad misplacement. The compliance certificate issued by the Verification Provider only covers the Signatory's policies for minimising ad misplacement.

\* JICWEBS is the UK's Joint Industry Committee for Web Standards and is made up of the following trade bodies: Association of Online Publishers (AOP), Internet Advertising Bureau (IAB), Newspaper Society, Newspapers Publishers Association, ISBA – the voice of Advertisers and the Institute of Practitioners in Advertising (IPA).

\*\* This will include ABC.

## 2.3. Reporting

### 2.3.1. Verification submission

A standard verification form, available from JICWEBS, should be completed and jointly submitted by the Signatory and Verification Provider to JICWEBS.

Against each principle this form should include a description of how the signatory has complied with the principle during the period of review. This should include sufficient information, from documented policies and processes, so that the reader can have a clear understanding of the policy and processes. As a minimum this should be in the form of a summary and/or extracts from relevant documents along with easily accessible links to the documents themselves.

The information on the verification submission will be replicated on the certificate.

### 2.3.2. Certificates and Seals

Certificates and seals will be issued by JICWEBS and published on [www.jicwebs.org](http://www.jicwebs.org)

The seal is comprised of

- a. JICWEBS DTSG Brand Safety logo
- b. Logo of verification provider (optional)
- c. Month and year that seal is valid to.

The certificate is comprised of;

- a. The seal
- b. Signatory's name and address,
- c. Signatory's logo (optional)
- d. Business/Brand verified
- e. Service provided
- f. Month of verification
- g. Compliance findings against the GPPs (as reported on the verification submission)
- h. Verification Provider's name and address
- i. Statement of the Verification Provider

## 2.4. Timing

### 2.4.1. First seal

A signatory should have their first seal issued within six months of being registered. For example, registration accepted in May 2015 — the first seal should be issued by JICWEBS by end of November 2015.

### 2.4.2. Subsequent seals

The subsequent seal must be issued before the end of the 'valid to' month and year on the current seal.

If a subsequent submission is made early then the new seal can be valid to 12 months from the current seal date, provided that the month of verification is within the timeframe set out in 2.4.4. For example — current seal valid to July 2015, verification work is done in March 2015, submission is made in April 2015 — then new seal would be valid to July 2016.

### 2.4.3. Verification submission

A joint submission by the Signatory and Verification Provider must be made to JICWEBS in consideration of a seal being issued. This should be at least two weeks before the end of the month in which the seal is to be issued.

If it is likely that the submission will not be made in time then the signatory should formally request JICWEBS to consider a later submission date. The signatory should explain the reason for the delay and suggest a revised submission date. JICWEBS will then inform the signatory of its decision.

### 2.4.4. Verification work

The month in which the verification work is completed should be no earlier than four months before the month in which the seal is issued. For example — the verification work is completed in March 2015 then the seal must be issued no later than July 2015.

### 2.4.5. Signatory listing

JICWEBS will maintain a list of signatories to the JICWEB DTSG GPPs. To be listed, a company must be currently registered with JICWEBS. In addition companies must have a current seal or be within the 6 month period before their first seal is to be issued.

Companies who have been granted a delayed submission date will be de-listed once the normal expected seal issue date has passed. They will be re-listed once a current seal is issued by JICWEBS.

## Appendix 1: Definitions

*Display Advertising:* display advertising is the display of visual files including images, Flash and video ('Display Ads') provided by buyers to sellers on a digital media property (or other connected application) when an internet user visits the digital media property. Display Ads come in varying formats.

*Seller:* A seller is a business that sells or is responsible for the placing of display advertising on digital media properties (or other connected application) (e.g., advertising network).

*Facilitator:* A facilitator is a business that provides a technology platform with the primary purpose of brokering, for compensation, the placement of display advertisements between buyers and sellers (e.g., advertising exchange). Facilitators provide the tools and controls to enable buyers and sellers to help protect brand safety in line with DTSG requirements.

*Buyer:* A buyer is a business that buys display advertising from a seller (advertiser or agency).

*Primary Agreement:* A primary agreement is a set of terms agreed between the buyer and seller.

*Content Verification (CV) Tool:* A CV tool is a technology product or service that may block or report the serving of a display advertisement onto destinations that have been defined as inappropriate to the advertising campaign by the buyer.

*Inappropriate/Appropriate Schedules:* These schedules may include/exclude sites, URLs or applications that are deemed either appropriate or inappropriate by buyers and sellers. Buyers' and sellers' agreement to the criteria for these schedules, whether communicated through the user interface or some other channel, should be pursuant to a primary agreement or terms and/or policies.

For definitions of all business models involved in the digital trading process see: [www.iabuk.net/resources/jargon-buster](http://www.iabuk.net/resources/jargon-buster).

## Chapter 3: Annex 2

### Signatories

Based on the information publicly available in JICWEBS' website<sup>241</sup>, at the time this study is being published a total of 40 entities are signatories of the GPPs:

- AD2ONE LTD
- Affectv
- AOL (UK) Ltd
- Amnet UK
- AppNexus Europe Ltd
- Bazaarvoice Ltd<sup>242</sup>
- byyd Tech
- Capify Media
- Collective Europe
- Crimtan
- Criteo
- DataXu
- DoubleClick Ad Exchange
- Exponential Interactive
- InSkin Media
- MaxPoint
- Media iQ
- Millennial Media Ltd
- OpenX
- Opera Mediaworks
- PERFORM Group
- Pulsepoint
- Quantcast
- RadiumOne
- RocketFuel
- Sociomantic Labs
- Specific Media
- SpotXchange (UK) Ltd
- StrikeAd UK Ltd
- Switch/Unanimis
- The Exchange Lab
- TubeMogul
- Unruly
- Ve Interactive Ltd<sup>243</sup>
- Vibrant Media
- Videology

---

<sup>241</sup> <http://www.jicwebs.org/agreed-principles/digital-trading-standards-group-good-practice-principles/151-dtsgsignatories>.

<sup>242</sup> This company has still not been awarded with JICWEBS' seal and compliance certificate.

<sup>243</sup> This company has still not been awarded with JICWEBS' seal and compliance certificate.

- VivaKi
- Xaxis Digital Ltd
- Yahoo
- YuMe Europe Limited



## Chapter 3: Annex 3

### Evolution of the trading of Display Advertising

The GPPs have replaced the IASH code of conduct since it became evident that the code was not flexible enough to allow its application to new online advertising trading models and technologies.

Formerly, there were three parties involved in the buying and selling of inventory: (i) the advertiser/agency, (ii) the publisher and (iii) the advertising network. Advertising networks were the intermediaries that acted as brokers between the advertiser/agency<sup>244</sup> and the publisher.

Nevertheless, the trading scenario has completely changed in the last decade. Indeed, the development of the internet and new technologies has led to so-called programmatic digital advertising, which is the current system used by the majority of advertisers/agencies and publishers to buy and to sell Display Advertising. This new trading system implies a better value for the advertiser and the publisher since trading activities are performed more effectively and efficiently using better targeting.

Advertising exchanges emerged in the context of the programmatic digital advertising. They are an automatic marketplace of inventory working as an online auction that allows the buyers and sellers to operate in real time through it rather than in a more manual process through other brokers. Advertising networks are still operative and they can trade in real time by plugging into advertising exchanges. One of the differences between an advertising exchange and an advertising network, is that in the case of the advertising network, it is the advertiser/agency who plugs into it to buy inventory from the publisher and the advertising exchange simply facilitates the trading of inventory between the buying and selling sides.

Apart from the advertisers/agencies, the publishers, the advertising exchanges and the advertising networks, other players are also involved nowadays in the trading of Display Advertising, e.g.:

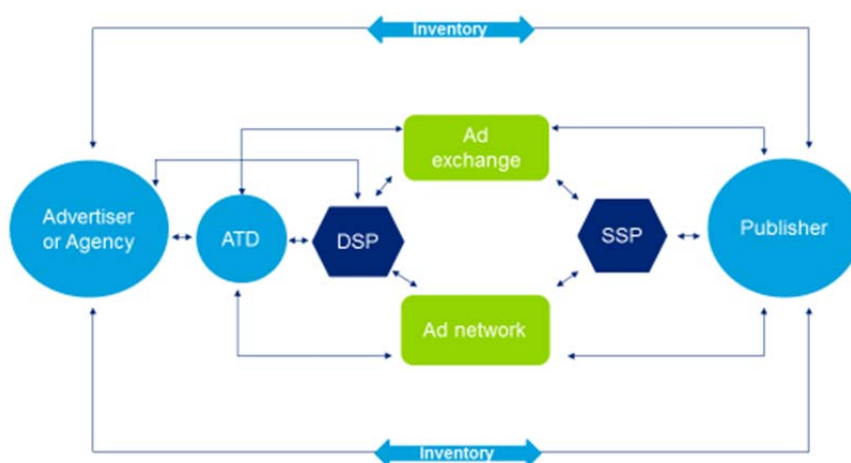
- Demand side:
  - Agency trading desks or ATDs: Specialised departments within agencies that buy and optimise inventory, often in real time, using proprietary technology or demand side platforms.
  - Demand side platforms or DSPs: Advertising technology platforms that enable the centralised purchase of inventory from different sources (e.g., advertising exchanges or supply side platforms). Amongst others, they offer advantages such as the generation of integrated reports or the possibility of performing real time auctions.
- Supply side:
  - Supply side platforms or SSPs: Advertising technology platform which represent publishers as the suppliers of inventory and give them the ability to increase their online advertising revenues by engaging with multiple demand side channels through a single vendor.
  - Sales houses: Organisations which sell advertising on behalf of publishers. Sales houses typically retain a percentage of the revenue they sell in exchange for their services. These organisations may combine a number of websites together and sell them as different packages to advertisers.

In working together, the aforementioned parties constitute the scenario of programmatic digital advertising. Under this system, for example, an advertiser and an agency may use demand side platforms, agency trading desks, advertising exchanges or advertising networks to buy inventory. On the other side, publishers may use supply side platforms or advertising exchanges to sell their inventory.

The flowchart below summarises the different connections between the trading parties in buying and selling display advertising nowadays:

---

<sup>244</sup> Means the communications agency responsible for advertisers' advertising campaigns.



Notwithstanding the aforementioned, according to the information provided by stakeholders interviewed for the purposes of this Chapter 3, not all the advertisers/agencies and the publishers use programmatic trading, it is normal that some of them buy and/or sell inventory without the intervention of all the parties which nowadays comprise the scenario of programmatic digital trading. For example, direct buying of inventory is normally carried out by premium publishers who avoid dealing with intermediaries and work directly with the advertisers/agencies themselves, which also allows them to negotiate a premium deal (direct buying can still employ programmatic techniques if the process has been automated – this is called a ‘private marketplace’).

The GPPs, under their Section 1.2 (‘What is digital advertising trading’) directly refer to the fact that the way in which digital display media is bought and sold has dramatically changed over the last ten (10) years and it provides a link to a video of IAB UK that explains how display advertising works<sup>245</sup>. In the same line, the progress report contains a chart that summarises the evolving display advertising market<sup>246</sup>.

<sup>245</sup> <http://www.iabuk.net/disciplines/display-trading/guide>.

<sup>246</sup> Progress Report, page 4. <http://www.jicwebs.org/agreed-principles/latest-news/170-minimising-the-risk-of-digital-display-advertising-misplacement>.

## Chapter 3: Annex 4

### CV tools

The GPPs establish that one of the means through which buyers and sellers may reduce advertising misplacement is by using CV tools. CV tools are technological products which may be used to assess a website's content resolving if its content is appropriate or inappropriate for the advertiser.

One of the advantages of CV tools is that they can ensure that advertising is placed according to the buying instructions of the advertiser. This means that they are able to recognise which content might be inappropriate for an advertiser while another advertiser deems it appropriate.

The way in which such CV tools work in practice can differ, so in order to provide clarity to buyers and sellers for selecting a CV tool, its suitability and adequacy has to be verified by an independent auditor meeting JICWEBS' standards. ABC is the industry owned auditor to JICWEBS that has thus far independently verified CV tools.

ABC has to certify that CV tools comply with a number of minimum requirements established by JICWEBS' Content Verification (CV) Product Principles<sup>247</sup>, namely:

'A CV Product will be tested against the following principles:

1. Block the serving of advertising on to pages which contain content, deemed to be inappropriate by the advertiser, in HTML source code. Detect inappropriate words on a web page or the code of that web page before or after the ad appears.
2. Block the serving of advertising on to pages which contain words in content delivered via a linked file deemed to be inappropriate by the advertiser. When the page appears in the browser it displays content pulled from another source which may be unrelated to the expected content on the page.
3. Register changes in page content and then block the serving of advertising on to pages which contain content, deemed to be inappropriate by the advertiser, in real time. A page which has rapidly changing content such as a forum.
4. **Block the serving of advertising on to domains and sub-domains, deemed inappropriate by the advertiser.** An inappropriate text string in the domain or sub-domain name such as <http://inappropriate.com> or <http://inappropriate.safesite.com>
5. **Block the serving of advertising on to pages which contain words in the URL, deemed to be inappropriate by the advertiser.** An inappropriate text string contained within the URL such as <http://normal.com/okay/inappropriate.aspx>).
6. **Block the serving of advertising on to aliases of an URL or domain, deemed to be inappropriate to the advertiser.** A URL may look like <http://normal.com/safe.aspx> but the page that is displayed is <http://inappropriate.com/unsafe.aspx>.
7. See through iframes and block the serving of advertising if keywords or URLs, deemed to be inappropriate, to the advertiser, are detected. Inappropriate words may be contained within the iframe which is embedded on a web page and the ad is served on the page, or vice versa.

---

<sup>247</sup> <http://www.jicwebs.org/content-verification-cv-product-principles/principles>.

An approved CV Product will also be able to serve ads correctly in equivalent scenarios that contain only appropriate content. In addition, the CV Product will:

1. **Operate consistently in allowing or blocking advertising when JavaScript is disabled.** If the product requires JavaScript to be enabled by a browser for it to make a decision as to whether the content is appropriate or not, does it block the serving of ads if JavaScript is disabled?
2. Be capable of incorporating any list of keywords or URLs, deemed to be inappropriate by the advertiser, into the CV product within 2 working days of that new list being produced.
3. Be configurable to block the serving of advertising to any URL not previously checked as safe, until the status is known, if identification of content is not in real time.

Certifications from ABC (i) confirm that a CV tool is capable of preventing advertising delivery on inappropriate content by blocking the advertising delivery and (ii) provide that the CV tool is correctly configured. Therefore, it is not guaranteed that an advertising will not be placed on a website with inappropriate content when using the CV tool in reality<sup>248</sup>. Indeed, ABC verifies that the CV tool is adequate for minimising advertising misplacement but they do not guarantee a secure result.

ABC has certified to JICWEBS the following five CV tools since the publication of the GPPs<sup>249</sup>:

- BrandShield by DoubleVerify Ltd.
- comScore vCE Validation by comScore.
- Project Sunblock V2 by Project Sunblock Ltd.
- Emediate SiteScreen from Emediate ApS.
- The AdSafe Firewall by Integral Ad Science.

---

<sup>248</sup> ABC, April 2015, 'Content Verification Certification Programme – Promoting a safer environment for online advertising', page 3.

<sup>249</sup> JICWEBS, Minimising the Risk of Digital Display Advertising Misplacement – a Joint Industry Committee for Web Standards (JICWEBS) Progress Report, 24 February 2015, page 5.

## Chapter 3: Annex 5

### European Union legal framework

#### Charter of Fundamental Rights

- Article 8: Protection of personal data.
  - '1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority'.
- Article 16: Freedom to conduct a business.
  - 'The freedom to conduct a business in accordance with Union law and national laws and practices is recognised.'
- Article 17: Right to property.
  - '2. Intellectual Property shall be protected'.
- Article 47: Right to an effective remedy and to a fair trial.
  - '1. Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article. 2. Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented.'

#### European Union Directives

- Article 3 of the InfoSoc Directive.
  - '(2) Member States shall provide for the exclusive right to authorise or prohibit the making available to the public, by wire or wireless means, in such a way that members of the public may access them from a place and at a time individually chosen by them: (a) for performers, of fixations of their performances; (b) for phonogram producers, of their phonograms; (c) for the producers of the first fixations of films, of the original and copies of their films; (d) for broadcasting organisations, of fixations of their broadcasts, whether these broadcasts are transmitted by wire or over the air, including by cable or satellite.'
- Article 8 of the InfoSoc Directive.
  - '1. Member States shall provide appropriate sanctions and remedies in respect of infringements of the rights and obligations set out in this Directive and shall take all the measures necessary to ensure that those sanctions and remedies are applied. The sanctions thus provided for shall be effective, proportionate and dissuasive. 2. Each Member State shall take the measures necessary to ensure that rightholders whose interests are affected by an infringing activity carried out on its territory can bring an action for damages and/or apply for an injunction and, where appropriate, for the seizure of infringing material as well as of devices, products or components referred to in Article 6(2). 3. Member States shall ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.'

- Article 3 of the Enforcement Directive.
  - '1. Member States shall provide for the measures, procedures and remedies necessary to ensure the enforcement of the intellectual property rights covered by this Directive. Those measures, procedures and remedies shall be fair and equitable and shall not be unnecessarily complicated or costly, or entail unreasonable time-limits or unwarranted delays. 2. Those measures, procedures and remedies shall also be effective, proportionate and dissuasive and shall be applied in such a manner as to avoid the creation of barriers to legitimate trade and to provide for safeguards against their abuse.'
- Article 9.1 of the Enforcement Directive.
  - '1. Member States shall ensure that the judicial authorities may, at the request of the applicant: (a) issue against the alleged infringer an interlocutory injunction intended to prevent any imminent infringement of an intellectual property right, or to forbid, on a provisional basis and subject, where appropriate, to a recurring penalty payment where provided for by national law, the continuation of the alleged infringements of that right, or to make such continuation subject to the lodging of guarantees intended to ensure the compensation of the rightholder; an interlocutory injunction may also be issued, under the same conditions, against an intermediary whose services are being used by a third party to infringe an intellectual property right; injunctions against intermediaries whose services are used by a third party to infringe a copyright or a related right are covered by Directive 2001/29/EC; (b) order the seizure or delivery up of the goods suspected of infringing an intellectual property right so as to prevent their entry into or movement within the channels of commerce.'
- Article 15 of the Enforcement Directive.
  - 'Member States shall ensure that, in legal proceedings instituted for infringement of an intellectual property right, the judicial authorities may order, at the request of the applicant and at the expense of the infringer, appropriate measures for the dissemination of the information concerning the decision, including displaying the decision and publishing it in full or in part. Member States may provide for other additional publicity measures which are appropriate to the particular circumstances, including prominent advertising.'
- Article 17.a of the Enforcement Directive.
  - 'Member States shall encourage: (a) the development by trade or professional associations or organisations of codes of conduct at Community level aimed at contributing towards the enforcement of the intellectual property rights, particularly by recommending the use on optical discs of a code enabling the identification of the origin of their manufacture.'
- Article 2.a of the Data Protection Directive:
  - 'personal data shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'.

## Chapter 3: Annex 6

### UK legal framework

#### Fundamental rights in UK

- HRA.
  - Introductory text, Article 6: Acts of Public Authorities. '(1) It is unlawful for a public authority to act in a way which is incompatible with a Convention right. (2) Subsection (1) does not apply to an act if: (a) as the result of one or more provisions of primary legislation, the authority could not have acted differently; or (b) in the case of one or more provisions of, or made under, primary legislation which cannot be read or given effect in a way which is compatible with the Convention rights, the authority was acting so as to give effect to or enforce those provisions. (3) In this section 'public authority' includes: (a) a court or tribunal, and; (b) any person certain of whose functions are functions of a public nature, but does not include either House of Parliament or a person exercising functions in connection with proceedings in Parliament. (5) In relation to a particular act, a person is not a public authority by virtue only of subsection (3)(b) if the nature of the act is private. (6) 'An act' includes a failure to act but does not include a failure to: (a) introduce in, or lay before, Parliament a proposal for legislation; or (b) make any primary legislation or remedial order'.
  - Schedule 1, Part II, Article 1: Right of property. 'Every natural or legal person is entitled to the peaceful enjoyment of his possessions. No one shall be deprived of his possessions except in the public interest and subject to the conditions provided for by law and by the general principles of international law. The preceding provisions shall not, however, in any way impair the right of a State to enforce such laws as it deems necessary to control the use of property in accordance with the general interest or to secure the payment of taxes or other contributions or penalties'.
  - Schedule 1, Part I, Article 6: Right to a fair trial. '1. In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interest of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice. 2. Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law. 3. Everyone charged with a criminal offence has the following minimum rights: (a) to be informed promptly, in a language which he understands and in detail, of the nature and cause of the accusation against him; (b) to have adequate time and facilities for the preparation of his defence; (c) to defend himself in person or through legal assistance of his own choosing or, if he has not sufficient means to pay for legal assistance, to be given it free when the interests of justice so require; (d) to examine or have examined witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him; (e) to have the free assistance of an interpreter if he cannot understand or speak the language used in court'.
  - Schedule 1, Part I, Article 8: Right to respect for private and family life. '1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the



interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others’.

## UK Regulations

- UK Copyright, Designs and Patents Act.
  - Section 16: The acts restricted by copyright in a work: ‘(1) The owner of the copyright in a work has, in accordance with the following provisions of this chapter, the exclusive right to do the following acts in the United Kingdom: (a) to copy the work (see section 17); (b) to issue copies of the work to the public (see section 18); (ba) to rent or lend the work to the public (see section 18A); (c) to perform, show or play the work in public (see section 19); (d) to communicate the work to the public (see section 20); (e) to make an adaptation of the work or do any of the above in relation to an adaptation (see section 21); and those acts are referred to in this part as the ‘acts restricted by the copyright’. (2) Copyright in a work is infringed by a person who without the licence of the copyright owner does, or authorises another to do, any of the acts restricted by the copyright. (3) References in this part to the doing of an act restricted by the copyright in a work are to the doing of it: (a) in relation to the work as a whole or any substantial part of it, and (b) either directly or indirectly; and it is immaterial whether any intervening acts themselves infringe copyright. (4) This chapter has effect subject to: (a) the provisions of chapter III (acts permitted in relation to copyright works), and (b) the provisions of chapter VII (provisions with respect to copyright licensing)’.
  - Section 20: Infringement by communication to the public. ‘(1) The communication to the public of the work is an act restricted by the copyright in: (a) a literary, dramatic, musical or artistic work, (b) a sound recording or film, or (c) a broadcast. (2) References in this part to communication to the public are to communication to the public by electronic transmission, and in relation to a work include: (a) the broadcasting of the work; (b) the making available to the public of the work by electronic transmission in such a way that members of the public may access it from a place and at a time individually chosen by them’.
  - Section 96: Infringement actionable by copyright owner. ‘(1) An infringement of copyright is actionable by the copyright owner. (2) In an action for infringement of copyright all such relief by way of damages, injunctions, accounts or otherwise is available to the plaintiff as is available in respect of the infringement of any other property right. (3) This section has effect subject to the following provisions of this chapter’.
  - Section 97: Provisions as to damages in infringement action. ‘(1) Where in an action for infringement of copyright it is shown that at the time of the infringement the defendant did not know, and had no reason to believe, that copyright subsisted in the work to which the action relates, the plaintiff is not entitled to damages against him, but without prejudice to any other remedy. (2) The court may in an action for infringement of copyright having regard to all the circumstances, and in particular to: (a) the flagrancy of the infringement, and (b) any benefit accruing to the defendant by reason of the infringement, award such additional damages as the justice of the case may require’.
  - Section 97.a: Injunctions against service providers. ‘(1) The High Court (in Scotland, the Court of Session) shall have power to grant an injunction against a service provider, where that service provider has actual knowledge of another person using their service to infringe copyright. (2) In determining whether a service provider has actual knowledge for the purpose of this section, a court shall take into account all matters which appear to it in the particular circumstances to be relevant and, amongst other things, shall have regard to: (a) whether a service provider has received a notice through a means of contact made available in accordance with regulation 6(1)(c) of the Electronic Commerce (EC Directive) Regulations 2002 (SI 2002/2013); and (b) the extent to which any notice includes: (i) the full name and address of the sender of the notice; (ii) details of the infringement in question. (3) In this section “service provider” has the meaning given to it by regulation 2 of the Electronic Commerce (EC Directive) Regulations 2002’.

- Section 107: Criminal liability for making or dealing with infringing articles, &c. '(1) A person commits an offence who, without the licence of the copyright owner: (a) makes for sale or hire, or (b) imports into the United Kingdom otherwise than for his private and domestic use, or (c) possesses in the course of a business with a view to committing any act infringing the copyright, or (d) in the course of a business: (i) sells or lets for hire, or (ii) offers or exposes for sale or hire, or (iii) exhibits in public, or (iv) distributes, or (e) distributes otherwise than in the course of a business to such an extent as to affect prejudicially the owner of the copyright, an article which is, and which he knows or has reason to believe is, an infringing copy of a copyright work. (2) A person commits an offence who: (a) makes an article specifically designed or adapted for making copies of a particular copyright work, or (b) has such an article in his possession, knowing or having reason to believe that it is to be used to make infringing copies for sale or hire or for use in the course of a business. (2A) A person who infringes copyright in a work by communicating the work to the public: (a) in the course of a business, or (b) otherwise than in the course of a business to such an extent as to affect prejudicially the owner of the copyright, commits an offence if he knows or has reason to believe that, by doing so, he is infringing copyright in that work. (3) Where copyright is infringed (otherwise than by reception of a communication to the public): (a) by the public performance of a literary, dramatic or musical work, or (b) by the playing or showing in public of a sound recording or film, any person who caused the work to be so performed, played or shown is guilty of an offence if he knew or had reason to believe that copyright would be infringed. (4) A person guilty of an offence under subsection (1)(a), (b), (d)(iv) or (e) is liable: (a) on summary conviction to imprisonment for a term not exceeding six months or a fine not exceeding £50,000, or both; (b) on conviction on indictment to a fine or imprisonment for a term not exceeding ten years, or both. (4A) A person guilty of an offence under subsection (2A) is liable: (a) on summary conviction to imprisonment for a term not exceeding three months or a fine not exceeding £50,000, or both; (b) on conviction on indictment to a fine or imprisonment for a term not exceeding two years, or both. (5) A person guilty of any other offence under this section is liable on summary conviction to imprisonment for a term not exceeding three months or a fine not exceeding level 5 on the standard scale, or both. (6) Sections 104 to 106 (presumptions as to various matters connected with copyright) do not apply to proceedings for an offence under this section; but without prejudice to their application in proceedings for an order under section 108 below'.
- Section 226: Primary infringement of design right. '(1) The owner of design right in a design has the exclusive right to reproduce the design for commercial purposes: (a) by making articles to that design, or (b) by making a design document recording the design for the purpose of enabling such articles to be made. (2) Reproduction of a design by making articles to the design means copying the design so as to produce articles exactly or substantially to that design, and references in this part to making articles to a design shall be construed accordingly. (3) Design right is infringed by a person who without the licence of the design right owner does, or authorises another to do, anything which by virtue of this section is the exclusive right of the design right owner. (4) For the purposes of this section reproduction may be direct or indirect, and it is immaterial whether any intervening acts themselves infringe the design right. (5) This section has effect subject to the provisions of chapter III (exceptions to rights of design right owner)'.
- Section 227: Secondary infringement: importing or dealing with infringing article. '(1) Design right is infringed by a person who, without the licence of the design right owner: (a) imports into the United Kingdom for commercial purposes, or (b) has in his possession for commercial purposes, or (c) sells, lets for hire, or offers or exposes for sale or hire, in the course of a business, an article which is, and which he knows or has reason to believe is, an infringing article. (2) This section has effect subject to the provisions of chapter III (exceptions to rights of design right owner)'.
- Section 229: Rights and remedies of design right owner. '(1) An infringement of design right is actionable by the design right owner. (2) In an action for infringement of design right all such relief by way of damages, injunctions, accounts or otherwise is available to the plaintiff as is available in respect of the infringement of any other property right. (3) The court may in an action for infringement of design right, having regard to all the circumstances and in particular to: (a) the flagrancy of the infringement, and (b) any benefit accruing to the defendant by reason of the infringement, award such additional damages as the justice of the case may require'.

- **UK Registered Designs Act.**

- **Section 7: Right given by registration.** '(1) The registration of a design under this Act gives the registered proprietor the exclusive right to use the design and any design which does not produce on the informed user a different overall impression. (2) For the purposes of subsection (1) above and section 7A of this Act any reference to the use of a design includes a reference to: (a) the making, offering, putting on the market, importing, exporting or using of a product in which the design is incorporated or to which it is applied; or (b) stocking such a product for those purposes. (3) In determining for the purposes of subsection (1) above whether a design produces a different overall impression on the informed user, the degree of freedom of the author in creating his design shall be taken into consideration. (4) The right conferred by subsection (1) above is subject to any limitation attaching to the registration in question (including, in particular, any partial disclaimer or any declaration by the registrar or a court of partial invalidity)'.
- **Section 7A: Infringements of rights in registered designs.** '(1) Subject as follows, the right in a registered design is infringed by a person who, without the consent of the registered proprietor, does anything which by virtue of section 7 of this Act is the exclusive right of the registered proprietor. (2) The right in a registered design is not infringed by: (a) an act which is done privately and for purposes which are not commercial; (b) an act which is done for experimental purposes; (c) an act of reproduction for teaching purposes or for the purpose of making citations provided that the conditions mentioned in subsection (3) below are satisfied; (d) the use of equipment on ships or aircraft which are registered in another country but which are temporarily in the United Kingdom; (e) the importation into the United Kingdom of spare parts or accessories for the purpose of repairing such ships or aircraft; or (f) the carrying out of repairs on such ships or aircraft. (3) The conditions mentioned in this subsection are: (a) the act of reproduction is compatible with fair trade practice and does not unduly prejudice the normal exploitation of the design; and (b) mention is made of the source. (4) The right in a registered design is not infringed by an act which relates to a product in which any design protected by the registration is incorporated or to which it is applied if the product has been put on the market in the European Economic Area by the registered proprietor or with his consent. (5) The right in a registered design of a component part which may be used for the purpose of the repair of a complex product so as to restore its original appearance is not infringed by the use for that purpose of any design protected by the registration. (6) No proceedings shall be taken in respect of an infringement of the right in a registered design committed before the date on which the certificate of registration of the design under this Act is granted'.
- **Section 24A: Action for infringement.** '(1) An infringement of the right in a registered design is actionable by the registered proprietor. (2) In an action for infringement all such relief by way of damages, injunctions, accounts or otherwise is available to him as is available in respect of the infringement of any other property right. (3) This section has effect subject to section 24B (exemption of innocent infringer from liability)'.

- **UK Trade Marks Act.**

- **Section 9: Rights conferred by registered trade mark.** '(1) The proprietor of a registered trade mark has exclusive rights in the trade mark which are infringed by use of the trade mark in the United Kingdom without his consent. The acts amounting to infringement, if done without the consent of the proprietor, are specified in section 10. (2) References in this Act to the infringement of a registered trade mark are to any such infringement of the rights of the proprietor. (3) The rights of the proprietor have effect from the date of registration (which in accordance with section 40(3) is the date of filing of the application for registration): Provided that: (a) no infringement proceedings may be begun before the date on which the trade mark is in fact registered; and (b) no offence under section 92 (unauthorised use of trade mark, &c. in relation to goods) is committed by anything done before the date of publication of the registration'.
- **Section 10: Infringement of registered trade mark.** '(1) A person infringes a registered trade mark if he uses in the course of trade a sign which is identical with the trade mark in relation to goods or services which are identical with those for which it is registered. (2) A person infringes a registered trade mark if he uses in the course of trade a sign where because: (a) the sign is identical with the trade mark and

is used in relation to goods or services similar to those for which the trade mark is registered, or (b) the sign is similar to the trade mark and is used in relation to goods or services identical with or similar to those for which the trade mark is registered, there exists a likelihood of confusion on the part of the public, which includes the likelihood of association with the trade mark. (3) A person infringes a registered trade mark if he uses in the course of trade a sign which: (a) is identical with or similar to the trade mark, and (b) is used in relation to goods or services which are not similar to those for which the trade mark is registered, where the trade mark has a reputation in the United Kingdom and the use of the sign, being without due cause, takes unfair advantage of, or is detrimental to, the distinctive character or the repute of the trade mark. (4) For the purposes of this section a person uses a sign if, in particular, he: (a) affixes it to goods or the packaging thereof; (b) offers or exposes goods for sale, puts them on the market or stocks them for those purposes under the sign, or offers or supplies services under the sign; (c) imports or exports goods under the sign; or (d) uses the sign on business papers or in advertising. (5) A person who applies a registered trade mark to material intended to be used for labelling or packaging goods, as a business paper, or for advertising goods or services, shall be treated as a party to any use of the material which infringes the registered trade mark if when he applied the mark he knew or had reason to believe that the application of the mark was not duly authorised by the proprietor or a licensee. (6) Nothing in the preceding provisions of this section shall be construed as preventing the use of a registered trade mark by any person for the purpose of identifying goods or services as those of the proprietor or a licensee. But any such use otherwise than in accordance with honest practices in industrial or commercial matters shall be treated as infringing the registered trade mark if the use without due cause takes unfair advantage of, or is detrimental to, the distinctive character or repute of the trade mark’.

- Section 14: Action for infringement. ‘(1) An infringement of a registered trade mark is actionable by the proprietor of the trade mark. (2) In an action for infringement all such relief by way of damages, injunctions, accounts or otherwise is available to him as is available in respect of the infringement of any other property right’.
- Section 15: Order for erasure &c. of offending sign. ‘(1) Where a person is found to have infringed a registered trade mark, the court may make an order requiring him: (a) to cause the offending sign to be erased, removed or obliterated from any infringing goods, material or articles in his possession, custody or control, or (b) if it is not reasonably practicable for the offending sign to be erased, removed or obliterated, to secure the destruction of the infringing goods, material or articles in question. (2) If an order under subsection (1) is not complied with, or it appears to the court likely that such an order would not be complied with, the court may order that the infringing goods, material or articles be delivered to such person as the court may direct for erasure, removal or obliteration of the sign, or for destruction, as the case may be’.
- Section 16: Order for delivery up of infringing goods, materials or articles. ‘(1) The proprietor of a registered trade mark may apply to the court for an order for the delivery up to him, or such other person as the court may direct, of any infringing goods, material or articles which a person has in his possession, custody or control in the course of a business. (2) An application shall not be made after the end of the period specified in section 18 (period after which remedy of delivery up not available); and no order shall be made unless the court also makes, or it appears to the court that there are grounds for making, an order under section 19 (order as to disposal of infringing goods, &c.). (3) A person to whom any infringing goods, material or articles are delivered up in pursuance of an order under this section shall, if an order under section 19 is not made, retain them pending the making of an order, or the decision not to make an order, under that section. (4) Nothing in this section affects any other power of the court’.
- UK Data Protection Act.
  - Section 1: Basic interpretative provisions. ‘[...] ‘personal data’ means data which relate to a living individual who can be identified: (a) from those data, or; (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual’.

## Chapter 3: Annex 7

### CJEU case law

PROMUSICAE CJEU RULING (29 JANUARY 2008)	
Parties	<ul style="list-style-type: none"> <li>▪ Productores de Música de España (hereinafter, '<b>PROMUSICAE</b>').</li> <li>▪ Telefónica de España, S.A.U. (hereinafter, '<b>TELEFONICA</b>').</li> </ul>
Facts	<ul style="list-style-type: none"> <li>▪ PROMUSICAE is a Spanish non-profit-making organisation of producers and publishers of musical and audio-visual recordings.</li> <li>▪ TELEFONICA is a Spanish commercial company whose activities include the provision of internet access services.</li> <li>▪ PROMUSICAE asked for TELEFONICA to be ordered to disclose the identities and physical addresses of certain persons to whom it provided internet access services and whose IP address and date and time of connection were known. According to PROMUSICAE, those persons used a file exchange program (peer-to-peer) and provided access in shared files of personal computers to phonograms in which the members of PROMUSICAE held the exploitation rights.</li> <li>▪ The Spanish judge ordered the preliminary measures requested by PROMUSICAE. TELEFONICA appealed against that order, arguing that under the Spanish Law implementing the E-Commerce Directive, the communication of data required by PROMUSICAE was authorised only in a criminal investigation or for the purpose of safeguarding public security and national defence, not in civil proceedings including for preliminary measures.</li> <li>▪ PROMUSICAE argued that the Spanish law implementing the E-Commerce Directive had to be interpreted in accordance with various provisions of the E-Commerce Directive, the InfoSoc Directive and the Enforcement Directive and with Articles 17.2 (<i>Right to Property</i>) and 47 (<i>Right to an effective remedy and to a fair trial</i>) of the Charter of Fundamental Rights. Such provisions did not allow a Member State to limit solely to the purposes expressly mentioned in that law the obligations to communicate the data in question.</li> </ul>
Preliminary Ruling	By its questions, the national court asked essentially whether Community law, in particular the E-Commerce Directive, the InfoSoc Directive and the Enforcement Directive read also in the light of Articles 17 ( <i>Right to Property</i> ) and 47 ( <i>Right to an effective remedy and to a fair trial</i> ) of the Charter of Fundamental Rights, must be interpreted as requiring Member States to lay down, in order to ensure effective protection of copyright, an obligation to communicate personal data in the context of civil proceedings.



PROMUSICAE CJEU RULING (29 JANUARY 2008)	
CJEU Decision	<ul style="list-style-type: none"> <li>▪ The CJEU has established that the E-Commerce Directive, the InfoSoc Directive, the Electronic Communications Directive, the Enforcement Directive and the E-Commerce Directive do not require Member States to impose an obligation to communicate personal data in order to ensure effective protection of copyright in the context of civil proceedings.</li> <li>▪ However, according to the CJEU, European law requires that, when incorporating those Directives into national law, Member States must take care to rely on an interpretation of them which allows a fair balance to be struck between the various fundamental rights protected by the EU legal order, namely, between the protection of personal data on the one hand and the protection of property (including intellectual property) and the right to an effective remedy on the other hand.</li> <li>▪ The mechanisms allowing those different rights and interests to be balanced are contained in the E-Commerce Directive, in that it provides for rules which determine in what circumstances and to what extent the processing of personal data is lawful and what safeguards must be provided for, and in the E-Commerce Directive, the InfoSoc Directive and the Enforcement Directive which reserve the cases in which the measures adopted to protect the rights they regulate affect the protection of personal data. They further result from the adoption by Member States of national provisions transposing those Directives and their application by national authorities.</li> <li>▪ Furthermore, when implementing those Directives, the Authorities and Courts of the Member States must not only interpret their national laws in a manner consistent with those Directives but also make sure that they do not rely on an interpretation of them which would be in conflict with the fundamental rights mentioned above or with the other general principles of EU law, such as the principle of proportionality.</li> </ul>

SVENSSON CJEU RULING (13 FEBRUARY 2014)	
Parties	<ul style="list-style-type: none"> <li>▪ Nils Svensson</li> <li>▪ Sten Sjögren</li> <li>▪ Madelaine Sahlman</li> <li>▪ Pia Gadd</li> </ul> <p>(hereinafter, jointly referred to as the <b>Applicants</b>)</p> <ul style="list-style-type: none"> <li>▪ Retriever Sverige AB. (hereinafter, <b>RETRIEVER</b>).</li> </ul>
Facts	<ul style="list-style-type: none"> <li>▪ The Applicants, all journalists, are the authors of press articles that were published in the <i>Göteborgs-Posten</i> newspaper and on the <i>Göteborgs-Posten</i> website.</li> <li>▪ RETRIEVER is a Swedish company that operates a website that provides its clients with lists of clickable Internet links to articles published by other websites. The articles linked by RETRIEVER's website were freely accessible on the <i>Göteborgs-Posten</i> newspaper's website.</li> <li>▪ The Applicants brought an action against RETRIEVER before the Stockholm District Court (<i>Stockholms tingsrätt</i>) in order to obtain compensation on the ground that RETRIEVER had made use, without their authorisation, of certain articles written by them by making them available to its clients.</li> <li>▪ By judgment of 11 June 2010, the Stockholm District Court rejected the Applicants' action. The Applicants then brought an appeal against this judgment before the</li> </ul>

SVENSSON CJEU RULING (13 FEBRUARY 2014)	
	<p>Svea Court of Appeal (<i>Svea hovrätt</i>). The Applicants claimed before this court, inter alia, that RETRIEVER had infringed their exclusive exploitation right to make their respective works available to the public, in that as a result of the services offered on its website, RETRIEVER's clients had access to the Applicants' works.</p> <ul style="list-style-type: none"> <li>RETRIEVER opposed alleging that the provision of lists of internet links to works communicated to the public on other websites does not constitute an act liable to affect the copyright in those works. It did not carry out any transmission of any protected work as its services are limited to indicating to its clients the websites on which the works that are of interest to them could be found.</li> </ul>
Preliminary Ruling	<p>By its questions, the national Court decided to refer to the CJEU for a preliminary ruling asking, inter alia:</p> <ul style="list-style-type: none"> <li>Whether Article 3.1 of the Infosoc Directive must be interpreted as meaning that the provision on a website of clickable links to protected works available on another website constitutes an act of communication to the public as referred to in that provision, where, on that other site, the works concerned are freely accessible.</li> <li>Whether it could be possible for a Member State to give wider protection to authors' exclusive right by enabling communication to the public to cover a greater range of acts than provided for in Article 3.1 of the Infosoc Directive.</li> </ul>
CJEU Decision	<ul style="list-style-type: none"> <li>The CJEU has established that, as per Article 3.1 of the Infosoc Directive, in a case where all the users of another website to whom the works at issue have been communicated by means of a clickable link could access those works directly on the website on which they were initially communicated, without the involvement of the manager of that other website, the users of the site managed by the latter must be deemed to be potential recipients of the initial communication and, therefore, as being part of the public taken into account by the copyright holders when they authorised the initial communication. Therefore, since there is no new public, the authorisation of the copyright holders is not required for a communication to the public.</li> <li>The CJEU also stated that, if the Member States were to be afforded the possibility of laying down that the concept of communication to the public includes a wider range of activities than those referred to in Article 3.1 of the Infosoc Directive, the functioning of the internal market would be bound to be adversely affected. Therefore, the mentioned article must be interpreted as precluding a Member State from giving wider protection to copyright holders by laying down that the concept of communication to the public includes a wider range of activities than those referred to in that provision.</li> </ul>

KINO.TO CJEU RULING (27 MARCH 2014)	
Parties	<ul style="list-style-type: none"> <li>UPC Telekabel Wien GmbH (hereinafter, '<b>TELEKABEL</b>').</li> <li>Constantin Film Verleih GmbH,</li> <li>Wega Filmproduktionsgesellschaft mbH,</li> </ul> <p>(hereinafter, jointly referred as the '<b>Production Companies</b>').</p>
Facts	<ul style="list-style-type: none"> <li>TELEKABEL is an Austrian internet service provider.</li> <li>The Production Companies are an Austrian and a German film production companies.</li> </ul>



KINO.TO CJEU RULING (27 MARCH 2014)	
	<ul style="list-style-type: none"> <li>Having established that a website was offering, without their agreement, either a download or 'streaming' of some of the films that the Production Companies had produced, the Production Companies referred the matter to the court responsible for hearing applications for interim measures with a view to obtaining, on the basis of Article 81(1)(a) of the Austrian Copyright Act an order enjoining TELEKABEL to block the access of its customers to the website at issue (i.e., kino.to), inasmuch as that site makes available to the public without their consent cinematographic works over which they hold a right related to copyright.</li> <li>By order of 13 May 2011, the Commercial Court of Vienna (<i>Handelsgericht Wien</i>) prohibited TELEKABEL from providing its customers with access to <i>kino.to</i> by blocking that website's domain name and current IP address and any other IP addresses of that website of which TELEKABEL might be aware.</li> <li>TELEKABEL appealed to the Austrian Supreme Court (<i>Oberster Gerichtshof</i>) and alleged, inter alia, that its services could not be considered to be used to infringe a copyright or related right within the meaning of Article 8.3 of the Infosoc Directive because it did not have any business relationship with the operators of the website at issue and it was not established that its own customers acted unlawfully. In any event, TELEKABEL claimed that the various blocking measures that may be introduced can all be technically circumvented and that some of them are excessively costly, which would be contrary to the rights envisaged in the Charter of Fundamental Rights.</li> </ul>
Preliminary Ruling	<p>The national Court decided to refer to the CJEU for a preliminary ruling asking, inter alia:</p> <ul style="list-style-type: none"> <li>Whether it is compatible with Union law, in particular with the necessary balance between the parties' fundamental rights, to prohibit in general terms an internet access provider from allowing its customers access to a certain website (thus without ordering specific measures) as long as the material available on that website is provided exclusively or predominantly without the rightholder's consent, if the access provider can avoid incurring coercive penalties for breach of the prohibition by showing that it had nevertheless taken all reasonable measures?</li> <li>If the answer to the previous question is in the negative: Whether it is compatible with Union law, in particular with the necessary balance between the parties' fundamental rights, to require an internet access provider to take specific measures to make it more difficult for its customers to access a website containing material that is made available unlawfully if those measures require not inconsiderable costs and can easily be circumvented without any special technical knowledge?</li> </ul>
CJEU Decision	<ul style="list-style-type: none"> <li>The CJEU has established that where several fundamental rights are at issue, the Member States must, when transposing a directive, ensure that they rely on an interpretation of the directive which allows a fair balance to be struck between the applicable fundamental rights protected by the European Union legal order.</li> <li>Furthermore, when implementing the measures transposing that directive, the authorities and courts of the Member States must not only interpret their national law in a manner consistent with that directive but also ensure that they do not rely on an interpretation of it that would be in conflict with those fundamental rights or with the other general principles of EU law, such as the principle of proportionality.</li> <li>In the case at issue, the CJEU observed that an injunction such as that at</li> </ul>

KINO.TO CJEU RULING (27 MARCH 2014)

issue in the main proceedings, taken on the basis of Article 8.3 of the Infosoc Directive, makes it necessary to strike a balance, primarily, between (i) copyrights and related rights, which are intellectual property and are therefore protected under Article 17.2 of the Charter of Fundamental Rights, (ii) the freedom to conduct a business, which economic agents such as internet service providers enjoy under Article 16 of the Charter of Fundamental Rights, and (iii) the freedom of information of internet users, whose protection is ensured by Article 11 of the Charter of Fundamental Rights.

## CHAPTER 4: DUTCH NOTICE-AND- TAKE-DOWN CODE OF CONDUCT



## Chapter 4: Glossary of terms

For the purposes of this Chapter 4:

- **AEPD**: the Spanish Data Protection Agency (Agencia Española de Protección de Datos).
- **Article 29 WP**: the Article 29 Data Protection Working Party that was set up under the Data Protection Directive. It has advisory status, acts independently and is composed of a representative of the supervisory authority(ies) designated by each European Union country, a representative of the authority(ies) established by the European Union institutions and bodies and a representative of the European Commission<sup>250</sup>.
- **BASCAP**: Business Action to Stop Counterfeiting and Piracy, a subgroup of the International Chamber of Commerce<sup>251</sup>.
- **BEUC**: the European Consumer Organisation (Bureau Européen des Unions de Consommateurs).
- **Bonnier CJEU Ruling**: the ruling issued on 13/04/2012 by the CJEU under case C-461/10, Bonnier v Perfect Communications, ECLI:EU:C:2012:219<sup>252</sup>.
- **BREIN**: Protection Rights Entertainment Industry Netherlands (the BREIN foundation)<sup>253</sup> (Beschermer Rechten Entertainment Industrie Nederland).
- **Charter of fundamental rights**: the Charter of Fundamental Rights of the European Union<sup>254</sup>.
- **CJEU**: the Court of Justice of the European Union.
- **Content Provider**: the person or organisation that has placed (contested) content on the internet<sup>255</sup>.
- **Cyberlockers**: online data hosting services that provide remote storage space within a secure storage architecture<sup>256</sup>.
- **Data Protection Directive**: the Directive of 24 October 1995 on Data Protection<sup>257</sup>. At the moment of the drafting of this Study, the Data Protection Directive was in force. This Directive **has been repealed** by the General Data Protection Regulation on May 2016.
- **DHPA**: the Dutch Hosting Providers Association<sup>258</sup>.
- **DMCA**: the USA Digital Millennium Copyright Law from 1998<sup>259</sup>.
- **DNS**: Domain Name System Servers.
- **Dutch Civil Code**: the Dutch Civil Code, 1992, (Burgerlijk Wetboek)<sup>260</sup>.
- **Dutch Criminal Code**: the Dutch Criminal Code of 3 March 1881, (Wetboek van Strafrecht)<sup>261</sup>.
- **Dutch Public Prosecutors Office**: the Prosecutors Office in the Netherlands.
- **E-Commerce Directive**: the Directive of 8 June 2000 on electronic commerce<sup>262</sup>.

<sup>250</sup> [http://ec.europa.eu/justice/data-protection/article-29/index\\_en.htm](http://ec.europa.eu/justice/data-protection/article-29/index_en.htm).

<sup>251</sup> <http://www.iccwbo.org/advocacy-codes-and-rules/bascap/welcome-to-bascap/>.

<sup>252</sup> <http://curia.europa.eu/juris/liste.jsf?num=C-461/10>.

<sup>253</sup> <http://www.anti-piracy.nl/english.php>. See complete list of Brein's participants in Annex 1 of this Chapter 4.

<sup>254</sup> Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012.

<sup>255</sup> Definition given by the Notice-and-take-down Code of Conduct.

[http://www.ecp.nl/sites/default/files/NTD\\_Gedragcode\\_Engels.pdf](http://www.ecp.nl/sites/default/files/NTD_Gedragcode_Engels.pdf).

<sup>256</sup> For more information about cyberlockers, <http://www.techopedia.com/definition/27694/cyberlocker>.

<sup>257</sup> Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23/11/1995 p. 0031 – 0050.

<sup>258</sup> <https://www.dhpa.nl/>.

<sup>259</sup> Digital Millennium Copyright Law, December, 1998 <http://www.copyright.gov/legislation/dmca.pdf>.

<sup>260</sup> The Dutch Civil Code, <http://dutchcivillaw.com/legislation/dcctitle6633.htm>.

<sup>261</sup> The Dutch Criminal Code, [http://www.ejtn.eu/PageFiles/6533/2014%20seminars/Omsenie/WetboekvanStrafrecht\\_ENG\\_PV.pdf](http://www.ejtn.eu/PageFiles/6533/2014%20seminars/Omsenie/WetboekvanStrafrecht_ENG_PV.pdf).

<sup>262</sup> Directive 2000/31/EC of the European Parliament and of the Council of June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ L 178, 17/07/2000 p. 1-16.

- **ECP:** the Electronic Commerce Platform (Platform voor de InformatieSamenleving).
- **Electronic Communications Directive:** the Directive of 12 July 2002 on the processing of personal data and the protection of privacy in the electronic communication sector<sup>263</sup>.
- **Enforcement Directive:** the Directive of 29 April 2004 on the enforcement of intellectual property rights<sup>264</sup>.
- **European Union Directives:** the E-Commerce Directive, the Data Protection Directive, the Enforcement Directive and the Directive on Privacy and Electronic Communications collectively.
- **FIOD-ECD:** Means the Fiscal Intelligence and Investigation Service and the Economic Investigation Service.
- **General Data Protection Regulation:** the Regulation of the European Parliament and of the Council 2016/679 on the protection of individuals with regard to the processing of personal data and on the free movement of such data<sup>265</sup>.
- **InfoSoc Directive:** the Directive of 22 May 2001 on the information society<sup>266</sup>.
- **Intermediary:** any company that provides a (telecommunications) service on the internet<sup>267</sup>.
- **IP Address:** numeric Internet Protocol Address.
- **ISP:** Internet Service Provider.
- **ISP Connect:** a Dutch ISP Association.
- **Japanese Law on the Limitation of Liability:** the Japanese Law on the Limitation of Liability for damages of specified telecommunications service providers and the right to demand disclosure of identification information of the senders<sup>268</sup>.
- **NICC:** the Dutch National Infrastructure against Cyber Crime.
- **Notifier:** a person or organisation that makes a report<sup>269</sup>.
- **NTD or the Code:** the Notice-and-Take-Down Code of Conduct implemented in the Netherlands.
- **PDPA:** the Dutch Personal Data Protection Law (*Wet Bescherming Persoonsgegevens*)<sup>270</sup>.
- **Promusicae CJEU Ruling:** the ruling issued on 29 January 2008 by the CJEU under case C-275/06, *Promusicae v Telefónica*, ECLI:EU:C:2008:54<sup>271</sup>.
- **Rightholder:** any individual or organisation holding rights to copyrights, patents or trade marks, based on the various explanations of the various stakeholders interviewed for the purposes of this Chapter 4.
- **VCP:** ‘voluntary collaboration practices’ developed by industry, public bodies and/or third parties such as non-governmental organisations and then adhered to by the respective industry in addressing

<sup>263</sup> Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201.

<sup>264</sup> Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, OJ L 157 of 30 April 2004.

<sup>265</sup> Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/CE OJ L 119, 4.5.2016, p. 1–88 <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>

<sup>266</sup> Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167, 22/06/2001 p. 10-19.

<sup>267</sup> Definition given by the Notice-and-take-down Code of Conduct.

[http://www.ecp.nl/sites/default/files/NTD\\_Gedragcode\\_Engels.pdf](http://www.ecp.nl/sites/default/files/NTD_Gedragcode_Engels.pdf).

<sup>268</sup> Law on the limitation of liability for damages of specified telecommunications service providers and the right to demand disclosure of identification information of the senders. [http://www.unesco.org/culture/pdf/anti-piracy/Japan/Jp\\_%20LimitLiability\\_Telecom\\_en](http://www.unesco.org/culture/pdf/anti-piracy/Japan/Jp_%20LimitLiability_Telecom_en).

<sup>269</sup> Definition given by the The Notice-and-take-down Code of Conduct.

[http://www.ecp.nl/sites/default/files/NTD\\_Gedragcode\\_Engels.pdf](http://www.ecp.nl/sites/default/files/NTD_Gedragcode_Engels.pdf).

<sup>270</sup> Upper House Of The Dutch Parliament - 25 892 - Rules for the protection of personal data (Personal Data Protection Act) (*Wet Bescherming Persoonsgegevens*), Session 1999-2000 N. 92.

<sup>271</sup> <http://curia.europa.eu/juris/liste.jsf?language=en&num=C-275/06>.

infringements of trade mark rights, design rights, copyright and rights related to copyright over the internet.

## Chapter 4: Structure and content

This Chapter 4 analyses the Code in depth, assessing the following elements:

- Role of signatories to the Code and third parties;
- Duties and procedures laid down by the Code;
- Coexistence of measures set out under the Code with European Union and Dutch legal frameworks and related case law;
- Role of technologies used in implementing the duties and procedures laid down by the Code;
- Costs assumed by the parties involved in implementation of the Code;
- Role of educational activities of parties involved in promoting the Code;
- Effectiveness of measures set out by the Code.

This Chapter 4 initially involved exhaustive desk research to identify the signatories to the NTD and third parties. A sample of these were then contacted and interviewed for the purposes of this Chapter 4.

The statements contained in the Chapter 4 on the signatories' and third parties' positions regarding the NTD and day-to-day procedure are based on the feedback and supporting documentation provided by those stakeholders that agreed to participate in Chapter 4.



## 1 Introduction

In 2000, the E-Commerce Directive was issued to set up an Internal Market framework for electronic commerce targeting consumers and business companies. The E-Commerce Directive was an attempt to harmonise, inter alia, European rules on electronic commerce as well as the liability of service providers.

The implementation of this E-Commerce Directive (an initiative of the Dutch government through the Ministry of Economic Affairs and the Ministry of Justice) was crucial for the development of the Code. For this a third party, the NICC, was designated to act as team leader of all negotiations and to draft and develop an NTD. The parties taking part in the meetings for the development and drafting of the Code, apart from NICC, were the ISP Overleg; the BREIN; ISP Connect; the DHPA, representing Dutch associations of ISPs; the Department of Public Prosecution, the Dutch Bureau for reporting child sexual abuse (*Meldpunt Kinderporno*), the Dutch Complaints Bureau for Discrimination on the Internet (*Meldpunt Discriminatie*) and Dutch telecom providers such as KPN.

The Code, which consists of seven articles and notes to the articles, was launched in 2008 and is divided into the following parts:

- Articles of the Code: these regulate its scope, the definitions used, the Intermediary's own notice-and-take-down policy, the reports, the evaluation process, the measures to be taken and the final provisions;
- Explanatory statement: this refers to the Code's main purposes and gives a brief explanation of the origins of the Code and its main characteristics (e.g., it creates no obligations);
- Explanatory notes to the articles.

Generally, a notice-and-take-down procedure establishes how Rightholders or their designated agents (normally rightholders' associations) warn ISPs of infringing content within their services. These notices generally include specific information, such as a description of the intellectual property right in question, the particular location of the infringement on a certain website and the infringing nature of the data or material, paired with a request for prompt removal or the blocking of access to such information. Due to the number of notices Intermediaries receive many responses are delayed leading to sustained infringing activity and blocked material that is even re-posted when 'staydown' duties are not met<sup>272</sup>.

In the Netherlands this notice-and-take-down procedure was embedded in the NTD. This code targets ISPs that provide a public telecommunications service in the Netherlands and have to deal with reports regarding unlawful content on the internet. The Code is self-regulating and as such does not impose any statutory obligation on its subscribers. ISPs can decide whether to subscribe to the NTD or to draft their own notice-and-take-down procedure by using the Code's guidelines. However, every ISP endorsing the Code must make it publicly available (usually on their website) for consultation.

The Code lays down the requirements for Notifiers, Content Providers and ISPs to interact and to remove allegedly unlawful content from the internet. In particular, it addresses the manner in which reports concerning alleged unlawful content on the internet are evaluated by Intermediaries and consequently removed.

One of the main purposes of the Code is for private individuals and organisations to reach an agreement. Furthermore, if in certain circumstances the application of the Code is not effective, the parties can always resort to the police or take the case to court.

Overall, the main objective of this Code is to ensure that every report is dealt with and to improve the speed and efficiency of take-down management and notification.

The following analysis addresses and studies the relevant characteristics of the NTD (the Code).

---

<sup>272</sup> Business Action to Stop Counterfeiting and Piracy '*Roles and Responsibilities of Intermediaries: Fighting Counterfeiting and Piracy in the Supply Chain*'. International Chamber of Commerce. March 2015. Page 57.

## 2. Signatories of the Code and third parties

This Section of Chapter 4 explains the specific role of the four main categories of stakeholders involved in the VCPs: rightholders, Intermediaries, civil society and public authorities.

### 2.1. Role of BREIN

Rightholders of intellectual property rights in the Netherlands have an important role in the application of the NTD. They report on any infringing content on the internet and request its removal. Although rightholders are freely entitled to individually report any infringing content to ISPs, in practice, there is one particular organisation that, inter alia, deals with the majority of reports and claims before Dutch courts: BREIN.

BREIN is a private rightholders association whose aim is to protect entertainment industry rights in the Netherlands. It constitutes a joint anti-piracy program for authors, artists, publishers, producers and distributors of music, film, games, interactive software and books in their fight against intellectual property infringements<sup>273</sup>.

At the beginning of the Code's development, BREIN litigated against several uncooperative ISPs whose collaboration was very important for the Code's success<sup>274</sup>. Moreover, BREIN had already litigated against these ISPs before the Code's implementation (e.g., in 2004 it was responsible for the shutting down of the Dutch 'eDonkey 2000' link giant 'ShareConnector').

Moreover, for issues related to unauthorised copying and distribution of entertainment products, both offline and online, BREIN is a central contact for rightholders, government, law enforcement bodies, trade and media in the Netherlands. BREIN also collaborates in investigations done by the anti-piracy team of the Fiscal and Economic Crime Service that is in charge of criminal investigations<sup>275</sup>.

BREIN examines websites, the legality of their services and content, to identify intellectual property rights infringements. If allegedly unauthorised content is found BREIN informs the website owner, if this is not possible the ISP is informed. Reports submitted to the ISP include BREIN's investigation on the site's management, its illegal aspects, evidence collected and any proof of previous attempts to contact the website owner.

### 2.2. Role of the ECP

In January 1998, the Dutch Ministry of Economic Affairs and the Dutch employers Association<sup>276</sup> backed the founding of the ECP.

The ECP<sup>277</sup> is an independent foundation that acts as an open and independent platform used by the government, companies (providers and users of products and services), civil societies, associations, scientific, educational and research institutions to exchange information and knowledge and join forces to spread information in the Netherlands.

With regard to the NTD, the ECP did not initially help to develop the Code but has done so later on. The ECP is now in charge of administering and developing the NTD. Within the scope of the NTD, the ECP acts as the central organisation, arranging meetings with the main stakeholders twice a year. In these meetings each stakeholder provides its experience (complaints and suggestions) to improve the Code and its application. The process and results are also analysed to confirm they are being fulfilled, for example hosting providers are monitored to see if they are reacting promptly or the number of complaints received is analysed.

ECP's activities not only include stakeholders subject to the NTD but also any individual or organisation interested in the NTD. To be included in ECP's public list of subscribers the interested party has to contact the ECP.

<sup>273</sup> The list of BREIN's participants can be found in Annex 1 of this Chapter 4.

<sup>274</sup> <http://www.ifpi.org/content/library/Razorback-eDonkey-servers-offline-140708.pdf>.

<sup>275</sup> BREIN. 'The art of protecting the creative.' <http://anti-piracy.nl/english.php> (accessed 17 July 2015).

<sup>276</sup> [http://ec.europa.eu/enterprise/sectors/ict/files/reply-en-ecp-nl\\_en.pdf](http://ec.europa.eu/enterprise/sectors/ict/files/reply-en-ecp-nl_en.pdf).

<sup>277</sup> [http://www.cit.sunderland.ac.uk/research/partners/view.cfm?id=125#Vh\\_OAbv7LIU](http://www.cit.sunderland.ac.uk/research/partners/view.cfm?id=125#Vh_OAbv7LIU).

## 2.3. Role of Intermediaries

Intermediaries are essential to ensure development of and compliance with the Code, they either follow the Code or draft their own notice-and-take-down code of conduct.

In this sense, the NTD defines an Intermediary as the ‘provider of a (telecommunications) service on the internet’<sup>278</sup>. Also, the explanatory notes to the Code’s articles specify that an Intermediary can be either a person or an organisation that provides online services to store, transmit or provide information. BASCAP’s<sup>279</sup> and ICC’s<sup>280</sup> report dated March 2015 describes the ‘Roles and Responsibilities of Intermediaries: Fighting Counterfeiting and Piracy in the Supply Chain’ and the E-Commerce Directive gives examples of different types of Intermediaries that can subscribe to the Code such as hosting providers, Intermediaries that act as channels to transmit the code (conduit) or those that provide space on the internet where content can be published by third parties.

On one hand BASCAP defines:

- Mere conduit or internet service (access) providers. An Intermediary has a mere conduit role when it transmits or provides access to a communication network of information provided by a service recipient. These are generally big telecommunication companies but there are also small providers of access services that include technical, automatic and passive roles in providing the service. These services do not involve any regular interaction with consumers, modification of data or the production, publishing or hosting of content. According to this, their role is also relevant for fighting against intellectual property right infringements by blocking access to a website where appropriate<sup>281</sup>.
- Domain name services: the importance of domain names lies in the fact that users identify and access to websites through them (e.g., google.com). Technically, the DNS execute the translation of the domain name into an IP Address. Domain name system registrars or their agents are able to terminate services with sites that are allegedly infringing intellectual property rights<sup>282</sup>.

On the other hand, the E-Commerce Directive defines:

- Internet hosting providers (Host). An Intermediary has a hosting role when it ‘hosts’ or stores information provided by a recipient of the service for customers. Hosts provide this service in two ways: directly through their network or offering the service for third party websites or platforms. The result of these two methods of service provision is that the host has access to the site and can take down content or block its access<sup>283</sup>.

---

<sup>278</sup> Article 1, section b. of the Code.

<sup>279</sup> Business Action to Stop Counterfeiting and Piracy.

<sup>280</sup> The International Chamber of Commerce.

<sup>281</sup> Business Action to Stop Counterfeiting and Piracy. ‘Roles and Responsibilities of Intermediaries: Fighting Counterfeiting and Piracy in the Supply Chain’ International Chamber of Commerce. March 2015. Page 68.

<sup>282</sup> Business Action to Stop Counterfeiting and Piracy ‘Roles and Responsibilities of Intermediaries: Fighting Counterfeiting and Piracy in the Supply Chain’. International Chamber of Commerce. March 2015. Page 65.

<sup>283</sup> Article 14 of the Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN>.

- Caching. An Intermediary has a caching role when the service provided constitutes information storage in an automatic, intermediate and temporary form. This would imply not being involved with the information transmitted, meaning that the Intermediary has no knowledge or control over such information. Therefore, unlawful content can be blocked or taken down upon previous indication<sup>284</sup>.

The most relevant NTD Intermediaries are two main Dutch associations: DHPA<sup>285</sup> and ISP Connect<sup>286</sup>. Both actively participated in the drafting and development of the NTD and its members have to comply with the Code and participate in different initiatives to develop new tools to increase its effectiveness such as the so-called 'Trusted Flagger' or the 'Task Force'. See Section 8 of this Chapter 4 ('Effectiveness').

DHPA represents the leading hosting and cloud providers in the Netherlands and ISP Connect the medium and small hosting providers in the Netherlands. Both associations are deeply involved in the development and application of the Code and inform their members, with adequate notice and in accordance with the Code's standards, if in order that they can perform an adequate notice-and-take-down process should be done.

## 2.4. Role of civil society

No consumer associations have taken part in the development and drafting of the Code. Some consumer associations that we contacted stated that they feel that consumers are not affected by the NTD as it is for ISPs, Rightholders and Content Providers. Notwithstanding this, the BEUC considerations on the enforcement of Intellectual Property Rights in light of consumers' rights in this area have been taken into account throughout the analysis.

---

<sup>284</sup> Article 13 of the Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN>.

<sup>285</sup> <https://www.dhpa.nl/>.

<sup>286</sup> <http://ispconnect.nl/>.

### 3. Duties and procedures

This Section summarises the duties and procedures detailed in the Code. Nevertheless, as stated previously, this Code is essentially voluntary and therefore it works as a framework code and each Intermediary has its own terms and conditions.

To properly illustrate the NTD procedure and the particular duties assigned to the parties of this Code it is important to identify who the relevant parties are:

- **Notifier.** The person or organisation that prepares a report. The Code<sup>287</sup> states that ‘the report concerns the reporting by a Notifier of (alleged) unlawful content on the Internet to an Intermediary with the objective of having this content removed from the Internet.’
- **Content Provider.** The person (or organisation) that has placed (contested) content on the internet. Any Individual, body or organisation that has placed certain content on the internet or that is responsible for space on the internet that a third party is able to use<sup>288</sup>.
- **Intermediaries:** The provider of an internet (telecommunications) service as defined by the Code. Additionally, Intermediaries offer services such as website building and virtual hosting. Intermediaries have the required equipment and telecommunication line access to have internet pop ups within the geographical area the service is provided in.

The NTD does not have an official list of participants; it is difficult to determine or control which Intermediaries have adhered to the NTD or have drafted and published their own Code<sup>289</sup>.

#### 3.1. Scope of application of the VCP

The territorial scope in which the Code is applied is limited to the territory of the Netherlands. This is stated in Articles 1b and Note to Article 1a and 1b of the Code:

- Article 1b states that this Code applies to Intermediaries that provide telecommunication services on the internet in the Netherlands.
- Note to Article 1a states that this Code also applies to every content that is in conflict with laws of the Netherlands.
- Note to Article 1b stipulates that this Code is used where the laws of the Netherlands are applicable. According to Article 1 section b of the Code, the NTD is applicable to Intermediaries in the Netherlands. In addition, the explanatory notes to Article 1a and Article 1b of the Code also establish its applicability to information that is in conflict with laws of the Netherlands and that is publicly available on the internet.

#### 3.2. Procedure

The Code does not provide a complete and systematic notice-and-take-down procedure for Intermediaries, but allows the former to either subscribe to the NTD or to draft their own notice-and-take-down-code of conduct. In the latter case, the Intermediary will have to observe the guidelines proposed by the Code in order to elaborate its own code of conduct<sup>290</sup>.

---

<sup>287</sup> Definition given by the The Notice-and-take-down Code of Conduct.

[http://www.ecp.nl/sites/default/files/NTD\\_Gedragcode\\_Engels.pdf](http://www.ecp.nl/sites/default/files/NTD_Gedragcode_Engels.pdf).

<sup>288</sup> Explanatory Statement of the NTD Code, page 2.

<sup>289</sup> A list of the organisations, which, among others, have endorsed the Code can be found on ECP’s website following this link <https://ecp.nl/werkgroep-notice-and-takedown>. According to this site, BREIN, KPN, SIDN (‘Stichting Internet Domeinregistratie Nederland’), DHPA, ISPConnect, T-Mobile/Online, Marktplaats/Ebay and Google.nl have endorsed the Code.

<sup>290</sup> Article 3 of the Code.

Intermediaries either need to publicly acknowledge their subscription to the NTD or, alternatively, launch their own notice-and-take-down code in accordance with Article 7a and 7b of the Code. This is to ensure that all signatories know who the other subscribers are and to avoid conflicts with other existing NTDs<sup>291</sup>.

The Code aims to empower Intermediaries to deal with reports of allegedly unauthorised content on their clients' websites. Unauthorised content could be intellectual property rights but also other kinds of unlawful content such as that related to terrorism, discrimination or child abuse.

The NTD process begins with the detection and reporting of the allegedly unauthorised content on the internet by an individual or an organisation to the corresponding Intermediary, requesting it to be removed in a report.

According to the NTD, an Intermediary can receive two different categories of reports: (i) those issued by the Public Prosecutor's Office, inspection or investigation services and (ii) those issued by a Notifier (private individual or entity).

### 3.2.1. Report from a Public Prosecutor's Office

According to Article 4a of the NTD, the Dutch Public Prosecutor's Office can issue a report on any unauthorised content on the internet and send it directly to the corresponding ISP. According to the ISP's feedback, when a report is received from a Public Prosecutor's Office the Code is no longer applicable and Dutch law rules. This is because these types of reports do not generally concern alleged copyright or intellectual property rights infringements but relate to other sorts of unauthorised content such as terrorism, discrimination or child abuse. Therefore, it is Dutch law and in particular the Dutch Criminal Code (*Wetboek van Strafrecht*) that is directly applicable.

Article 54a of the Dutch Criminal Code establishes that the Intermediary who receives a request from a Public Prosecutor to stop certain data from being transmitted or stored, will not be prosecuted for its illegality if it complies with the order and removes the unauthorised content. Although Article 54a of the Dutch Criminal Code will be further analysed in Section 4 of this Chapter 4 ('Coexistence of the measures set forth under the VCP with European Union and Dutch legal frameworks and related case'), it is important to note that complying with the Public Prosecutor's Office order limits liability if the Intermediaries themselves comply with the request. This article underlines the power of Prosecuting Officers, whose reports have immediate effect.

In order to avoid liabilities subject to the Dutch Criminal Code, Intermediaries must deal with these reports immediately, without previously evaluating their content as an authorised body<sup>292</sup> will have done so.

### 3.2.2. Report from a Notifier

The Code encourages Notifiers to reach an agreement with the corresponding Content Provider prior to proceeding to report to the Intermediary.

In certain cases, as it may be difficult to discern who the Content Provider is (they could remain anonymous or fail to respond<sup>293</sup>), the Notifier must request the Intermediary for the contact details of the Content Provider (see the explanatory statement of the Code). After the Content Provider, the next party to be contacted is the Website Provider, which will generally be contacted through its online question and answer service. The next party in the chain would be the Hosting Provider, then

<sup>291</sup> The explanatory note to Article 7b of the Code states: 'This provision is included to prevent conflict with other NTD procedures that already exist. Websites that are based on a very large amount of input from third parties for example (such as advertisement sites and sites to which photos and videos can be uploaded), have NTD systems that for reasons of practicability are not based on direct communication with the Content Providers'.

<sup>292</sup> Explanatory notes to the Articles of the Code, note to Article 5a.

<sup>293</sup> For example, there are certain services that operate with technical features that hide the real IP address from where the content is delivered, in these cases only these service providers know the real IP address making it take longer to identify the owner and remove the content.

the Internet Access Provider and finally the Physical Access Provider (cable, glass or fibre). Notwithstanding this, most of the Intermediaries interviewed affirm that in practice, once they are informed by the Notifier, they will try to resolve the conflict usually by way of emails. Nonetheless, the Code does not state which means of communication should be used.

Reports can be about unlawful content or ‘undesirable content’ (according to criteria published by Intermediaries). Notifiers are responsible for the accuracy and completeness of their reports and must include all information specified in Article 4b of the Code such as the contact details of the Notifier, the location (URL) of the content and the reason why the content is considered unlawful or undesirable.

According to Article 5 of the NTD Intermediaries must evaluate Notifiers reports. In practice this process begins by checking the reported website’s activity and whether the Content Provider has authorisation to exercise the allegedly unlawful activity. The Code does not establish a mandatory deadline for Intermediaries to do this, it only suggests that five (5) days is a reasonable timeframe for this to be done in. However, if the concerned Intermediary follows its own notice-and-take-down code of conduct, the evaluation must take into account the standards and deadlines established therein.

Despite the lack of an official deadline in the Code to evaluate any infringing content, in practice this takes between two and three days although each case is different.

Notifiers can exceptionally request Intermediaries to evaluate a report immediately. Article 4c of the Code provides that the Notifier must provide the Intermediary with a complete and detailed explanation of why the Report should be dealt with as a matter of urgency. In any case, the final decision on whether to deal urgently with a Report remains with the Intermediary. The explanatory notes to Article 4c of the Code give an example of a report to be dealt with as a matter of urgency: unlawful content already removed from the internet and placed in another location. In this case scenario Notifiers can inform the corresponding Intermediary and request it to urgently remove, justifying its request by enclosing a copy of the previous report. The main logic behind this approach is the importance that the Code contributes to the ‘stay-down’ of infringing content so that content already removed does not reappear on other websites.

Once the Intermediary has evaluated a report, different actions are taken depending on the results obtained:

### *3.2.2.1. There is no doubt about the unlawfulness of the content*

As established in Article 6b of the Code, if the Intermediary has no doubt about the unlawfulness of the content, all measures must be taken in order to take it down. Nevertheless, this only takes place when the unlawful content is evidently illegal, like, for instance, child abuse content. Otherwise, it is very challenging for an Intermediary – who is not an expert on intellectual property rights - to determine whether certain content infringes copyright or any other intellectual property right. Moreover, if the Intermediary determines the content is unequivocally unlawful when it is actually not, the latter may be held liable for any possible damages arising from the take-down measure<sup>294</sup>.

As soon as the Intermediary identifies that the content is unequivocally unlawful it must take all measures necessary to take down the unauthorised content. According to the notes of Article 6b of the Code, if possible, Intermediaries should first request the Content Providers to remove the unlawful content<sup>295</sup> themselves, but if not possible it is up to the Intermediaries to remove it.

---

<sup>294</sup> The European Digital Rights (EDRi), an association of civil and human rights organisations from across Europe, read a draft of this document and stated that: ‘‘Takedown’’ is a broad term which can be applied in various ways. The Code does not provide any guidance on this issue, missing the opportunity to introduce various safeguards and best practices. For example, it is preferable to make content inaccessible to certain parties rather than to delete it entirely. Likewise, the interference should be as limited as possible in light of the notice’s scope: for example, when the notice is directed at an image on a web page, the Intermediary should only to make that image inaccessible rather than the entire web page.’

<sup>295</sup> EDRi, after reading a draft of this document, noted that an order of types of Intermediaries to be approached to obtain contact information should be established. EDRi considers that ‘Notifiers should first approach hosting providers and afterwards ISPs etc. This is not reflected in the operative part of the Code. Since the measures possible at each step up the chain is more disproportionate than the one before, this principle should be translated into an explicit requirement. This principle of priority should apply not only to information



### 3.2.2.2. *The Intermediary considers the content is legitimate*

Article 6a of the Code establishes that if the Intermediary finds the content referred to in the report to be legitimate it must inform the Notifier and explain why it reached that conclusion.

### 3.2.2.3. *The Intermediary is not able to unequivocally determine whether the content is unlawful*

#### 3.2.2.3.1. THE CONTENT PROVIDER IS KNOWN

In the event the Intermediary is unable to decide whether the content is unequivocally unlawful or not, the Code encourages, when the Content Provider is known, the Intermediary to act in two specific ways:

- Contact the Content Provider<sup>296</sup> to inform them about the Report and request the removal of the infringing content, or;
- Advise the Notifier to reach an agreement with the Content Provider. If there is no possibility of reaching an agreement with the Content Provider, the Notifier has two options depending on the nature of the content concerned:
  - If it is believed that the concerned content involves a criminal offence, the official report can be submitted to the police or;
  - If the content concerned is considered to be unlawful under civil law, the Notifier can take the dispute with the Content Provider to court.

#### 3.2.2.3.2. THE CONTENT PROVIDER IS UNKNOWN

Despite the aforementioned, the Content Provider might be unwilling to make themselves known to the Notifier, and deadlock may occur leaving the Intermediaries with the following options:

- Provide the Notifier with the contact details of the Content Provider, with a view to try to reach an agreement or;
- Remove the content concerned. In this case, the Code requires the Intermediary to handle the situation with due caution and to ensure that no more content than that referred to on the Report is removed. In practice, when the content cannot be determined as unequivocally unlawful, Intermediaries usually suggest that the Notifier takes action against the Content Provider before a court, before proceeding to remove the content themselves, in order to avoid any kind of liability<sup>297</sup>.

According to one of the stakeholders interviewed, if it is not possible to identify who the Content Provider is, the Intermediary will refer the Notifier to court. Also, it was explained to us that in practice, the privacy of the Content Provider is maintained.

---

requests, but also to takedown requests. If someone further down the chains receives a takedown request, their first question should be 'have you already tried to resolve the issue with the Content Provider and with other Intermediaries?'

<sup>296</sup> EDRI, after reading a draft of this document, considers that 'the Code generally lacks detailed rules on the circumstances and conditions for contacting the Content Provider. [...], prior notification of the Content Provider can objectively be considered to be essential (as indeed, has recently been required by the The Hague District Court in a case concerning copyright infringement on Google Play). Rb. Den Haag (vz) 06.11.2015, ECLI:NL:RBDHA:2015:12706. (Google v. BREIN).'

<sup>297</sup> The Code establishes that 'The Intermediary can decide to provide the Notifier with the Content Provider's name and contact details or to remove the content concerned. The Intermediary exercises due caution in the execution of the measures that have to be taken to ensure that the removal of any more content than that to which the report refers is avoided.'

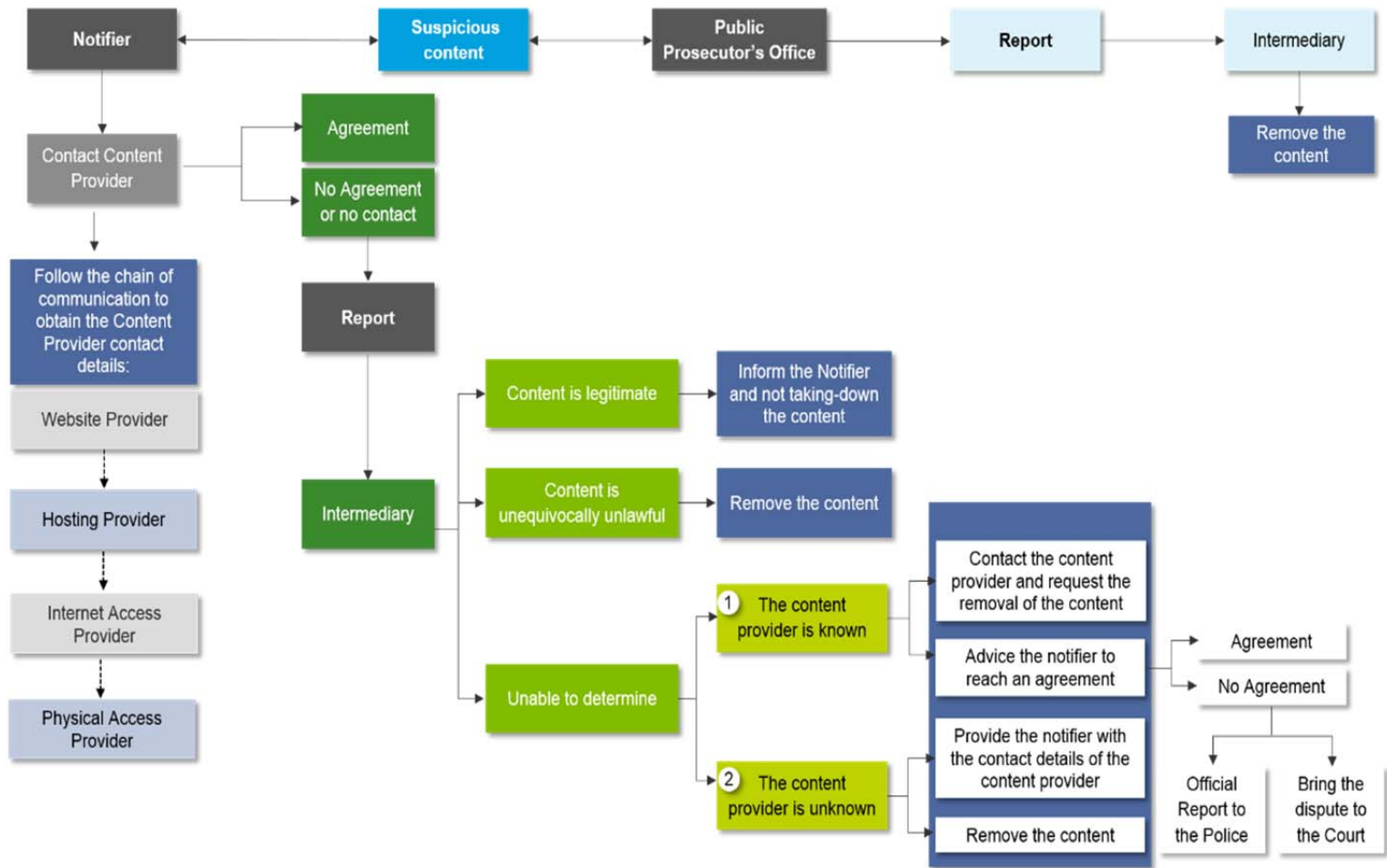
### 3.3. Penalties and sanctions

The Code does not set forth any penalty or sanction for the non-observance of its provisions by its signatories. As a voluntary collaboration practice, Intermediaries are entitled to freely sign the Code or draft their own notice-and-take-down code of conduct. Therefore, establishing a penalty for Intermediaries would not be in line with the nature and aims of the Code. Even if an Intermediary takes more than seven days to resolve its evaluation process it does do so, every report is dealt with and this is in line with one of the Code's main goals.

According to Intermediaries' feedback, some of them have banned certain hosting providers from their associations for refusing to comply with the Code. If their members want to become part of these associations they have to comply with the NTD.

Finally, if an Intermediary does not comply with the corresponding court order whereby it must take down any unauthorised content it will have to face legal consequences for non-compliance with a court resolution in accordance with Dutch law.

### 3.4. NTD procedure flowchart



### 3.5. NTD in the Netherlands

As previously stated, Article 3 of the Code establishes that Intermediaries can draft their own notice-and-take-down code of conduct and it further specifies ‘that the public must be able to consult and that it is consistent with this code’. Intermediaries are also required to determine in which manner and in what time frame reports shall be evaluated and define what they consider to be ‘undesirable content’ in their public conditions of use.

According to the aforementioned, notice-and-take-down codes have been implemented in numerous companies present in the online environment in the Netherlands such as SIDN<sup>298</sup>, Layar<sup>299</sup>, WeTransfer<sup>300</sup>, Drillster<sup>301</sup> and eBay<sup>302</sup>. An analysis of their codes of conduct shows that most measures for the take down of unlawful content are common to all of these companies’ procedures, but there are also certain divergences.

The Code establishes that any unlawful content must be reported on. These reports must always include certain details established by the Code and also some additional documents or information such as proof of failed attempts to contact the Content Provider. Also, in some cases, the importance of considering the chain of responsibility and communication between all parties involved is explicitly stated<sup>303</sup>. All communications are sent by email.

All reports are evaluated to decide whether to remove the content in question or not. In the case of Layar, WeTransfer and Drillster if the content concerned is found to be clearly not unlawful or illegal, a notification is sent to the Notifier explaining why the content should not be removed. On the other hand, if it is determined that the content is unequivocally unlawful, the content concerned will be removed. Finally, if it is not clear whether a content is unlawful or not the Content Provider is asked to remove the content or to contact the Notifier.

However, SIDN, a company registering and managing domain names in the Netherlands, limits the scope of its notice-and-take-down code. Complainants may ask SIDN to either release the details of an offending domain name’s registration or, as a last resort, make a domain name unreachable by removing the link between the domain name and the associated IP address. In the latter case, a notice-and-take-down request form has to be completed, including all the necessary attachments, for SIDN to assess.

eBay has created its own so-called Verified Right Owners Program. This makes it easier for rights owners to request (report on) the removal of listings or items containing materials that infringe their intellectual property rights. The Verified Right Owners Program simplifies the take-down procedure; eBay reviews all notifications from the ‘Verified Right Owners’ and consequently might remove the alleged infringing content as well as reject inappropriate or non-intellectual property related claims<sup>304</sup>.

Furthermore, other organisations such as WeTransfer, Layar or Drillster have their own different NTD procedures. All three organisations, when receiving a report from a Public Prosecutor, automatically consider it to be reliable and therefore they remove any infringing content without questioning it.

On the issue of indemnity in these take down cases, there is a discernible uniformity between these companies’ take-down procedures and the explicit indemnity and lack of liability stated for any action arising from performing the take-down at issue.

<sup>298</sup> ‘SIDN Notice and Take Down Procedure.’ [https://www.sidn.nl/a/nl-domain-name/complaining-about-the-content-of-a-website?language\\_id=2](https://www.sidn.nl/a/nl-domain-name/complaining-about-the-content-of-a-website?language_id=2) (accessed 3 July 2015).

<sup>299</sup> ‘LAYAR Notice and Takedown Code.’ <https://www.layar.com/legal/notice-takedown/> (accessed 3 July 2015).

<sup>300</sup> ‘WETRANSFER Notice and Take Down Policy’ <https://www.wetransfer.com/documents/ntd.pdf> (accessed 3 July 2015).

<sup>301</sup> ‘DRILLSTER Terms of Service.’ <https://www.drillster.com/info/es/tos> (accessed 3 July 2015).

<sup>302</sup> ‘eBay VERO Take-Down Requests.’ <http://www.ebay.com/gds/eBay-VERO-take-down-requests-/10000000019095038/g.html> (accessed 3 July 2015).

<sup>303</sup> On this detail, companies such as SIDN or Layar indicate the need to, firstly, take the matter up with the first party in this chain, namely, the publisher of the unlawful content or the Content Provider. In the event that reaching an agreement with the latter is impossible, a report can be issued to the email provided by the organisation for this purpose.

<sup>304</sup> The E-Bay Verified Right Owners Program: <http://www.ebaymainstreet.com/issues/verified-rights-owners-programme-vero>.

Overall, it can be inferred that the main principles of the NTD are embedded in these companies' codes, yet, as allowed by the Code, these still personalise certain aspects of the procedure in relation to the nature of their business.

### 3.6 Notes on other Notice-and-take-down procedures in other countries: United States of America and Japan

Notice-and-take-down codes have been established in different countries worldwide, not only in Europe but also in countries such as the United States of America or Japan.

Notice-and-take-down Codes of Conduct of the United States, Japan and the Netherlands have similar characteristics despite being developed in different countries with different legislations. None of the Codes have a legislative character regulating their notice-and-take-down procedure. However, all of them have certain legal provisions that act as a guideline. For example, Japan has the Trade mark Law<sup>305</sup>, the Intellectual Property Basic Law<sup>306</sup> and the Law on the Limitation of Liability. In the United States, notice-and-take-down provisions are covered by the DMCA. Lastly, in the Netherlands, the incentive for the development of notice-and-take-down procedures is laid out in the E-Commerce Directive, which differs from the DMCA in that it deals with different issues regarding electronic commerce and not only copyright infringement.

Additionally, all the established requirements to carry out a notice-and-take-down are very similar in these countries, with very few disparities. Regarding the disparities, in Japan for instance, only rightholders or their representatives can issue reports and initiate the process. In the United States the signature of an authorised individual to act on behalf of the rightholder alleging the infringement is needed. By contrast, in the Netherlands, anyone can initiate the process by reporting an infringement. Also, in the Netherlands it is preferable to reach an agreement with the Content Provider before contacting the Intermediary.

Despite these singularities, the process in these three countries has the following steps in common:

- (i) The rightholder, or in the case of Netherlands anyone who considers there is unlawful content on the internet, will contact the Intermediary and inform of any infringement, in a written request, that must include information about: a) the specific content infringing their rights, b) the right infringed and c) the reason for alleging such infringement.
- (ii) Once the notification is submitted, the Intermediary must examine the request in order to assess and decide on whether there is an intellectual property infringement or not.
- (iii) When, after the examination, it is established that the content at issue is not unlawful, the Intermediary will inform the Notifier and explain the reasoning behind it.
- (iv) If, on the other hand, the content turns out to be unlawful, it will be removed.

Moving on to consider Intermediaries' liabilities, notice-and-take-down procedures in the USA, Japan and the Netherlands envisage a limitation to liability or 'Safe Harbor'<sup>307</sup> whereby Intermediaries won't be held liable when complying with certain requirements under particular circumstances. In Japan this 'Safe Harbor' provision is regulated under Article 3 of the Law on the Limitation of Liability. Meanwhile, in the United States, the rules relating to Intermediaries' liabilities are covered by the DMCA in its Article 17 U.S.C. § 512(c) (3) (A). Finally, in the Netherlands the 'Safe Harbors' derive from Articles 12 to 14 of the E-Commerce Directive, which will be further explained in Section 4 of this Chapter 4 ('Coexistence of the measures set forth under the VCP with European Union and Dutch legal frameworks and related case law').

<sup>305</sup> Trade mark Law. [http://www.wipo.int/wipolex/en/text.jsp?file\\_id=188401](http://www.wipo.int/wipolex/en/text.jsp?file_id=188401).

<sup>306</sup> Intellectual Property Basic Law <http://www.wipo.int/edocs/lexdocs/laws/en/ip/ip098en.pdf>.

<sup>307</sup> BASCAP report 'Roles and responsibilities of Intermediaries: fighting counterfeiting and piracy in the supply chain', page 13.

Intermediaries also have to consider secondary liabilities<sup>308</sup>. According to the Legal Information Institute, Cornell University Law School<sup>309</sup>, secondary liability occurs when ‘a person may be held liable for infringement even though he or she did not actually engage in infringing activities’. This means that in certain cases passive Intermediaries could be held liable for copyright infringement when they are not protected by the ‘Safe Harbor’ provision (for not accomplishing the requirements needed). In this regard, international courts have adopted different approaches regarding secondary liability. Moreover, some of them have decided cases by establishing that certain Intermediaries should be held liable for facilitating the infringement of intellectual property rights.

Overall, the most important difference between Europe and the United States is that in European countries failure to comply with a notice-and-take-down code does not entail any sort of liability in contrast with American law where there are no notice-and-take-down codes and the main statutory law governing liability is the DMCA. Furthermore, in Europe liability will only arise if there is a standard for secondary liability under the specific national law of the country. This is due to the fact that the E-Commerce Directive authorises liability exemptions for passive Intermediaries who do not play an active role collaborating with the users<sup>310</sup>. In this sense, Recital 42 in the preamble of this Directive, states:

(...) the exemptions from liability established in this Directive cover only cases where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient; this activity is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored.

---

<sup>308</sup> Graeme B. Dinwoodie ‘Secondary Liability for Online Trademark Infringement: The International Landscape’.

<sup>309</sup> [https://www.law.cornell.edu/wex/contributory\\_infringement](https://www.law.cornell.edu/wex/contributory_infringement).

<sup>310</sup> Emerald Smith, ‘Lord of the Files: International Secondary Liability for Internet Service Providers’, page 1573.

## 4. Coexistence of the measures set forth under the VCP with European Union and Dutch legal frameworks and related case law

This Section 4 of the Chapter 4 ('Coexistence of the measures set forth under the VCP with the European Union and Dutch legal frameworks and related case law') summarises both European Union and Dutch legal frameworks and any related case law that may impact on the practical application of the Code's provisions.

The considerations included in this Section are based upon the following hierarchy of legal sources:

- Charter of Fundamental Rights in Section 4.1.1. of this Chapter 4 ('Charter of Fundamental Rights').
- European Convention on Fundamental Rights in Section 4.1.2. of this Chapter 4 ('European Convention on Human Rights').
- European Union Directives in Section 4.2. of this Chapter 4 ('European Union Directives').
- Constitutional prerequisites and fundamental rights in the Netherlands in Section 4.3. of this Chapter 4 ('Constitutional prerequisites and fundamental rights in the Netherlands').
- Dutch Regulations in Section 4.4. of this Chapter 4 ('Dutch Regulations').

### 4.1. Fundamental rights

#### 4.1.1. Charter of Fundamental Rights

Certain measures envisaged by the Code may have an impact on the following fundamental rights provided for by the Charter of Fundamental Rights<sup>311</sup>:

- Article 8: 'Protection of personal data'. This right generally serves to protect the self-determination right of an individual regarding the use of personal data related to them.
- Article 11: 'Freedom of expression and information'. This Article protects the right of every individual to express itself about every aspect they want as well as the freedom to impart and receive ideas and information.

The enforceability and acceptability of self-regulatory measures like this Code depends on, inter alia, whether the fundamental rights of the persons concerned have been taken into consideration.

In light of such considerations, a fair balance between the interests of the parties concerned is required while VCP models have to respect and safeguard the aforementioned fundamental rights.

#### 4.1.2. European Convention on Fundamental Rights

Certain measures envisaged by the Code may have an impact on the following fundamental rights provided for by the European Convention on Human Rights<sup>312</sup>:

- Article 8: 'Right to respect for private and family life'. This right protects respect for one's private life and states that it cannot be interfered with by a public authority unless it is required by law and for the benefit of society.
- Article 10: 'Freedom of expression'. This Article states that freedom of expression must be protected and safeguarded.

---

<sup>311</sup> See complete wording in Annex 3 of this Chapter 4.

<sup>312</sup> See complete wording in Annex 3 of this Chapter 4.



## 4.2. European Union Directives

Certain measures envisaged by the Code may have an impact on the following provisions of the European Union Directives<sup>313</sup>:

- Article 12 of the E-Commerce Directive. This Article obliges Member States to ensure that an Intermediary acting in the role of a mere conduit will not be liable for the content it transmits or stores when it neither initiates the transfer of the information it is providing, nor selects the receiver of the transmission, nor selects or modifies the information contained in such a transmission.
- Article 13 of the E-Commerce Directive. This Article obliges Member States to ensure that Intermediaries with a caching role will not be liable for the information they store in the following events

(...) (a) the provider does not modify the information; (b) the provider complies with conditions on access to the information; (c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry; (d) the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of information; and (e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access has been disabled, or that a court or an administrative authority has ordered such removal or disablement (...).

- Article 14 of the E-Commerce Directive. This Article obliges Member States to ensure that Intermediaries with a hosting role will not be liable for the content stored on their services by means of a request from a consumer or third party when either the Intermediary has no information or knowledge of the illegal activity or content, or after acquiring such knowledge removes or disables access to the unauthorised content.
- Article 15 of the E-Commerce Directive. This Article prohibits Member States from imposing a general obligation on Intermediaries to monitor the information they transmit or store or to seek facts or circumstances indicating illegal activity when providing hosting, mere conduit or caching services.
- Article 11 of the Enforcement Directive. This Article encourages Member States to ensure that rightholders are in a position to apply injunctions against Intermediaries whose services are used by a third party to infringe intellectual property rights.
- Article 7(f) of the Data Protection Directive. This Article permits Member States to process personal data when it is necessary for the purposes of the legitimate interests pursued by the Controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests of fundamental rights and freedoms of the data subject.

The aforementioned European Union Directives have been at issue in the following CJEU cases<sup>314</sup>:

- Bonnier CJEU Ruling

This Ruling establishes that an Intermediary has to consider the Content Providers' privacy rights and not only the Notifier's intellectual property rights when disclosing personal information from the Content Provider to the Notifier. This may impact on the Dutch VCP since the Code foresees the disclosure of the personal data of the Content Provider<sup>315</sup>.

<sup>313</sup> See complete wording in Annex 3 of this Chapter 4.

<sup>314</sup> See detail description in Annex 6 of this Chapter 4.

<sup>315</sup> <http://curia.europa.eu/juris/document/document.jsf?text=&docid=121743&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=196710>.

- Promusicae CJEU Ruling

This Ruling establishes that the protection of intellectual property rights is not of a higher order than other fundamental rights meaning that the protection of intellectual property rights does not prevail over other rights such as data protection.

### 4.3. Constitutional prerequisites and fundamental rights in the Netherlands

Certain measures envisaged by the Code may have an impact on the following fundamental rights set forth by the Dutch Constitution<sup>316</sup>:

- Article 7: 'Freedom of Expression'. Protects the right of Dutch citizens to publish thoughts or opinions of Dutch citizens. It also ensures, inter alia, the prohibition of censorship on radio or television broadcasts by establishing that there shall be no prior supervision of the contents published on those media.
- Article 10: 'Privacy'. Protects the right of individuals to have accurate knowledge in relation to the data processing of their personal data, as well as of the data recorded concerning them.

### 4.4. Dutch Regulations

As a member of the European Union, the Netherlands has implemented into national law the European Union Directives analysed previously in this Chapter 4. Certain measures included in the Code may have an impact on the following articles of the Dutch Regulations<sup>317</sup>:

- Article 6:162c of the Dutch Civil Code defines a tortious act as an act or omission violating a law-imposed duty from which a violation of a third party right results.
- Article 6:196c of the Dutch Civil Code implements Articles 12-14 of the E-Commerce Directive regarding the different types of Intermediaries that exist (mere conduits, caching and hosting).
- Article 54a of the Dutch Criminal Code implements Article 13 of the E-Commerce Directive regarding the liability of the caching Intermediary.
- Article 8 of the PDPA implements the Data Protection Directive.

The Dutch Regulations have been considered by the Dutch Courts in the following cases:

- Decision of the District Court of The Hague, 24 October - *BREIN v XS Networks B.V.*

This decision deals with a conflict between the intellectual property rights of the rightholders and the data protection rights of the Content Providers as well as with the issue of the liability of Intermediaries. In this case, the Court declared that *XS Networks* acted unlawfully and had to assume liability as they were aware of the unlawfulness of the activities of the Content Provider and had not removed the content or forwarded the contact details to *BREIN*.

- Decision of the Dutch Supreme Court, 25 November 2005 - *Pessers v Lycos*

In this decision the main issue was the disclosure of personal data. *Pessers* (a well-known eBay stamp seller) requested *Lycos* (a Dutch hosting provider of a website containing information criticising *Pessers*) to disclose personal information of the site's Content Provider. *Lycos* refused to do so alleging that the mentioned content had not been proven to be unlawful. In addition, the Dutch Supreme Court declared that even though freedom of expression is truly significant it is not an absolute right and depending on the circumstances different interests may prevail.

---

<sup>316</sup> See complete wording in Annex 4 of this Chapter 4.

<sup>317</sup> See complete wording in Annex 4 of this Chapter 4.

- Decision of the Court of The Hague, 4 September 2003 - *Scientology v XS4ALL13*

In this decision the Court stated that Intermediaries are not publishing information themselves but simply providing the means for third parties to publish and therefore they are not themselves infringing any copyright. Nonetheless, the Court clarified that, whenever an Intermediary receives notice of unauthorised content on a website, it must take the necessary steps to remove it. So in the event an Intermediary is notified and does not remove the alleged unlawful content, it would be acting unlawfully. This decision acknowledges the different types of Intermediaries according to their role as established in the E-Commerce Directive and implemented in the Dutch Civil Code.

- Decision of the District Court of Utrecht, 9 July 2002 - *Teleatlas v Planet Internet*

This decision concerned a conflict between data protection and intellectual property rights. In this specific case, the District Court stated that a request for the release of personal data should be dealt with under Article 8 of the PDPA. This article permits the disclosure of personal data, when it is strictly necessary, in order to assert the interests of the controller and the interests of the person whose data will be processed do not prevail. Additionally, the Court stressed that other measures should also be taken to retrieve the person's data.

#### 4.5. Analysis of the VCP in relation to the European Union and Dutch legal frameworks and case law

In light of the European Union and Dutch legal frameworks and the related case law discussed in the preceding Sections of this Chapter 4, it appears that certain duties and procedures envisaged by the Code may raise issues with regard to certain fundamental rights or legal provisions. This Section contains an analysis of the following rights:

- Article 3b of the Code regarding the determination of 'undesirable content' by the Intermediary;
- Article 4a and 5c of the Code regarding notification from the Public Prosecutors Office to take down unlawful content;
- Article 6 of the Code regarding performance of the evaluation process by Intermediaries and removal of infringing content;
- Article 6c of the Code regarding disclosure of the Content Providers' personal data by the Intermediary.

Pursuant to the Promusicae CJEU Ruling, the protection of intellectual property rights will not be understood as being of a higher interest than other fundamental rights. Therefore, during the subsequent analysis, the impact of the Code on the following fundamental rights will be reviewed in detail:

- Freedom of expression of the Content Provider (Section 4.5.1);
- Right to the protection of personal data related to the Content Provider (Section 4.5.2).

In addition, it will also be analysed as to, whether certain duties established by the Code are in line with Articles 12 to 15 of the E-Commerce Directive as well as Articles 6:162c and 6:169c of the Dutch Civil Code, Article 54a of the Dutch Criminal Code and Article 8 of the PDPA.

As established above, due to the voluntary nature of the Code it only serves as a guideline for Intermediaries to be able to develop their own public notice-and-take-down procedures. The exact implementation of the Code by Intermediaries through their own procedures will be decisive in determining the legal grounds and safeguards that are put into place. However, the NTD establishes methods to help Intermediaries operate with care within the existing legal framework and with respect to third party rights.

##### 4.5.1. Coexistence of the Code with the freedom of expression of the Content Provider

As already mentioned, freedom of expression is a fundamental right protected by both the European Convention on Fundamental Rights and the Charter of Fundamental Rights. Every individual has the right to express themselves as well as the freedom to impart and to receive ideas and information.

The following Sections analyse whether the application of the Code may put at risk Content Providers' freedom of expression.

#### *4.5.1.1. Intermediaries' and 'undesirable content'*

Firstly, it should be assessed whether what an Intermediary considers to be undesirable content could have an impact on Content Provider's freedom of expression.

According to Article 3b of the NTD, Intermediaries are allowed to draft the conditions governing the use of the services they are offering. In particular, these conditions shall include criteria establishing what may be classified as undesirable content. The aim of this provision is to grant Intermediaries the opportunity to decide which content they do not wish to transmit or to store.

Undesirable content goes further than the notion of unlawful content. Indeed, unlawful content is content that contravenes the applicable law<sup>318</sup> and, as far as undesirable content is concerned, it is the Intermediary and not the law who considers and determines the nature of the content.

Therefore, although ISP Intermediaries are entitled to establish which content is undesirable, the content to be removed could indeed be legal. Consequently, the meaning of 'undesirable content', which exceeds the parameters of lawfulness, could be subject to an action if it is in conflict with the right of freedom of expression of the Content Provider.

According to the information obtained in the interviews for this Chapter 4, to avoid any risk Intermediaries do not usually remove content that is not clearly illegal. They recommend the rightholder(s) to start a judicial procedure to determine whether the disputed content is illegal.

#### *4.5.1.2. Evaluation process by Intermediaries and removal of unlawful content*

According to Article 4a of the Code, Intermediaries have to ensure, that they remove any content which is 'unequivocally unlawful'.

Some of the content could be evidently unlawful such as child pornography or informational crimes related to terrorism (e.g., incitement or terrorism), therefore no conflict with the right of freedom of expression will arise and the content must be immediately removed. Nevertheless, in other cases, the Intermediary's decision about unequivocal unlawfulness of the content is less clear. In order to avoid any conflict with the Content Provider's freedom of expression Intermediaries have to ensure that the content they are removing is unequivocally unlawful.

According to Article 4b of the Code, reports from a Notifier concerning unlawful content need to comply with certain content requirements. Among others, the Notifier needs to justify why the content of the report is unlawful or why it conflicts with the criteria for undesirable content established in the Intermediary's own notice-and-take-down code of conduct. After receiving a report, the Intermediary has to evaluate it to determine whether the reported content is unlawful and/or punishable (criminal content)<sup>319</sup>. Nonetheless, the Intermediary will not make this evaluation if the report comes from an investigation regarding a criminal offence resulting from an inspection or investigation service or from the Dutch Public Prosecutor's Office<sup>320</sup>.

The aforementioned Article 6 of the NTD establishes that, if as a result of the evaluation process, the Intermediary resolves that the content is unequivocally unlawful, the latter shall immediately remove or disable content. Likewise, if possible, the Intermediary shall firstly inform the Content Provider of the report and the fact that their web content has been found to be unlawful and secondly, if necessary, assist the internet ISP to remove the unlawful content<sup>321</sup>.

---

<sup>318</sup> Note to Article 3b of the NTD Code.

<sup>319</sup> Paragraph a, Article 4 and Paragraph b, Article 5 of the NTD Code.

<sup>320</sup> What constitutes an inspection or investigation service is not quite clear, although it often refers to procedures of public authorities.

<sup>321</sup> In this regard, the Court of the Hague in its decision dated on the 4 September 2003 between Scientology and XS4ALL13, which will be further detailed in Section 4.4 of this Chapter 4 ('Dutch Regulations'), clarified that once the ISP notices that one of its clients has provided illegal information, the ISP has the duty to remove such unauthorised content.

Intermediaries must be very diligent throughout the evaluation process and study of reports provided by Notifiers. It is important to reach the most favourable balance possible between the involved parties' rights. If the removal of the content does not follow an appropriate balancing test between the involved parties' rights, this process may be in conflict with the duties of care<sup>322</sup> that the Intermediary has with regard to the Content Provider's right to freedom of speech.

Despite the aforementioned, the right of freedom of expression may be limited when conflicting with other rights and principles such as the right to privacy, intellectual property, libel, slander, public order and others<sup>323</sup>. A removal of content is not in violation of this fundamental right of expression if these other rights precede.

In fact, according to information obtained in the interviews for this Chapter 4 Intermediaries avoid risks by not usually removing content that is not clearly illegal according to their evaluation process. In such cases they recommend pursuing justice in order to determine if the disputed content is illegal or not and if it is found to be illegal they then order it to be removed<sup>324</sup>.

#### 4.5.1.3. Notification from the Dutch Public Prosecutor's Office

The NTD also refers to situations where Intermediaries receive a notification from the Dutch Public Prosecutor's Office ordering the removal of certain unlawful content.

According to the Code, unlawful content is to be understood as any content in conflict with civil law<sup>325</sup>. Furthermore, Article 6:162 of the Dutch Civil Code confirms this approach<sup>326</sup>.

In line with Article 54a<sup>327</sup> of the Dutch Criminal Code a prior authorisation of an examining judge (*'rechter commissaris'*) is required for the removal of unlawful content. As per the Note to Article 54a of the Dutch Criminal Code, the Intermediary has to immediately remove the disputed content without initiating an evaluation procedure.

Therefore, the chain of communications in a Criminal Code procedure would be: (1) the Dutch Public Prosecutor's Office informs the judge of the unlawful content located within the services provided by an Intermediary. (2) In the event that the judge issues the corresponding authorisation for its removal, the Dutch Public Prosecutor's Office is entitled to notify the Intermediary ordering it to immediately remove the unlawful content. Intermediaries would be obliged to remove the illegal content.

As regards the NTD, neither Article 4a nor Article 5a of the Code address the requirement of a judge's authorisation for content removal, as established in the Dutch Criminal Code. It is only states that if the Dutch

<sup>322</sup> The concept of 'due care' is foreseen under Article 6:162 of the Dutch Civil Code. An interpretation and applicability of the concept of 'due care' relies on specific facts and circumstances, it could be understood that the ISP could be liable for damages committed by an act or an omission that is in breach of the law or the unwritten duty of care.

<sup>323</sup> Court of First Instance Haarlem 14 May 2008 (ECLI:NL:RBHAA:2008:BD1446) and Court of First Instance 8 May 2014 (ECLI:NL:RBMNE:2014:3637).

<sup>324</sup> The International Video Federation (IVF), in commenting on a draft of this document noted that 'Complaints are made by the right holders themselves or by the signatory content protection organization that represents the vast majority of copyright content holders, i.e. BREIN, and therefore enjoys a high degree of reliability. If a right holder states that a website is unlawfully making available its content, hosting providers should be able to make a decision in good faith to take measures as a diligent economic operator.'

<sup>325</sup> Paragraph a, Article 1 of the NTD Code states '(...) 'A distinction must be made between information that constitutes a criminal offence and information that is conflict with civil law (unlawful).'

<sup>326</sup> Article 6:162: Definition of a 'tortious act': '1. A person who commits a tortious act (unlawful act) against another person that can be attributed to him, must repair the damage that this other person has suffered as a result thereof. 2. As a tortious act is regarded a violation of someone else's right (entitlement) and an act or omission in violation of a duty imposed by law or of what according to unwritten law has to be regarded as proper social conduct, always as far as there was no justification for this behaviour. 3. A tortious act can be attributed to the tortfeasor [the person committing the tortious act] if it results from his fault or from a cause for which he is accountable by virtue of law or generally accepted principles (common opinion)'. For more information, see Annex 4.

<sup>327</sup> Article 54a: 'An Intermediary which provides a telecommunication service that consists of the transfer or storage of data from a third party, shall not be prosecuted in its capacity as Intermediary telecommunication provider if it complies with an order from the public prosecutor to take all measures that may be reasonably required of it in order to disable this data, which order shall be issued by the public prosecutor after he has applied for and received a written authorisation from the examining magistrate'. For more information, see Annex 4 of Chapter 4.

Public Prosecutor's Office orders an Intermediary to remove unlawful content regarding a criminal offence, then it must ensure that all measures available are taken to do so and without any prior evaluation.

This would mean that the Public Prosecutors' Office could issue a notification declaring content unlawful under civil law<sup>328</sup>, obliging the Intermediary to automatically remove it without the involvement of a judge.

The mentioned action could raise issues concerning the duty of care of ISPs with regard to the Content Providers' freedom of speech.

However, according to the information provided by ISPs, as far as can be assessed at present, the Dutch Public Prosecutors' Office does not declare unlawfulness under civil law and no Public Prosecutor Report has been issued for matters not related to criminal offences. Therefore, in practice, there is no risk of conflict with Content Provider's rights of freedom of expression.

#### 4.5.2. Coexistence of the Code with data protection and privacy

This Section analyses whether certain duties relating to the disclosure of a Content Provider's personal data by an Intermediary, as laid down in the Code, are in line with the Data Protection Directive and the PDPA.

Article 8 of the PDPA allows the Intermediary to process personal data and disclose it to the Notifier if this is essential to protect legitimate interests<sup>329</sup>. This Article is the enactment in national law of Article 7(f) of the Data Protection Directive, which specifies that personal data processing and its disclosure to third parties is legitimate as long as such processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data is disclosed. The limits to such processing are defined by respect for the fundamental rights and freedoms of the data subject.

Likewise, as stated by the Court of Justice in the *Promusicae* CJEU Ruling<sup>330</sup>, the Intermediary must, pursuant to the obligations established in the Directive on Privacy and Electronic Communications, ensure the confidentiality of related traffic data kept without the consent of the users concerned.

The NTD establishes in Article 6c that, in the event that it is not possible to come to an unequivocal judgment regarding whether specific content is unlawful, the Intermediary has two options: (i) inform the Content Provider of this situation, or (ii) contact the Notifier. Under the NTD, in certain circumstances where the Content Provider is known to the Intermediary but does not react or reach an agreement with the Notifier, the Intermediary can decide whether to give the Notifier the name and contact details of the Content Provider. The Notifier can then choose to pursue the matter through a civil and/or criminal judicial procedure.

As a result of the implementation of the Data Protection Directive<sup>331</sup> in the Netherlands, the PDPA applies if the Content Provider whose name and contact details are received by the Notifier is a private individual.

Determination of the legitimacy of processing personal data is subject to the performance of a balancing test, evaluating the relative strengths of the legitimate interests of the controller (or third parties to whom the data is disclosed) and the interests or fundamental rights of the data subject<sup>332</sup>. If this situation occurs, Article 8 of the

---

<sup>328</sup> Article 4a of the Code: 'Reports from inspection or investigation services can be made in two (2) ways. Formal legal reports are made by the Public Prosecutor's Office and have an imperative character. There is an obligation on Intermediaries to comply with them.

An investigatory authority or inspectorate can also make an 'ordinary' report, just like any private individual. In this situation it is important that the investigatory authority or inspectorate makes it clear that the report is not a formal legal order. Where a formal legal order is involved, it should be verifiable that the report has been made by the Public Prosecutor's Office or the inspection or investigation service. Where an investigative officer makes a report that does not constitute a formal legal order, this must be explicit in the report.'

<sup>329</sup> In this sense, the District Court of Utrecht decision dated 9 July 2002 between *Teleatlas* and *Planet Internet* resolved that the disclosure of personal data by *Planet Internet* was to be performed in accordance with Article 8 of the PDPA. This case law will be further detailed in Section 4.4 of this Chapter 4 ('Dutch Regulations').

<sup>330</sup> *Ibid.* Note 266.

<sup>331</sup> *Ibid.* Note 254.

<sup>332</sup> Although it will be further detailed in Section 4.4 of this Chapter 4 ('Dutch Regulations'), in the case of the District Court of the Hague of 24 October 2012 (*BREIN v Networks B.V.*), the collision between data protection and intellectual property rights was discussed. The Court



PDPA and Article 7(f) of the Data Protection Directive will be the legal grounds for processing the data subject's personal data. The current text of Article 7(f) can be relied upon in a wide range of situations as long as its requirements, including a balancing test, are satisfied.

The 'Opinion of 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC'<sup>333</sup>, dated April 2014 and elaborated by the Working Party (WP) set up under Article 29 of Directive 95/46/EC has developed a number of useful factors to be considered when carrying out balancing tests<sup>334</sup>. The legitimate interest of third parties may also be applicable<sup>335</sup>. This possibility may include situations where a controller goes beyond its specific legal obligations as specified in the laws and regulations in order to assist law enforcement or private stakeholders in their efforts to combat illegal activities. The opinion includes enforcement of IP rights.

In this respect, the 'Working document on data protection issues related to intellectual property rights' dated January 2005 and elaborated by the WP set up under Article 29 of Directive 95/46/EC<sup>336</sup>, provides data protection guidelines for rightholders and ISPs in the exercise of their rights against individuals suspected of copyright violation. In this document, the Article 29 WP highlights the obligation to comply with the information, purpose limitation and the compatibility of data protection principles when rightholders need to complete all the personal information of the author of a possible infringement with additional details that could be found with the help of ISPs and/or in other databases, such as the Whois database<sup>337</sup>.

The Controller's legitimate interests need to respect fundamental rights and freedoms contained in the European Convention of Fundamental Rights and the Charter on Fundamental Rights (e.g., freedom of expression and information or the presumption of innocence and right of defence). Analysing multiple elements such as (a) the nature of personal data, (b) the way the data is being processed, (c) reasonable expectations of the data subjects and (d) the status of the controller and data subject, will be necessary in order to assess the impact on the data subject.

The following Dutch Court Resolutions should be taken into account:

---

resolved that the concrete circumstances of the case obliged Networks B.V. to provide the exact contact details of the Content Provider as BREIN's interest in obtaining the data in question (the protection of intellectual property rights) prevailed over any other parties' rights.

<sup>333</sup> [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf).

<sup>334</sup> (a) assessing the controller's legitimate interest, (b) impact on the data subjects, (c) provisional balance and (d) additional safeguards applied by the controller to prevent any undue impact on the data subjects.

<sup>335</sup> The Opinion of the Article 29 WP in its page 29: 'General public interest or third party's interest. Finally, the legitimate interest of third parties may also be relevant in a different way. This is the case where a controller — sometimes encouraged by public authorities — is pursuing an interest that corresponds with a general public's interest or a third party's interest. This may include situations where a controller goes beyond its specific legal obligations set in laws and regulations to assist law enforcement or private stakeholders in their efforts to combat illegal activities, such as money laundering, child grooming, or illegal file sharing online. In these situations, however, it is particularly important to ensure that the limits of Article 7(f) are fully respected.'

<sup>336</sup> 'Working document on data protection issues related to intellectual property rights', 18 January 2005, WP 104.

<sup>337</sup> Ibid. Note 324 'The content of databases, be they public or not, can only be processed and further used for a purpose compatible with the one for which they were first collected. As regards the Whois database, the Working party has already emphasised in its opinion of 13 June 2003 (Opinion 2/2003 on the application of data protection principles to the Whois directories. WP 76) that 'from the data protection viewpoint it is essential to determine in very clear terms what is the purpose of the Whois and which purpose(s) can be considered as legitimate and compatible to the original purpose. [...] This is an extremely delicate matter as the purpose of the Whois directories cannot be extended to other purposes just because they are considered desirable by some potential users of the directories. Some purposes that could raise data protection (compatibility) issues are for example the use of the data by private sector actors in the framework of self-police activities related to alleged breaches of their rights e.g. in the digital right management field.'

(...) 'In Belgium, Rightholders have been requesting the collaboration of ISPs to send warnings to users. In the United-States, ISPs were requested to communicate the ID of their clients directly to the music industry representatives, without Court order. This led to several court decisions (i.e., the Verizon case — December 2003), where finally such direct communication of information to Rightholders was considered illegal by the Court. As another example, the Australian legislation (through the 'Anton Pillar order') permits the search of inquiries, including domiciliary visits, by private actors such as holders of IP rights. (...) In this context, the French data protection legislation, for example, now includes an exemption aiming specifically at allowing the processing of judicial data by specific Rightholders defined by the law 337, in certain circumstances and subject to prior authorisation by the French DPA.'



- The Dutch Supreme Court provides, in its resolution of 25 November 2005 in *Lycos v Pessers*<sup>338</sup>, a list of four situations in which the provider acts unlawfully in not providing the Content Provider's personal data to the Notifier: (i) when the possibility that the information is unlawful and harmful vis-à-vis the third party is sufficiently likely; (ii) when the third party has a real interest in obtaining the personal data; (iii) when it is likely that in the specific case no less drastic option exists to obtain the personal data; and (iv) when the balance between the interests of the Notifier, the ISP and the website owner involved (as far as known) implies that the interest of the Notifier should prevail.
- The Hague District Court stated, in its preliminary relief of 5 January 2007 in *BREIN v KPN*<sup>339</sup>, that KPN should provide the name and address of the operator and close down said website.
- Amsterdam Appeal Court stated, in its 3 July 2008 ruling in *BREIN v Leaseweb (everlasting.nu)*<sup>340</sup>, that notifications from Brein complied with the requirement to provide data, and that, therefore, Leaseweb had to provide the name and address of the operator.
- The European Court of Justice established, in its *Promusicae* CJEU Ruling<sup>341</sup> of 29 January 2008, and *Bonnier* CJEU Ruling<sup>342</sup> of 19 April 2012, that an Intermediary has to consider not only the Notifier's intellectual property rights but also the Content Providers' privacy rights when disclosing personal information from the Content Provider to the Notifier.

Some critics state that the NTD's dispositions allowing an Intermediary to disclose a Content Provider's personal data to a Notifier might not contain an appropriate evaluation of all parties' concerns. The following passage from a letter sent to the permanent representations in Brussels evidences BEUC's concerns regarding the disclosure of personal data: 'Identifying alleged infringers should only be permitted in line with the European Charter and all conditions in the IPR Enforcement Directive. (...) Personal information of online users must only be disclosed to public law enforcement authorities. Disclosure of users' information to third parties is incompatible with data protection rules. This includes IP addresses, both static and dynamic. These are personal data since a third party can easily discover the natural person using the IP address. (...)'<sup>343</sup>.

Summarising the content of Article 7(f) of the Data Protection Directive, Article 8 of the PDPA and Article 29 of the WP's opinion<sup>344</sup>, it can be concluded that in order to carry out the legitimate transmission of the Content Provider's personal data, it is very important to do so after a balancing test involving the rights in question and the special characteristics of each situation. Article 29 of the WP's opinion emphasises the fact that every situation regarding fundamental rights collisions must be treated with due caution. Due to the importance of the rights protected by them it is important to study every single case and evaluate, by means of a balancing test, which fundamental right must prevail according to the special circumstances of every case as there is no prior court order covering the disclosure.

Likewise, according to the resolution of the Dutch Supreme Court of 25 November 2005 in *Lycos v Pessers*<sup>345</sup>, it will also be necessary to analyse each circumstance case by case, as a hosting provider may be acting unlawfully by refusing to provide the name and address of the infringer.

Some Dutch Intermediaries stated that (i) they do not disclose the identity of the Content Provider at first request — the complaint has to be assessed in order to check whether the Content Provider has been reached; and (ii) the

<sup>338</sup> See Annex 6 of Chapter 4.

<sup>339</sup> See Annex 6 of Chapter 4.

<sup>340</sup> See Annex 6 of Chapter 4.

<sup>341</sup> Judgment of the European Court of Justice from the 29 January 2008, C-275/06, *Promusicae* CJEU Ruling.

<sup>342</sup> Judgment of the European Court of Justice from the 13 April 2012, C-461/10, *Bonnier* CJEU Ruling.

<sup>343</sup> BEUC, 'Letter regarding Enforcement of Intellectual Property Rights', 17 September 2014, page 2, Section 'Disclosure of personal information'.

<sup>344</sup> Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC.

<sup>345</sup> Situations when the provider acts unlawfully in not providing the Content Provider's personal data to the Notifier: (i) when the possibility that the information is unlawful and harmful vis-à-vis the third party is sufficiently likely; (ii) when the third party has a real interest in obtaining the personal data; (iii) when it is likely that in the specific case no less drastic option exists to obtain the personal data; and (iv) when the balance between the interests of the Notifier, the ISP and the website owner involved (as far as known) implies that the interest of the Notifier should prevail.

agreement often signed between the Content Provider and the Intermediary stipulates that there is a limit of two days to respond to the complaint. Therefore, the Content Provider is informed that if there is no response, the Intermediary will then proceed to give the complainant the relevant contact details (name and address) in order for the complainant's lawyer to send a summons.

In conclusion, and following Dutch Court rulings and ISPs' practice (through the information provided by terms and conditions, any particular agreement, standard business clauses, etc. on the provision of information and personal data), Article 8 of PDPA would allow an ISP to process personal data and provide it to the Notifier when the balance<sup>346</sup> between the parties involved implies that the interest of the Notifier should prevail.

#### 4.5.3. Coexistence of the NTD with the provisions of the E-Commerce Directive and the Dutch E-Commerce Law

The E-Commerce Directive encourages Member States to draw up voluntary codes of conduct<sup>347</sup>. These codes of conduct should include the E-Commerce Directive provisions, which deal with, inter alia, contracts concluded by electronic means, commercial communications and Intermediaries' liability. The latter has special significance in relation to the NTD as it encouraged the development of the notice-and-take-down procedure established in the Code. Likewise, the Enforcement Directive (through its Article 11) encourages Member States to ensure that rightholders are in a position to apply injunctions against Intermediaries whose services are used by a third party to infringe intellectual property rights.

Regarding the E-Commerce Directive dispositions, the NTD is entirely voluntary. Intermediaries can freely decide whether to draw up their own notice-and-take-down code or not. Moreover, in terms of liability the legal provisions established at European and national level will be the only mechanism of enforceability.

The Netherlands has a clear statutory 'Safe Harbour' regime by virtue of the application of Article 6:196c of the Dutch Civil Code and Article 54a of the Dutch Criminal Code — both of which convert into national law Articles 12 to 14 of the E-Commerce Directive<sup>348</sup>. In general terms, 'Safe harbours' protect Intermediaries as long as they comply with certain technical conditions and take determined actions before and after noticing the existence of unlawful content within their services. In addition, Intermediaries are required to take certain measures to limit the use of unlawful content by their customers, such as implementing customers' policies or terms of use that prohibit the use of unlawful content. Intermediaries may also be requested to act expeditiously and remove illegal content as soon as they become aware of its existence.

If an Intermediary fails to comply with the 'Safe Harbour' conditions, it will not be protected under the limits to liability established, and the risk for the Intermediary to be held liable increases.

The following Section studies 'Safe Harbour' rules applicable in the Netherlands in accordance with the E-Commerce Directive, the Dutch Civil Code and the Dutch Criminal Code.

---

<sup>346</sup> Although it will be further detailed in Section 4.4 of this study ('Dutch Regulations'), in the case of the District Court of the Hague of 24 October 2012 (BREIN v Networks B.V.), the collision between data protection and intellectual property rights was discussed. The Court resolved that the concrete circumstances of the case obliged Networks B.V. to provide the exact contact details of the Content Provider as BREIN's interest in obtaining the data in question (the protection of intellectual property rights) prevailed over any other parties' rights.

<sup>347</sup> In this sense, this encouragement is expounded in Article 16 of the E-Commerce Directive. In addition, Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights also encourages Member States to draft codes of conduct: 'Industry should take an active part in the fight against piracy and counterfeiting. The development of codes of conduct in the circles directly affected is a supplementary means of bolstering the regulatory framework. The Member States, in collaboration with the Commission, should encourage the development of codes of conduct in general. (...)'.

<sup>348</sup> LIDC Congress in Oxford 2011 — 'Dutch National Report', page 14. Milica Antic (SOLV Lawyers, Amsterdam), Arend Lagemaat (DLA Piper Lawyers, Amsterdam Office), Bart van der Sloot (Institute for Information Law, Law Faculty, University of Amsterdam) and Maarten van Stekelenburg (DLA Piper Lawyers, Amsterdam Office).

#### *4.5.3.1. Application to Intermediaries of the exception of liability provided for by Articles 12 to 14 of the E-Commerce Directive and by Dutch law*

The E-Commerce Directive regulates Intermediaries' liabilities. Articles 12 to 14 of the E-Commerce Directive address liability exceptions for three different roles of Intermediaries in relation to the content of the information transmitted or stored. In this sense, the key to deciding whether they are liable or not for the illegal or unlawful content provided through their service depends on the knowledge or control they have over the information being transmitted or stored. The Intermediary roles that could be subject to these exceptions are defined as 'mere conduit', 'caching' and 'hosting'.

Article 14 of the E-Commerce Directive obliges Member States to ensure that Intermediaries with a hosting role are not liable for content stored on their services if they have no information or knowledge of any illegal activity or content or if, after acquiring such knowledge, they remove or disable access to the illegal content.

In accordance with the aforementioned, this liability exception is dependent upon either (a) a lack of knowledge or control over the information Intermediaries are transmitting or storing or (b) Intermediaries promptly disabling access to unlawful content or activity as soon as they become aware of the illegality thereof.

In spite of the liability exceptions and obligations addressed to Member States, the E-Commerce Directive expressly reserves the entitlement of Courts or administrative authorities of Member States to require the service provider to either terminate or prevent an infringement. Nevertheless, regarding hosting services, the E-Commerce Directive allows Member States to remove or disable access to information by establishing certain procedures.

At a national level, the following needs to be considered:

- **The Dutch Civil Code**

The E-Commerce Directive was converted into national law in the Member States; accordingly, in The Netherlands, the Dutch Civil Code has incorporated the Intermediaries' liability system into its Article 6:196c. Dutch law also divides the regulation of liability into the three different roles mentioned in the above paragraph.

According to Dutch law, Intermediaries could be liable for the content of the information they transmit or store by means of the general rule of 'due care' contained in the law. Article 6:162 of the Dutch Civil Code defines the concept of a tortious act as an act or omission violating a duty imposed by the law and resulting in the violation of a third party right. Furthermore, this applies not only to all duties established by law but also to what, according to custom or tradition, is understood as unwritten law and regarded as proper social conduct.

Notwithstanding the aforementioned, the application of duty of care depends on several circumstances and situations. Therefore, it is important to acknowledge case law in order to evaluate the consequences of applying this rule to any concrete liability that an Intermediary may be subject to. Additionally, the Intermediary could be liable for damages if the duty of care towards any act or omission related to the unlawful act is not observed.

Likewise, in accordance with the E-Commerce Directive, Article 6:196c of the Dutch Civil Code concludes by allowing Dutch Courts to issue a court order to terminate or prevent an infringement or an injunction for the removal or disabling of access to information.

- **The Dutch Criminal Code**

Besides civil liability, Intermediaries also recognise the possibility of being subject to criminal liability. Nevertheless, Article 54a of the Dutch Criminal Code states that an Intermediary shall not be prosecuted if it complies with a formal legal order from the Public Prosecutor's Office to remove certain content, with prior authorisation from the Examining Judge (*rechter-commissaris*).

Article 6:196c of the Dutch Civil Code and Article 54a of the Dutch Criminal Code exempts Intermediaries from incurring criminal liability for the content of the information provided as long as the Intermediary blocks the conflictive content, thus complying with the legal order previously supported by the investigating judge.

Accordingly, an Intermediary that merely transmits or stores information from third parties without modifying it, would not be liable for the content stored on its services by means of a request from a consumer or third party when the Intermediary either has no information or knowledge of the illegal activity or content or, after having acquired such knowledge, removes or disables access to the illegal content. Intermediaries could also be liable if they do not comply with the content removal order imposed by a Court.

#### 4.5.3.2. *Compatibility of the NTD with Article 15.1 of E-Commerce Directive*

Article 15.1 of E-Commerce Directive does not affect the Code as Intermediaries are not obliged to seek facts or circumstances indicating illegal activity. Through the application of the Code, Intermediaries do not lose their 'Safe Harbour' protection as they have to deal with reports once received.

#### 4.5.4. Summary of findings relating to the coexistence of the Code with the European Union and Dutch legal frameworks and case law

This Section summarises the findings made under Section 4 of this Chapter 4 ('Coexistence of the measures set forth under the VCP with European Union and Dutch legal frameworks and related case law') regarding the compatibility of the NTD with the European Union and Dutch legal frameworks and case law.

##### 4.5.4.1. *Coexistence of the NTD with fundamental rights*

The following conclusions have been reached concerning the coexistence of the NTD with certain fundamental rights:

- **Freedom of expression of the Content Provider**

According to the analysis, there are some scenarios where the freedom of expression of the Content Providers could be affected:

- *Determination of 'undesirable' content by the Intermediary.* An Intermediary could remove content not complying with the established conditions for desirable content, but this content could turn out to be perfectly legal. Consequently, Intermediaries could be subject to certain arguments that their action was in conflict with the right of freedom of expression of the Content Provider.
- *Evaluation process by Intermediaries and removal of infringing content.* Intermediaries are responsible for removing any content considered 'unlawful'. Intermediaries have to remain diligent throughout the evaluation process; if they do not act according to the general concept of duty of care, they might become liable for damages for breach of duty. So far, Courts have not yet established any parameters to follow to ensure an appropriate evaluation procedure. Therefore, if Intermediaries do not follow the duty of care expected in this balancing exercise, the removal of the content may also be considered a breach of the Content Provider's right of freedom of expression.
- *Content formally ordered to be removed by the Public Prosecutor's Office.* This requires no additional evaluation by the Intermediary. Nor does the Code provide a legal basis for the Public Prosecutor to order illegal content to be removed or foresee the involvement of a judge. Removal of the content under these circumstances could conflict with an Intermediary's duties of care with regard to the Content Provider's freedom of expression.

Pursuant to the information obtained from Intermediaries, some types of content are considered clearly unlawful, for example, content relating to child pornography or information crimes related to terrorism such as incitements to terrorism. However, content related to IP rights needs to be analysed before being removed. The breadth of the notion of 'undesirable' may thus be a cause of concern as it could go further than unlawful content.

Therefore, in relation to IP infringements, Intermediaries need to proceed with caution. Pursuant to the information obtained in the interviews carried out with Intermediaries, when there is a very straightforward case, Intermediaries remove the content. In cases where Intermediaries have doubts, no immediate action is taken and the parties are referred to the judicial procedure.

▪ **Right to the protection of personal data related to the Content Provider**

The NTD establishes the possibility that Intermediaries may disclose the Content Provider's personal data under Article 6c. However, it does not provide any guidelines on how the Intermediary is to effect the disclosure in question.

As long as the Content Provider's fundamental rights are respected, Article 8 of the PDPA and Article 7(f) of the Data Protection Directive allow the Content Provider's contact details to be provided to the Notifier where this is indispensable for the purposes of the legitimate interests of the Intermediaries. According to the Article 29 WP, in order to release this personal data, a balancing test must be undertaken. This balancing test must examine, on one hand, the legitimate interests of the Content Provider, and, on the other hand, the legitimate interests of the third parties to whom the data is disclosed.

According to Dutch Court rulings, it will be necessary to analyse each situation on a case-by-case basis, but a hosting provider may be acting unlawfully by refusing to provide the name and address of the infringer, taking into account the list of situations enumerated by the Dutch Supreme Court in its decision of 25 November 2005 in *Lycos v Pessers*: (i) when the possibility that the information is unlawful and harmful vis-à-vis the third party is sufficiently likely; (ii) when the third party has a real interest in obtaining the personal data; (iii) when it is likely that in the specific case no less drastic option exists to obtain the personal data; and (iv) when the balance between the interests of the Notifier, the ISP and the website owner involved (as far as known) implies that the interest of the Notifier should prevail.

Therefore, following Dutch Court rulings and the practices carried out by Intermediaries (through the information provided by terms and conditions, any particular agreement, standard business clauses, etc. on the provision of information and personal data), Article 8 PDPA allows the Intermediary to process and disclose personal data to the Notifier, without the consent of the Content Provider, when the balance undertaken implies that the interest of the Notifier should prevail.

**4.5.4.2. Coexistence of the NTD with the E-Commerce Directive and the Dutch E-Commerce Law**

In the Netherlands, 'Safe Harbour' rules are applied by virtue of the application of Article 6:196c of the Dutch Civil Code and Article 54a of the Dutch Criminal Code. Pursuant to these provisions, Intermediaries are not liable for the content stored on their servers by means of a request from a consumer or third party when either the Intermediary has no information or knowledge of the illegal activity or content or, after having acquired such knowledge, removes or disables access to the illegal content.

## 5. Technologies

Despite the fact that the NTD uses technology for its functioning, no technical improvement has been developed by the application of the Code. According to the information obtained during the interviews, parties use emails for communicating and exchanging information. However, in certain other elements of the complaint mechanisms, for example helpdesks, new technology has been put in place for content removal.

Overall, all the technology used for the application of the Code already existed before its implementation. Nevertheless, as will be explained further in Section 8 of this Chapter 4, ('Effectiveness'), relevant stakeholders are trying to create new initiatives, like the 'Task Force', which would need to see new technologies implemented in order to ensure the proper and effective functioning of the NTD.

## 6. Costs

According to the information provided by the Intermediaries, each signatory to the Code and each rightholder assumes its own costs. Therefore, application of the NTD does not involve any cost sharing. Besides, according to the information obtained during the interviews with relevant stakeholders, none of them has an exact figure of the Code's implementation on costs, though all of them agreed on it not being too costly.

Moreover, all Intermediaries and rightholders interviewed confirm that implementation and application of the Code saves them high litigation costs, since with application of the NTD, many cases can be resolved without a court claim.



## 7. Education

There have been no educational activities directed towards consumers or individuals. However, Intermediaries, through their associations, have provided their members with all sorts of information in the form of flowcharts or reports on the Code in order to facilitate its implementation and solve all possible queries in this respect.

One of the main initiatives within the 'Task Force' will concern additional materials, with a view to educating the community. In this regard, on 13 November 2015, a meeting was scheduled by the Intermediaries, the main focus of which was to discuss the inefficient and almost non-existent education activities, and the possibility of taking action in this regard.

## 8. Effectiveness

As previously described, under the NTD regime, Intermediaries have a duty to remove illegal and harmful internet content once they have been informed that their servers are hosting any. Nevertheless, stakeholders interviewed expressed their concerns as to the criteria used by Intermediaries to determine whether the content they are hosting is illegal or harmful. This gives confusion and keeps raising doubts whether it is appropriate to delegate self-regulation to private actors.

As an example of the effectiveness of the Code, the subsequent information and data published by Leaseweb<sup>349</sup>, one of the leading hosting providers worldwide, and by BREIN, the most representative and active rightholders' association in the Netherlands, provide a useful overview:

- Leaseweb: every two years Leaseweb launches a Law Enforcement Transparency Report focused on three different countries: the Netherlands, Germany and the United States. The purpose of the Law Enforcement Transparency Report is to analyse and shed light on specific enforcement requests such as child abuse material notices and government requests to remove content, forensic images and provide consumer information. This report keeps track of all requests and assesses how they are dealt with, contributing to a safer internet where all rights are protected.

Moreover, this report publishes all information related to valid law enforcement requests. Regarding requests totally or partially rejected, there is no factual data but one main initiative is to also include these requests in the future so that the report is as complete as possible.

In this context, according to the Law Enforcement Transparency Report 2012<sup>350</sup>, most of the existing requests concerned child abuse material (175 reports submitted) and, compared with removal of content, which had very little impact (only two filed reports), and consumer information (46 filed reports). In 2013<sup>351</sup>, requests related to child abuse were also the most common (112 filed reports), while consumer information remained static (only 47 reports) and there was no data available for content removed. However, work still needs to be done on transparency.

- BREIN: According to BREIN's 2010 yearbook<sup>352</sup>, in that year, more than 600 illegal sites and services were made inaccessible. These were mainly P2P (bittorrent) sites but also usenet sites as well as streaming and link sites that made use of cyberlockers. At Dutch cyberlockers, more than 45 000 unauthorised files were removed upon notices from BREIN; as well as auction sites, around 100 000 ads for illegal copies of books, films, TV series, games and music were removed. In addition, about 100 actions were undertaken against persistent illegal traders.

BREIN's review 2014 and preview 2015<sup>353</sup> stated that there were 362 rogue sites in 2014 amongst which 148 were cyberlocker link sites, 7 cyberlockers, 98 bittorrent sites, 80 streaming sites, 21 usenet link sites and 6 sites offering illegal physical media instead of files. All of them were taken down. The majority of these sites operated anonymously. In general they did not react and were taken down by their respective hosting providers. Most sites had very different types of content such as music, audiovisual, books and games. Overall, there has been a gradual decline in the number of illegal websites hosted in the Netherlands and the annual number of sites taken down by BREIN went down from 700 to just over 350.

It is also important to note that around 80 % of these take downs are carried out by hosting providers, however, a high percentage of the websites or content removed goes abroad. Indeed, as stated by BREIN:

- if global figures are to be considered, out of every 100 illegal sites, 90 are taken down by hosting providers and 80 of those sites go abroad or hide behind programs such as Cloudflare. These sites are still pursued by BREIN, but around half them persist by continually switching hosting provider and do not stop unless the operators are identified and can be held liable. In such situations, these cases are often

<sup>349</sup> <https://www.leaseweb.com/>.

<sup>350</sup> <http://blog.leaseweb.com/2013/04/11/leaseweb-first-hosting-provider-worldwide-to-launch-law-enforcement-transparency-report/>.

<sup>351</sup> <http://blog.leaseweb.com/2014/02/25/law-enforcement-transparency-report-2014-july-1-december-31/>.

<sup>352</sup> BREIN Yearbook 2010 <http://www.anti-piracy.nl/artikelen.php?id=17>.

<sup>353</sup> BREIN review 2014 and preview 2015 <http://www.anti-piracy.nl/artikelen.php?id=26>.

dealt with through the mechanisms of the Domain Name System and IP blocking, preventing access to these websites. Such blocking is carried out in multiple EU Member States but in the Netherlands is still subject to legal proceedings currently pending before the Supreme Court.

Google also applies this effective measure, in 2014 it removed over 4.4 million search results reported by BREIN that were leading to unlawful content. Most of these search results related to music (64 %), followed by videos (24 %) and by books and videogames (14 %).

Moreover, over 5.132 interventions were done on 'auction sites' removing many advertisements for illegal recorded media.

According to parties' feedback, the NTD is a very efficient tool as it contributes to resolve conflicts in 95 % of the cases. Its effectiveness is tested when Notifier reports are studied by the Intermediary in question, which does not mean that content always has to be removed. However, according to the parties' information, the number of complaints and websites removed under this regime has decreased.

In spite of the positive results of this practice, some relevant stakeholders are studying the possibility of implementing new measures to further improve its effectiveness. Although these initiatives are merely under discussion, two are gaining force, namely, the 'Task Force' and the 'Trusted Flagger', explained below.

## Future actions

Learning from their experience applying the NTD Intermediaries agree that the effectiveness and applicability of the Code could be improved. Currently, they<sup>354</sup> are studying two different possibilities: creating a complaint centre (the Task Force) that could receive all reports and creating a tool called 'Trusted Flagger' that would be a help desk where users could consult experts to know if content is illegal or not.

- Task Force: intermediaries want to merge and create a complaint centre to receive all reports.

One practical concern for small Intermediaries regarding the NTD is that they usually do not have a legal department to deal with the legal evaluation of reports received. Besides, it would not be economically sustainable for them to have a legal department focused on evaluating reports as they only receive a few claims each year. On the contrary, larger Intermediaries do normally have a legal department as they receive more reports of this kind.

It is particularly important to note the significance that this initiative will have for the NTD Code of Conduct. This centre would facilitate small hosts' role in the Code by sharing costs and improving the effectiveness of reports' evaluations. This complaint centre would also speed up the process itself. One of the aspects targeted is the interaction between stakeholders as there is currently no formal format for their communications.

In addition, one of the means being considered is the creation of a general NTD tool, which could be added to hosting parties' websites. This tool would help users to administer complaints, track their progress and compile statistics for the parties involved.

- Trusted Flagger: Intermediaries want to create a help desk for users to contact when unauthorised content is found on the internet. Experts with access to the correct means/tools could verify if the content illegal and find the contact details of the Content Provider. Any NTD claims from the 'Trusted Flagger' help desk would have automatic effect, Intermediaries would have to immediately remove the content with no need of further investigation.

The Dutch Hosting Provider Association also implements a more simplified process that could be used as an example too: once the complaint is received the Intermediary analyses it and verifies the information, being able to ask for more information on (i) the specific content infringing any rights, (ii) the specific right infringed, (iii) and the reason for alleging such infringement. Once the Intermediary decides that the content is unlawful, it provides the Notifier with the Content Provider's contact details. If the Content Provider cannot be contact or is unwilling to remove the content at issue the Intermediary can remove it. If the Intermediary considers the content to be legal, it informs the Notifier. In addition, in those cases where the Intermediary considers it necessary (an emergency), this process will be swiftly put into place on the same day.

---

<sup>354</sup> ISP Connect and DHPA are willing to develop these tools.

## Chapter 4: Annex 1

### BREIN's members

- The music, video and interactive departments of the Dutch Association of Producers and Importers of image - and sound carriers (*'Nederlandse Vereniging van Producenten en Importeurs van beeld - en geluidsdragers'* or *'NVPI'*).
- The Dutch Publishers Association, (*'Nederlands Uitgeversverbond'* or *'NUV'*) , on behalf of the publishers of multimedia software.
- The Dutch association of entertainment retailers, (*'Nederlandse Vereniging voor Europees Recht'* or *'NVER'*)
- The international organisation of major motion picture producers, Motion Picture Association, or *'MPA'*.
- The joint licensor of non-theatrical video performance rights (*'Stichting Videma'*).
- The Dutch association of film distributors (*'Nederlandse Vereniging van Filmdistributeurs'* or *'NVF'*).
- The Dutch music rights collecting society Buma/Stemra on behalf of composers, textwriters and music publishers.
- The Dutch neighbouring rights collecting society Sena on behalf of performing artists.
- The International Association of Music Producers or *'IFPI'* and the International Association of Interactive Distributors or *'ISFE'* and ESA.<sup>355</sup>

---

<sup>355</sup> BREIN, the art of protecting the creative. <http://www.anti-piracy.nl/english.php> (accessed 29 June 2015).

## Chapter 4: Annex 2

### Notice-and-take-down Code of Conduct<sup>356</sup>

#### 1. Scope

- a. This code establishes a procedure for Intermediaries to deal with reports of unlawful content on the internet.
- b. The code is provided for Intermediaries that provide a public (telecommunications) service on the internet in the Netherlands.
- c. This code is not applicable to situations in which other statutory obligations or liabilities apply for Intermediaries on the basis of legislation and jurisprudence.

#### 2. Definitions

- a. A report concerns the reporting by a Notifier of (alleged) unlawful content on the internet to an Intermediary with the objective of having this content removed from the internet.
- b. The Notifier is a person or organisation that makes a report.
- c. The Content Provider is the person (or organisation) that has placed (contested) content on the internet.
- d. An Intermediary is the provider of a (telecommunications) service on the internet.
- e. An inspection or investigation service is a legally appointed governmental service that has general or particular powers of investigation.

#### 3. Intermediary's own notice-and-take-down policy

Intermediaries have their own notice-and-take-down procedure that the public must be able to consult and that is consistent with this code. This procedure describes how Intermediaries deal with reports of unlawful content on the internet.

By means of this procedure, intermediaries wish to ensure that a report is always dealt with and that unlawful content is removed from the internet.

- a. An Intermediary publishes a procedure in which the manner and within which time limits reports are dealt with by the Intermediary. Distinctions can be made between various different forms of service provision within this procedure.
- b. An Intermediary can publish conditions of use within its service provision agreement in which criteria state what constitutes undesirable content in the view of the Intermediary.

#### 4. Reports

It is preferable that a report is only made once it is likely that the Notifier and the Content Provider will be unable to reach an agreement. The Notifier is responsible for ensuring reports are correct and complete.

- a. The Intermediary must be able to verify that reports as part of an investigation regarding a criminal offence have originated from an inspection or investigation service, or – in the case of a formal legal order – from the Public Prosecutor's Office.
- b. For reports other than those stated in Article 4a, the Notifier in any case provides the following information:

---

<sup>356</sup> The Notice-and-take-down Code of Conduct: [http://www.ecp.nl/sites/default/files/NTD\\_Gedragcode\\_Engels.pdf](http://www.ecp.nl/sites/default/files/NTD_Gedragcode_Engels.pdf)

- the contact details of the Notifier;
  - the information that the Intermediary needs to be able to evaluate the content, at least including the location (URL);
  - a description of why the content is unlawful according to the Notifier, or why it is in conflict with the criteria published by the Intermediary governing undesirable content;
  - a statement of the reason why this Intermediary is being approached as the most appropriate Intermediary to deal with the matter.
- c. A Notifier can request that the Intermediary deals with the report as a matter of urgency. The reasons for this should be fully explained by the Notifier. The Intermediary determines whether the report is dealt with as a matter of urgency on the basis of the explanation of the reasons.
- d. An Intermediary can request an explicit indemnity from a Notifier against claims from the Content Provider as a result of taking measures in the context of dealing with the report.

## 5. Evaluation

On receipt of a report, it is dealt with by the Intermediary according to the Intermediary's own procedure.

- a. Reports as referred to in Article 4a concern punishable content.
- b. An Intermediary evaluates reports as referred to in Article 4b to determine whether they are unequivocally unlawful and/or punishable.

## 6. Measures to be taken

The Intermediary takes action on the basis of the results of the evaluation process.

- a. In the event that the Intermediary determines that the content concerned is not unequivocally unlawful, the Intermediary informs the Notifier accordingly, together with the reasons for this.
- b. In the event that the Intermediary determines that the content concerned is unequivocally unlawful, the Intermediary ensures that the content concerned is immediately removed.
- c. In the event that it has not been possible to come to an unequivocal judgment as to whether the content concerned is unlawful, the Intermediary informs the Content Provider about the report with the request to remove the content or to contact the Notifier. If the Notifier and the Content Provider are unable to reach an agreement, the Notifier can choose to make an official report to the police if in his or her opinion it concerns a criminal offence. If it concerns content that is alleged to be unlawful under civil law, it is preferable that the Notifier is able to bring his or her dispute with the Content Provider before the courts. Should the Content Provider be unwilling to make him or herself known to the Notifier, the Intermediary can decide to provide the Notifier with the Content Provider's name and contact details or to remove the content concerned.
- d. The Intermediary exercises due caution in the execution of the measures that have to be taken to ensure that the removal of any more content than that to which the report refers is avoided.

## 7. Final provisions

- a. Those who subscribe to and make use of this code make this known.
- b. Those who make use of an alternative NTD procedure make this known.
- c. Notifiers and intermediaries can come to a mutually acceptable agreement to make use of (shortened) procedures that differ from or that are supplementary to this code of conduct.
- d. Amendments to this code are made on the instigation of the initiators of this code.

## EXPLANATORY STATEMENT

### INTRODUCTION

This NTD code is one of the items of an initiative of organisations that are doing their best to combat the presence of unlawful information ('content') on (the Dutch component of) the internet. The initiative has originated from the desire of governmental and private sector organisations to establish agreements in the field of Notice-and-Take-Down (NTD). A description of the form and substance that these organisations have given to these agreements is presented in this code. Use has been made of both expertise in the field and best practices in the drawing up of the NTD code.

The code establishes no new statutory obligations, but is intended to help organisations to operate with care within the existing legislative framework in the removal of information from the internet at the request of third parties. A procedure is described for this. Complying with the code is voluntary, and there can be no formal enforcement in the case of noncompliance. The benefits of complying with the code lie in the achievement of more efficient procedures and in the reduction of liability risks. The organisations that endorse the code operate according to the procedures described here. It is therefore a code of conduct that lays down the conditions for the interactions between the parties involved.

The NTD code addresses the way reports concerning (alleged) unlawful content on the internet are dealt with. In addition, the code can also be employed with respect to content that intermediaries consider to be undesirable or damaging. The code should contribute to the ability of private individuals and organisations to deal effectively with these types of reports between themselves as far as possible. The possibility always remains for them to bring the matter before the courts or to make an official report to the police.

A Notifier wishes that certain content be removed from the internet. In the first case the Notifier should communicate this to the Content Provider. The Content Provider is the person, body or organisation that has placed certain content on the internet or that is responsible for the space on the internet of which a third party is able to make use (a forum, for example). In practice, however, the Content Provider is often unknown to the Notifier. In such cases the Notifier can turn to an Intermediary.

The NTD code provides preconditions for the procedure that the Intermediary follows in order to facilitate the resolution of the conflict. In this respect it is important that the Notifier finds the appropriate Intermediary: the Content Provider uses a facility provided by the Intermediary on the internet. Who the most appropriate Intermediary is can vary from case to case. It is also possible that an Intermediary does not respond or is also unknown. In these cases it is possible to 'scale up' to the next Intermediary.

### EXAMPLE:

There is a website on which third parties (private citizens) can post short films they have made themselves. A short film has been placed on this site that contains discriminatory content. The Content Provider is the individual who posted the film. If this person is unknown (if the film was posted anonymously), the first Intermediary who can be contacted about this is the owner of the website on which the film has been posted. If the website owner is also unknown or does not respond, the next Intermediary is the company that provides the space for the site to its owner (hosting service). Scaling up to the next level could involve contacting the company that provides access to the hosting provider (access provider/'mere conduit').

The objective of the NTD code is to ensure that a report is always dealt with. This does not mean that the content must always be removed. It may well be that a report is made with respect to a site that eventually is found not to be in conflict with the law. If the content is found to be in conflict with the law, an Intermediary must facilitate or assist in the removal of the unacceptable content, or in bringing the Notifier into contact with the Content Provider.



## EXPLANATORY NOTES TO THE ARTICLES

### ▪ Note to Article 1a:

The code applies to information that conflicts with the laws of the Netherlands. A distinction must be made between information that constitutes a criminal offence and information that is in conflict with civil law (unlawful). The parties involved are also free to decide for themselves which information is considered as 'undesirable', irrespective of the question of it being in conflict with the law. They can deal with this undesirable information in the same way as information that is in conflict with the law.

### ▪ Note to Article 1b:

An Intermediary is a person or organisation offering services in any manner relating to the storage, transmission or provision of information on the internet. It concerns situations in which the laws of the Netherlands are applicable, and on the public part (in a physical sense) of the internet.

Amongst others, examples encompass:

- hosting
- mere conduit
- space on the internet where third parties can place content.

Examples: bit torrent sites, a forum, auction and shopping sites, sites with space for (links to) (self-made) films, music etc.

Internal corporate networks, for example, are not 'public', and therefore do not fall under the scope of this code.

### ▪ Note to Article 1c:

For specific application areas, different rules may apply that go further than what is laid down in this code. The rules laid down in the law and jurisprudence will always take precedence of course.

An example in practice would be the (illegal) distribution of copyright protected content on the internet, for which liabilities would apply to intermediaries that would take precedence over those described in this code of conduct. This code of conduct also provides no barrier to a legal injunction or a formal legal order.

### ▪ Note to Articles 2c and 2d:

The code makes a distinction between 'Content Provider' (Article 2b) and 'Intermediary' (Article 2c). In practice it can occur that the Intermediary facilitates the content of third parties in such a way that the service provided by the Intermediary may also be considered to be unlawful. This can be the case for example where a website refers to illegal material in a structural way. In these cases, the 'Intermediary' can be treated as the 'Content Provider'. A 'Notifier' can be a private citizen or a governmental organisation, but also a body that has been established to, and is specialised in, reporting instances with respect to specific subjects.

### ▪ Note to Article 2e:

In addition to the police, this can also refer to particular or special investigatory services and inspectorates.

### ▪ Note to Article 3a:

A reasonable time limit by which an evaluation can be completed is for example 5 working days, in cases where it can be disputed whether the content is wrongful or unlawful.

The reasonableness of the time limit is related to the severity of the alleged infringement and the social upheaval that may become associated with this. In cases where it is clearly indisputable a judgment can be arrived at very quickly.

- Note to Article 3b:

Intermediaries can establish criteria for content that they find undesirable and for content whose availability on the internet they wish to play no part in facilitating. Undesirable content goes further than unlawful content: the law determines what is unlawful content, while the Intermediary determines what is undesirable content. The Intermediary evaluates a report concerning undesirable content on the basis of the criteria the Intermediary has established for undesirable content.

- Note to Article 4:

On the grounds of effectiveness, the code states that the Notifier and the Content Provider should first try to reach a mutually acceptable agreement. Should this prove to be impossible, the complaint is 'scaled up' to an Intermediary. This can be the case if the Content Provider is anonymous or fails to respond. It is important that the Intermediary has selected who is most able to intervene effectively. Distinguishing between 'hosting providers' and 'access providers' is also important. Access providers are often technically unable to remove information because their service consists solely of the provision of access to the internet. There is no obligation on Notifiers to first make contact with the Content Provider.

- Note to Article 4a:

Reports from inspection or investigation services can be made in two (2) ways. Formal legal reports are made by the Public Prosecutor's Office and have an imperative character. There is an obligation on intermediaries to comply with them.

An investigatory authority or inspectorate can also make an 'ordinary' report, just like any private individual. In this situation it is important that the investigatory authority or inspectorate makes it clear that the report is not a formal legal order. Where a formal legal order is involved, it should be verifiable that the report has been made by the Public Prosecutor's Office or the inspection or investigation service. Where an investigative officer makes a report that does not constitute a formal legal order, this must be explicit in the report.

- Note to Article 4b:

The Notifier is responsible for ensuring the correctness of the report and that the Intermediary has sufficient information to be able to evaluate the content concerned. It is vital that the Notifier indicates as precisely as possible where the content concerned is located, for example if only a specific section of a website is considered to be unlawful.

- Note to Article 4c:

In practice it can happen that certain content that has been removed from the internet later returns, perhaps in another location. In such cases it is possible that a Notifier advises the Intermediary of this (for example by appending examples from an earlier report or – if the same Intermediary is involved – by referring to the salient features of the earlier report). This enables the Intermediary to deal with the report more quickly, and may allow some steps in the procedure to be omitted. In this way the code not only facilitates a Take-Down, but also a Stay-Down. Moreover, given the nature of the contested content it is also possible to request that the report be dealt with as a matter of urgency.

- Note to Article 4d:

The responsibility for a report lies with the Notifier. The liability of the intermediaries is dependent on the type of service they provide (hosting, mere conduit and/or caching), and is described in Article 6:196c of the Civil Code. (The relevant provisions of 'Directive 2000/31/EC of the European Parliament and the Council' of June 8, 2000 have been implemented into Dutch law by Article 6:196c of the Civil Code). In addition to this, the Intermediary and the Notifier can agree that the Intermediary is explicitly indemnified against claims from the Content Provider as a consequence of the measures taken in dealing with the report. This is associated with the practice of some Intermediaries and 'professional' Notifiers. The indemnity is especially important in cases where it is not possible to be unequivocal about whether the matter concerns unlawfulness or a criminal offence. In addition, it must not be possible to hold an Intermediary liable for responding to a report that itself later proves to be unlawful.

- Note to Article 5a:

Content that the Public Prosecutor's Office formally orders to be removed requires no (additional) evaluation by the Intermediary. The evaluation has in these cases already been performed by an authorised body.

- Note to Article 5b:

Reports that relate to conflict with civil law (cases of unlawfulness) are evaluated by the Intermediary. This also applies to criminal offences that are reported by private individuals, or that are reported by a inspection or investigation service where a formal legal order is not involved. In parallel with the concept of 'unequivocal unlawfulness' in civil law, the Intermediary can make a judgment as to whether in his or her opinion a criminal offence may be involved. Early action can also be taken against these offences by Notifiers and intermediaries without the intervention of a governmental body.

Criminal enforcement (tracing, prosecution, trial and punishment) will be particularly applicable where it serves the public interest or when private interests are involved that cannot be protected by the parties concerned themselves.

In cases where an Intermediary cannot, or wishes not to, conduct the evaluation him or herself, a third party can be brought in to do so. The responsibility for the evaluation remains with the Intermediary. The involvement of a third party should make the minimum impact possible on the 'reasonable time limit' as referred to in the note to Article 3a.

- Note to Article 6a:

It can happen that in the Intermediary's judgment the content concerned is legitimate, while the Notifier is of the opinion that it is (unequivocally) unlawful. In these cases the Intermediary must give the Notifier his or her supporting arguments.

- Note to Article 6b:

As there is no doubt concerning the unlawfulness of the content concerned, the Intermediary should immediately take measures that lead to the content being taken off-line. Where possible, the Intermediary first contacts the Content Provider about this, for example where his or her cooperation may be expected in its immediate removal.

- Note to Article 6c:

The Intermediary is responsible for the evaluation of a report. It can be that the Intermediary is unable to unequivocally determine whether the content is unlawful. This Article specifically concerns these cases, and has as its objective the achievement of a resolution of the conflict between Notifier and Content Provider as often as possible. The first step is to inform the Content Provider about the report in order that he or she can remove the content him or herself. Should the Content Provider wish not to do this, he or she is requested to make contact with the Notifier (if contact between them about this report has not already taken place). If the Content Provider does not comply with this request an impasse is created in cases of alleged unlawfulness (under civil law) that can only be resolved by the Intermediary. This can be achieved on the one hand by taking the content offline, or on the other hand by providing the Content Provider's name and contact details to the Notifier. Under Dutch law, Intermediaries are not legally obligated to know and maintain a record of the names and contact details of their clients and making names and contact details available is not legally enforceable in all cases. Case law indicates that the making available of name and contact details from an Intermediary to a Notifier should take place if the published information (a) could be unlawful in respect of the Notifier, (b) could lead to damage being caused to the Notifier, and (c) if a less severe way to obtain the name and contact details is unavailable to the Notifier. Thereafter the Intermediary shall weigh up the degree of seriousness of the privacy interests of the website holder against that of the interests of the 'victim' of the publication.

As can be understood from the above, situations may occur in practice where neither the information is taken off-line nor the name and contact details are provided to the Notifier. It is expected of Intermediaries that they make every possible effort to prevent these situations from occurring. Under Dutch law, a Content Provider who 'renders a service relating to the information society' (Article 3:15d of the Civil Code) must, inter alia, make his identity and address easily, directly and permanently accessible for those who make use of this service.

If it concerns a criminal offence (where no formal legal order has been issued by the Public Prosecutor's Office), and if the Intermediary and the Content Provider cannot reach a mutually acceptable agreement, the Intermediary may be unable to resolve this impasse. In this case, the Notifier can choose to make an official report to the police, over which a judgment can then be made by the competent authorities.

- Note to Article 6d:

The possibilities for an Intermediary to intervene on the basis of having received a report can be technically restricted on the internet. The Intermediary may only be able to remove part of the content, or in so doing may remove other content to which the report does not refer. In these instances, the code explains that due caution must be taken to ensure that the wish to remove content is matched as closely as possible with the technical possibilities for doing so. What must be prevented as far as possible is that information that does not conflict with the law is removed. When cases such as this arise, further consultation between the Notifier and the Intermediary may be necessary in addition to the procedure described in this code. On the basis of these further consultations, the Notifier may amend the report so that the Intermediary can then deal more effectively with it.

- Note to Article 7a:

It is important that parties that are complying with this code of conduct know who each other's participants are.

- Note to Article 7b:

This provision is included to prevent conflict with other NTD procedures that already exist. Websites that are based on a very large amount of input from third parties for example (such as advertisement sites and sites to which photos and videos can be uploaded), have NTD systems that for reasons of practicability are not based on direct communication with the Content Providers.

- Note to Article 7c:

This code is first and foremost intended for Notifiers and Intermediaries who do not know each other or where contact is being made between them for the first time. But this code must not stand in the way of further collaboration between them. Intermediaries are therefore free to omit the evaluation process in cases where they regard a Notifier as a 'trusted party' for instance. There are already several examples of this in practice.

- Note to Article 7d:

The intention is that the code will be continually amended over time so that it is adapted to allow for new insights and new technical developments. The maintenance and monitoring of this code is therefore under the stewardship of a number of organisations referred to here as its 'initiators'. To ensure its effective working in practice, it is also important that Intermediaries, private individuals (Notifiers) and governmental services give their support to the code.

## Chapter 4: Annex 3

### European Union legal framework

#### Charter of Fundamental Rights<sup>357</sup>

- Article 7: respect for private and family life  
Everyone has the right to respect for his or her private and family life, home and communications
- Article 8: protection of personal data  
1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority.
- Article 11: freedom of expression and information  
1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. 2. The freedom and pluralism of the media shall be respected.
- Article 17: right to property  
2. Intellectual Property shall be protected.
- Article 48: presumption of innocence and right to defend  
1. Everyone who has been charged shall be presumed innocent until proved guilty according to law. 2. Respect for the rights of the defence of anyone who has been charged shall be guaranteed.

#### European Convention on Fundamental Rights<sup>358</sup>

- Article 8: right to respect for private and family life  
1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.
- Article 10: freedom of expression  
1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises. 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the

<sup>357</sup> Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012. [http://www.europarl.europa.eu/charter/pdf/text\\_en.pdf](http://www.europarl.europa.eu/charter/pdf/text_en.pdf).

<sup>358</sup> European Convention on Fundamental Rights, [https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Convention\\_ENG.pdf](https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Convention_ENG.pdf).

prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

## European Union Directives

- Article 12 of the E-Commerce Directive<sup>359</sup>

It is necessary to exclude certain activities from the scope of this Directive, on the grounds that the freedom to provide services in these fields cannot, at this stage, be guaranteed under the Treaty or existing secondary legislation; excluding these activities does not preclude any instruments which might prove necessary for the proper functioning of the internal market; taxation, particularly value added tax imposed on a large number of the services covered by this Directive, must be excluded from the scope of this Directive.

- Article 13 of the E-Commerce Directive

This Directive does not aim to establish rules on fiscal obligations nor does it pre-empt the drawing up of Community instruments concerning fiscal aspects of electronic commerce.

- Article 14 of the E-Commerce Directive

The protection of individuals with regard to the processing of personal data is solely governed by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data<sup>(19)</sup> and Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector<sup>(20)</sup> which are fully applicable to information society services; these Directives already establish a Community legal framework in the field of personal data and therefore it is not necessary to cover this issue in this Directive in order to ensure the smooth functioning of the internal market, in particular the free movement of personal data between Member States; the implementation and application of this Directive should be made in full compliance with the principles relating to the protection of personal data, in particular as regards unsolicited commercial communication and the liability of Intermediaries; this Directive cannot prevent the anonymous use of open networks such as the Internet.

- Article 15 of the E-Commerce Directive

The confidentiality of communications is guaranteed by Article 5 Directive 97/66/EC; in accordance with that Directive, Member States must prohibit any kind of interception or surveillance of such communications by others than the senders and receivers, except when legally authorised.

- Article 16 of the E-Commerce Directive (Codes of conduct: 1)

Member States and the Commission shall encourage: (a) the drawing up of codes of conduct at Community level, by trade, professional and consumer associations or organisations, designed to contribute to the proper implementation of Articles 5 to 15; (b) the voluntary transmission of draft codes of conduct at national or Community level to the Commission; (c) the accessibility of these codes of conduct in the Community languages by electronic means; (d) the communication to the Member States and the Commission, by trade, professional and consumer associations or organisations, of their assessment of the application of their codes of conduct and their impact upon practices, habits or customs relating to electronic commerce; (e) the drawing up of codes of conduct regarding the protection of minors and human dignity. 2. Member States and the Commission shall encourage the involvement of associations or organisations representing consumers in the drafting and implementation of codes of conduct

---

<sup>359</sup> Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market OJ L 178, 17/07/2000 p. 0001 – 0016.

affecting their interests and drawn up in accordance with paragraph 1(a). Where appropriate, to take account of their specific needs associations representing the visually impaired and disabled should be consulted.

- Article 1.1 of the Data Protection Directive<sup>360</sup>

In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

- Article 7 of the Data Protection Directive

Member States shall provide that personal data may be processed only if: (a) the data subject has unambiguously given his consent; or (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or (d) processing is necessary in order to protect the vital interests of the data subject; or (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed ; or (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 d.

- Article 29 of the Data Protection Directive

1. The Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors. 2. Member States shall make provision for trade associations and other bodies representing other categories of controllers which have drawn up draft national codes or which have the intention of amending or extending existing national codes to be able to submit them to the opinion of the national authority. Member States shall make provision for this authority to ascertain, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives. 3. Draft Community codes, and amendments or extensions to existing Community codes, may be submitted to the Working Party referred to in Article 29. This Working Party shall determine, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives. The Commission may ensure appropriate publicity for the codes which have been approved by the Working Party.

- Article 11 of the Enforcement Directive<sup>361</sup>

This Directive does not aim to establish harmonised rules for judicial cooperation, jurisdiction, the recognition and enforcement of decisions in civil and commercial matters, or deal with applicable law. There are Community instruments which govern such matters in general terms and are, in principle, equally applicable to intellectual property.

---

<sup>360</sup> Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23/11/1995 p. 0031 – 0050.

<sup>361</sup> Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, OJ L 157 of 30 April 2004.



▪ Article 5 of the Directive on Privacy and Electronic Communications<sup>362</sup>

1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality. 2 Paragraph 1 shall not affect any legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication. 3. Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/ 46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society.

---

<sup>362</sup> Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002, on concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201.

## Chapter 4: Annex 4

### Dutch legal system

#### The Dutch Civil Code<sup>363</sup>

- Article 6:162: definition of a 'tortious act'

1. A person who commits a tortious act (unlawful act) against another person that can be attributed to him, must repair the damage that this other person has suffered as a result thereof. 2. As a tortious act is regarded a violation of someone else's right (entitlement) and an act or omission in violation of a duty imposed by law or of what according to unwritten law has to be regarded as proper social conduct, always as far as there was no justification for this behaviour. 3. A tortious act can be attributed to the tortfeasor [the person committing the tortious act] if it results from his fault or from a cause for which he is accountable by virtue of law or generally accepted principles (common opinion).

- Article 6: 196c: liability for services of the information society

1. A person who provides a service of the information society as meant in Article 3:15d, paragraph 3, of the Civil Code, consisting of the transmission in a communication network of information provided by a recipient of the service or providing access to a communication network, is not liable for the information transmitted, on condition that the provider: a. does not initiate the transmission; b. is not the one who decides to whom the information will be transmitted; and c. has not selected or modified the information contained in the transmission. 2. For the purpose of paragraph 1 the acts of transmission and of merely providing access to a communication network include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission. 3. A person who provides a service of the information society as meant in Article 3:15d, paragraph 3, of the Civil Code, consisting of the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, is not liable for the automatic, intermediate and temporary storage of that information, on condition that the provider: a. does not modify the information; b. complies with conditions on access to the information; c. complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry; d. does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and; e. acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement. 4. A person who provides a service of the information society as meant in Article 3:15d, paragraph 3, of the Civil Code, consisting of the storage of information provided by a recipient of the service, is not liable for the information that is stored at the request of a recipient of the service, on condition that the provider: a. does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or; b. upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information. 5. The above mentioned paragraphs do not affect the possibility to get a court order to terminate or prevent an infringement or an injunction for the removal or disabling of access to information.

---

<sup>363</sup> The Dutch Civil Code, <http://dutchcivillaw.com/legislation/dcctitle6633.htm>.

## The Dutch Criminal Code<sup>364</sup>

- Article 54a

An Intermediary which provides a telecommunication service that consists of the transfer or storage of data from a third party, shall not be prosecuted in its capacity as Intermediary telecommunication provider if it complies with an order from the public prosecutor to take all measures that may be reasonably required of it in order to disable this data, which order shall be issued by the public prosecutor after he has applied for and received a written authorisation from the examining magistrate.

## Dutch Constitution<sup>365</sup>

- Article 7: Freedom of Expression

1. No one shall require prior permission to publish thoughts or opinions through the press, without prejudice to the responsibility of every person under the law. 2. Rules concerning radio and television shall be laid down by Act of Parliament. There shall be no prior supervision of the content of a radio or television broadcast. 3. No one shall be required to submit thoughts or opinions for prior approval in order to disseminate them by means other than those mentioned in the preceding paragraphs, without prejudice to the responsibility of every person under the law. The holding of performances open to persons younger than sixteen years of age may be regulated by Act of Parliament in order to protect good morals. 4. The preceding paragraphs do not apply to commercial advertising.

## Personal Data Protection Law ('Wet Bescherming Persoonsgegevens')<sup>366</sup>

- Article 8

Personal data may only be processed where: a. the data subject has unambiguously given his consent for the processing; b. the processing is necessary for the performance of a contract to which the data subject is party, or for actions to be carried out at the request of the data subject and which are necessary for the conclusion of a contract; c. the processing is necessary in order to comply with a legal obligation to which the responsible party is subject; d. the processing is necessary in order to protect a vital interest of the data subject; e. the processing is necessary for the proper performance of a public law duty by the administrative body concerned or by the administrative body to which the data are provided, or f. the processing is necessary for upholding the legitimate interests of the responsible party or of a third party to whom the data are supplied, except where the interests or fundamental rights and freedoms of the data subject, in particular the right to protection of individual privacy, prevail.

---

<sup>364</sup>The Dutch Criminal Code, [http://www.eitn.eu/PageFiles/6533/2014%20seminars/Omsenie/WetboekvanStrafrecht\\_ENG\\_PV.pdf](http://www.eitn.eu/PageFiles/6533/2014%20seminars/Omsenie/WetboekvanStrafrecht_ENG_PV.pdf).

<sup>365</sup>The Dutch Constitution, <http://www.servat.unibe.ch/icl/nl000000.html>.

<sup>366</sup>Personal Data Protection Law, [http://www.coe.int/t/dghl/standardsetting/dataprotection/national%20laws/NL\\_DP\\_LAW.pdf](http://www.coe.int/t/dghl/standardsetting/dataprotection/national%20laws/NL_DP_LAW.pdf).

## Chapter 4: Annex 5

### International legal framework

#### DMCA<sup>367</sup>

- Article 17 Code §512 - limitations on liability relating to material online:

(a) Transitory Digital Network Communications.— A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider's transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections, if— (1) the transmission of the material was initiated by or at the direction of a person other than the service provider; (2) the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider; (3) the service provider does not select the recipients of the material except as an automatic response to the request of another person; (4) no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for the transmission, routing, or provision of connections; and (5) the material is transmitted through the system or network without modification of its content. (b) System Caching.— (1) Limitation on liability.— A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the intermediate and temporary storage of material on a system or network controlled or operated by or for the service provider in a case in which— (A) the material is made available online by a person other than the service provider; (B) the material is transmitted from the person described in subparagraph (A) through the system or network to a person other than the person described in subparagraph (A) at the direction of that other person; and (C) the storage is carried out through an automatic technical process for the purpose of making the material available to users of the system or network who, after the material is transmitted as described in subparagraph (B), request access to the material from the person described in subparagraph (A), if the conditions set forth in paragraph (2) are met. (2) Conditions.— The conditions referred to in paragraph (1) are that— (A) the material described in paragraph (1) is transmitted to the subsequent users described in paragraph (1)(C) without modification to its content from the manner in which the material was transmitted from the person described in paragraph (1)(A); (B) the service provider described in paragraph (1) complies with rules concerning the refreshing, reloading, or other updating of the material when specified by the person making the material available online in accordance with a generally accepted industry standard data communications protocol for the system or network through which that person makes the material available, except that this subparagraph applies only if those rules are not used by the person described in paragraph (1)(A) to prevent or unreasonably impair the intermediate storage to which this subsection applies; (C) the service provider does not interfere with the ability of technology associated with the material to return to the person described in paragraph (1)(A) the information that would have been available to that person if the material had been obtained by the subsequent users described in paragraph (1)(C) directly from that person, except that this subparagraph applies only if that technology— (i) does not significantly interfere with the performance of the provider's system or network or with the intermediate storage of the material; (ii) is consistent with generally accepted industry standard communications protocols; and (iii) does not extract information from the provider's system or network other than the information that would have been available to the person described in paragraph (1)(A) if the subsequent users had gained access to the material directly from that

---

<sup>367</sup> Digital Millennium Copyright Law, December 1998 <http://www.copyright.gov/legislation/dmca.pdf>.

person; (D) if the person described in paragraph (1)(A) has in effect a condition that a person must meet prior to having access to the material, such as a condition based on payment of a fee or provision of a password or other information, the service provider permits access to the stored material in significant part only to users of its system or network that have met those conditions and only in accordance with those conditions; and (E) if the person described in paragraph (1)(A) makes that material available online without the authorisation of the copyright owner of the material, the service provider responds expeditiously to remove, or disable access to, the material that is claimed to be infringing upon notification of claimed infringement as described in subsection (c)(3), except that this subparagraph applies only if— (i) the material has previously been removed from the originating site or access to it has been disabled, or a court has ordered that the material be removed from the originating site or that access to the material on the originating site be disabled; and (ii) the party giving the notification includes in the notification a statement confirming that the material has been removed from the originating site or access to it has been disabled or that a court has ordered that the material be removed from the originating site or that access to the material on the originating site be disabled. (c) Information Residing on Systems or Networks At Direction of Users.— (1) In general.— A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider— (A) (i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing; (ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or (iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material; (B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and (C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity. (2) Designated agent.— The limitations on liability established in this subsection apply to a service provider only if the service provider has designated an agent to receive notifications of claimed infringement described in paragraph (3), by making available through its service, including on its website in a location accessible to the public, and by providing to the Copyright Office, substantially the following information: (A) the name, address, phone number, and electronic mail address of the agent. (B) other contact information which the Register of Copyrights may deem appropriate. The Register of Copyrights shall maintain a current directory of agents available to the public for inspection, including through the Internet, and may require payment of a fee by service providers to cover the costs of maintaining the directory. (3) Elements of notification.— (A) To be effective under this subsection, a notification of claimed infringement must be a written communication provided to the designated agent of a service provider that includes substantially the following: (i) A physical or electronic signature of a person authorised to act on behalf of the owner of an exclusive right that is allegedly infringed. (ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site. (iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material. (iv) Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted. (v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorised by the copyright owner, its agent, or the law. (vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorised to act on behalf of the owner of an exclusive right that is allegedly infringed. (B) (i) Subject to clause (ii), a notification from a copyright owner or from a person authorised to act on behalf of the copyright owner that fails to comply substantially with the provisions of subparagraph (A) shall not be considered under paragraph (1)(A) in determining whether a service provider has actual knowledge or is aware of facts or circumstances from which infringing activity is apparent. (ii) In a case in which the notification that is provided to the service provider's designated agent fails to comply substantially with all the provisions of subparagraph (A) but substantially complies with clauses (ii), (iii), and (iv) of subparagraph (A), clause (i) of this subparagraph applies only if the service provider promptly attempts to contact the person making the notification or takes other reasonable steps to assist in the

receipt of notification that substantially complies with all the provisions of subparagraph (A).(d) Information Location Tools.— A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider referring or linking users to an online location containing infringing material or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hypertext link, if the service provider— (1) (A) does not have actual knowledge that the material or activity is infringing; (B) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or (C) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material; (2) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and (3) upon notification of claimed infringement as described in subsection (c)(3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity, except that, for purposes of this paragraph, the information described in subsection (c)(3)(A)(iii) shall be identification of the reference or link, to material or activity claimed to be infringing, that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate that reference or link. (e) Limitation on Liability of Nonprofit Educational Institutions.— (1) When a public or other nonprofit institution of higher education is a service provider, and when a faculty member or graduate student who is an employee of such institution is performing a teaching or research function, for the purposes of subsections (a) and (b) such faculty member or graduate student shall be considered to be a person other than the institution, and for the purposes of subsections (c) and (d) such faculty members or graduate student's knowledge or awareness of his or her infringing activities shall not be attributed to the institution, if— (A) such faculty members or graduate student's infringing activities do not involve the provision of online access to instructional materials that are or were required or recommended, within the preceding 3-year period, for a course taught at the institution by such faculty member or graduate student; (B) the institution has not, within the preceding 3-year period, received more than two notifications described in subsection (c)(3) of claimed infringement by such faculty member or graduate student, and such notifications of claimed infringement were not actionable under subsection (f); and (C) the institution provides to all users of its system or network informational materials that accurately describe, and promote compliance with, the laws of the United States relating to copyright. (2) For the purposes of this subsection, the limitations on injunctive relief contained in subsections (j) (2) and (j)(3), but not those in (j)(1), shall apply. (f) Misrepresentations.— Any person who knowingly materially misrepresents under this section— (1) that material or activity is infringing, or (2) that material or activity was removed or disabled by mistake or misidentification, shall be liable for any damages, including costs and attorneys' fees, incurred by the alleged infringer, by any copyright owner or copyright owner's authorised licensee, or by a service provider, who is injured by such misrepresentation, as the result of the service provider relying upon such misrepresentation in removing or disabling access to the material or activity claimed to be infringing, or in replacing the removed material or ceasing to disable access to it.(g) Replacement of Removed or Disabled Material and Limitation on Other Liability.— (1) No liability for taking down generally.— Subject to paragraph (2), a service provider shall not be liable to any person for any claim based on the service provider's good faith disabling of access to, or removal of, material or activity claimed to be infringing or based on facts or circumstances from which infringing activity is apparent, regardless of whether the material or activity is ultimately determined to be infringing. (2) Exception.— Paragraph (1) shall not apply with respect to material residing at the direction of a subscriber of the service provider on a system or network controlled or operated by or for the service provider that is removed, or to which access is disabled by the service provider, pursuant to a notice provided under subsection (c)(1)(C), unless the service provider— (A) takes reasonable steps promptly to notify the subscriber that it has removed or disabled access to the material; (B) upon receipt of a counter notification described in paragraph (3), promptly provides the person who provided the notification under subsection (c)(1)(C) with a copy of the counter notification, and informs that person that it will replace the removed material or cease disabling access to it in 10 business days; and (C) replaces the removed material and ceases disabling access to it not less than 10, nor more than 14, business days following receipt of the counter notice, unless its designated agent first receives notice from the person who submitted the notification under subsection (c)(1)(C) that such person has filed an action seeking a court order to restrain the subscriber from engaging in infringing activity relating to the material on the service provider's system or network. (3) Contents of counter notification.— To be effective under this subsection, a counter



notification must be a written communication provided to the service provider's designated agent that includes substantially the following: (A) A physical or electronic signature of the subscriber. (B) Identification of the material that has been removed or to which access has been disabled and the location at which the material appeared before it was removed or access to it was disabled. (C) A statement under penalty of perjury that the subscriber has a good faith belief that the material was removed or disabled as a result of mistake or misidentification of the material to be removed or disabled. (D) The subscriber's name, address, and telephone number, and a statement that the subscriber consents to the jurisdiction of Federal District Court for the judicial district in which the address is located, or if the subscriber's address is outside of the United States, for any judicial district in which the service provider may be found, and that the subscriber will accept service of process from the person who provided notification under subsection (c)(1)(C) or an agent of such person. (4) Limitation on other liability.— A service provider's compliance with paragraph (2) shall not subject the service provider to liability for copyright infringement with respect to the material identified in the notice provided under subsection (c)(1)(C). (h) Subpoena To Identify Infringer.— (1) Request.— A copyright owner or a person authorised to act on the owner's behalf may request the clerk of any United States district court to issue a subpoena to a service provider for identification of an alleged infringer in accordance with this subsection. (2) Contents of request.— The request may be made by filing with the clerk— (A) a copy of a notification described in subsection (c)(3)(A); (B) a proposed subpoena; and (C) a sworn declaration to the effect that the purpose for which the subpoena is sought is to obtain the identity of an alleged infringer and that such information will only be used for the purpose of protecting rights under this title. (3) Contents of subpoena.— The subpoena shall authorise and order the service provider receiving the notification and the subpoena to expeditiously disclose to the copyright owner or person authorised by the copyright owner information sufficient to identify the alleged infringer of the material described in the notification to the extent such information is available to the service provider. (4) Basis for granting subpoena.— If the notification filed satisfies the provisions of subsection (c)(3)(A), the proposed subpoena is in proper form, and the accompanying declaration is properly executed, the clerk shall expeditiously issue and sign the proposed subpoena and return it to the requester for delivery to the service provider. (5) Actions of service provider receiving subpoena.— Upon receipt of the issued subpoena, either accompanying or subsequent to the receipt of a notification described in subsection (c)(3)(A), the service provider shall expeditiously disclose to the copyright owner or person authorised by the copyright owner the information required by the subpoena, notwithstanding any other provision of law and regardless of whether the service provider responds to the notification. (6) Rules applicable to subpoena.— Unless otherwise provided by this section or by applicable rules of the court, the procedure for issuance and delivery of the subpoena, and the remedies for noncompliance with the subpoena, shall be governed to the greatest extent practicable by those provisions of the Federal Rules of Civil Procedure governing the issuance, service, and enforcement of a subpoena duces tecum. (i) Conditions for Eligibility.— (1) Accommodation of technology.— The limitations on liability established by this section shall apply to a service provider only if the service provider— (A) has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers; and (B) accommodates and does not interfere with standard technical measures. (2) Definition.— As used in this subsection, the term 'standard technical measures' means technical measures that are used by copyright owners to identify or protect copyrighted works and— (A) have been developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process; (B) are available to any person on reasonable and non-discriminatory terms; and (C) do not impose substantial costs on service providers or substantial burdens on their systems or networks. (j) Injunctions.— The following rules shall apply in the case of any application for an injunction under section 502 against a service provider that is not subject to monetary remedies under this section: (1) Scope of relief.— (A) With respect to conduct other than that which qualifies for the limitation on remedies set forth in subsection (a), the court may grant injunctive relief with respect to a service provider only in one or more of the following forms: (i) An order restraining the service provider from providing access to infringing material or activity residing at a particular online site on the provider's system or network. (ii) An order restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is engaging in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that



are specified in the order. (iii) Such other injunctive relief as the court may consider necessary to prevent or restrain infringement of copyrighted material specified in the order of the court at a particular online location, if such relief is the least burdensome to the service provider among the forms of relief comparably effective for that purpose. (B) If the service provider qualifies for the limitation on remedies described in subsection (a), the court may only grant injunctive relief in one or both of the following forms: (i) An order restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is using the provider's service to engage in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order. (ii) An order restraining the service provider from providing access, by taking reasonable steps specified in the order to block access, to a specific, identified, online location outside the United States. (2) Considerations.— The court, in considering the relevant criteria for injunctive relief under applicable law, shall consider— (A) whether such an injunction, either alone or in combination with other such injunctions issued against the same service provider under this subsection, would significantly burden either the provider or the operation of the provider's system or network; (B) the magnitude of the harm likely to be suffered by the copyright owner in the digital network environment if steps are not taken to prevent or restrain the infringement; (C) whether implementation of such an injunction would be technically feasible and effective, and would not interfere with access to noninfringing material at other online locations; and (D) whether other less burdensome and comparably effective means of preventing or restraining access to the infringing material are available. (3) Notice and ex parte orders.— Injunctive relief under this subsection shall be available only after notice to the service provider and an opportunity for the service provider to appear are provided, except for orders ensuring the preservation of evidence or other orders having no material adverse effect on the operation of the service provider's communications network. (k) Definitions—(1) Service provider.— (A) As used in subsection (a), the term 'service provider' means an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received. (B) As used in this section, other than subsection (a), the term 'service provider' means a provider of online services or network access, or the operator of facilities therefor, and includes an entity described in subparagraph (A). (2) Monetary relief.— As used in this section, the term 'monetary relief' means damages, costs, attorneys' fees, and any other form of monetary payment. (l) Other Defenses Not Affected.— The failure of a service provider's conduct to qualify for limitation of liability under this section shall not bear adversely upon the consideration of a defense by the service provider that the service provider's conduct is not infringing under this title or any other defense. (m) Protection of Privacy.— Nothing in this section shall be construed to condition the applicability of subsections (a) through (d) on— (1) a service provider monitoring its service or affirmatively seeking facts indicating infringing activity, except to the extent consistent with a standard technical measure complying with the provisions of subsection (i); or (2) a service provider gaining access to, removing, or disabling access to material in cases in which such conduct is prohibited by law. (n) Construction.—Subsections (a), (b), (c), and (d) describe separate and distinct functions for purposes of applying this section. Whether a service provider qualifies for the limitation on liability in any one of those subsections shall be based solely on the criteria in that subsection, and shall not affect a determination of whether that service provider qualifies for the limitations on liability under any other such subsection.

## Japanese Law on the Limitation of Liability<sup>368</sup>

- Article 3: limitation of liability for damages

1. When any right of others is infringed by information distribution via specified telecommunications, the specified telecommunications service provider who uses specified telecommunications facilities for said specified telecommunications hereinafter in this paragraph referred to as a 'relevant service provider') shall not be liable for any loss incurred from such infringement, unless where it is technically possible to take measures for preventing such information from being transmitted to unspecified persons and such

<sup>368</sup> Law on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders. [http://www.unesco.org/culture/pdf/anti-piracy/Japan/jp\\_%20LimitLiability\\_Telecom\\_en](http://www.unesco.org/culture/pdf/anti-piracy/Japan/jp_%20LimitLiability_Telecom_en).

event of infringement falls under any of the following items. However, where said relevant service provider is the sender of said information infringing rights, this shall not apply. (i) In cases where said relevant service provider knew that the infringement of the rights of others was caused by information distribution via said specified Telecommunications (ii) In cases where said relevant service provider had knowledge of information distribution by said specified telecommunications, and where there is a reasonable ground to find that said relevant service provider could know the infringement of the rights of others was caused by the information distribution via said specified telecommunications (2) When a specified telecommunications service provider has taken measures to block transmission of information via specified telecommunications, said specified telecommunications service provider shall not be liable for any loss incurred by a sender of such information, transmission of which is prevented by said measures, so far as said measures have been taken within the limit necessary for preventing transmission of said information to unspecified persons and said measures fall under any of the following items: (i) In cases where there was a reasonable ground for said specified telecommunications service provider to believe that the rights of others were infringed without due cause by the information distribution via said specified telecommunications (ii) In cases where a person alleging that his right was infringed by distribution of information via a specified telecommunications filed a petition that said specified telecommunications service provider take measures to prevent said information infringing his right (hereinafter referred to as 'infringing information') from being transmitted (hereinafter in this item referred to as 'transmission prevention measures'), indicating the infringing information and the allegedly infringed right and the reason why said person insists on said infringement (hereinafter in this item referred to as 'infringing information, etc.') and where said specified telecommunications service provider provided such infringing information, etc. to the sender of said infringing information and inquired the sender if said sender agrees with implementing said transmission prevention measures, where said specified telecommunications service provider has not received any notice from said sender indicating his disagreement with implementation of said transmission prevention measures after seven days from the day of said inquiry to said sender.

## Chapter 4: Annex 6

### Case law

#### Dutch case law

BREIN VS XS NETWORKS B.V. (24 OCTOBER 2012)	
Parties	<ul style="list-style-type: none"> <li>▪ BREIN</li> <li>▪ XS Networks</li> </ul>
Facts	<ul style="list-style-type: none"> <li>▪ XS Networks B.V. is a hosting ISP that hosts numerous websites, such as <a href="http://www.sumotorrent.com">www.sumotorrent.com</a> (hereinafter referred to as 'Sumotorrent'), a BitTorrent website. This case concerned the liability of the hosting provider (XS Networks) both for not providing the name and address information and for not promptly ceasing the services to the infringer.</li> <li>▪ BREIN repeatedly contacted XS Networks since 2008 in order to request the cessation of the provision of the hosting service to Sumotorrent, who was providing infringing content in prejudice of BREIN's members. BREIN also requested that XS Networks provide the contact information for Sumotorrent in order to comply with the NTD and to try to reach an agreement. XS Networks either did not respond to BREIN's request or provided incorrect contact details of Sumotorrent owner. Finally, Sumotorrent's site was closed, but not because of XS Networks decision of taking down the unauthorised content but because they were ceasing to operate.</li> <li>▪ BREIN claimed that users and holders of Sumotorrent infringed rights of their members via Sumotorrent by downloading and making available protected content such as films, music, games, television programs, software or ebooks without the permission required. The rightholders of this content (and members of BREIN) did not authorise the use of their creations through Sumotorrent. Furthermore, BREIN claimed that titles and film posters that were displayed at Sumotorrent also lacked their rightholders' permission. The examination of the case by the District Court of the Hague was divided into the following assessments:</li> <li>▪ Unlawful activities, infringement of copyright and neighbouring rights by Sumotorrent: The District Court of the Hague claimed that 'users of Sumotorrent infringe or at any rate have infringed the copyright and neighbouring rights of the parties affiliated to BREIN'. Nevertheless, the court decided that there was not sufficient evidence for BREIN's claim regarding Sumotorrent's collaboration in the infringement of their users of BREIN's affiliate's copyrights. Despite the aforementioned conclusion, the District Court of the Hague found that Sumotorrent was infringing the copyright of the titles and film posters displayed on their site, as they were inserted – and therefore made public - without the rightholders' authorisation.</li> <li>▪ Hosting activities: The District Court of the Hague asserted that XS Networks was the host of Sumotorrent. Nevertheless, XS Networks alleged that they were not a host but only offered server space with no connection to the content included on their customers' websites, also adding that their duties were to turn on or switch off the connection to the internet from the conflictive website. Nevertheless, the court resolved that their activity was a hosting service so these allegations were not admitted.</li> <li>▪ Keeping Sumotorrent removed: The court considered that it was evident that the</li> </ul>

	<p>activity carried out at Sumotorrent was unlawful and that it was repeatedly reported to XS Networks. Besides, the Court also considered that providing copyright-protected content without the corresponding rightholders' authorisation is unlawful. Hence, XS Networks had responsibility over the referred to content as the ISP and should have taken it down. XS Networks alleged that their responsibility was exempted by means of the application of Article 6:196c paragraph 4 of the Dutch Civil Code. But this was rejected by the District Court of the Hague for the motives mentioned in the paragraph above.</p> <ul style="list-style-type: none"> <li>▪ Providing Sumotorrent's identification details: BREIN also claimed from XS Networks the provision of the contact details of Sumotorrent owners and alleged that the defendant provided incorrect or false data.</li> </ul>
District Court of the Hague Decision	<ul style="list-style-type: none"> <li>▪ The motivation behind the District Court of the Hague's resolution is related to the case detailed in the previous section from the Dutch Supreme Court regarding Lycos vs. Pessers. It considers that the specific circumstances of the case determine that XS Networks was obliged to provide the exact contact details of Sumotorrent's owner as BREIN's interest in obtaining the referred to data prevailed among any other party's rights.</li> <li>▪ Conclusively, the District Court of the Hague declared that XS Networks acted unlawfully and ought to assume liability, for being aware of the unlawfulness of Sumotorrent's activities and not immediately ceasing to provide services to the latter, and neither provide the data of the owner of the illegal website to BREIN when demanded. As a consequence, XS Networks was prohibited from making publicly available Sumotorrent's (or the same customer of Sumotorrent) content and was ordered to provide BREIN all contact details necessary to contact Sumotorrent's owner.</li> <li>▪ Additionally, the court ordered that XS Networks was responsible for the damages caused to BumaStemra (member of BREIN) plus the costs of the court procedure and a penalty of ten (10) Euros per day for non-compliance with the Court's resolution.</li> </ul>

#### PESSERS V LYCOS DUTCH RULING (25 NOVEMBER 2005)

Parties	<ul style="list-style-type: none"> <li>▪ Pessers</li> <li>▪ Lycos</li> </ul>
Facts	<ul style="list-style-type: none"> <li>▪ In the context of a dispute between Pessers (a well-known seller of stamps in eBay) and Lycos (a Dutch provider hosting a website containing information criticising Pesser), Pessers contacted Lycos asking for the name and address of the person who had included material that was allegedly defamatory towards him. Lycos refused to do so, and this led to a Court ruling for Pessers against Lycos for the purpose of obtaining the name and address of the wrongdoer in order to recover damages.</li> <li>▪ In this regard, Lycos claimed that the disclosure of the personal data requested was unlawful as it was not made clear that the content of the website was illegal, so they did not have to provide such contact details.</li> <li>▪ Moreover, this Dutch Supreme Court ruling is key as it also provides a list of four (4) situations when the provider acts unlawfully by the non-provision of the personal data of the Content Provider to the Notifier: <ol style="list-style-type: none"> <li>1) When the possibility that the information is unlawful and harmful vis-à-vis the third party is sufficiently likely;</li> </ol> </li> </ul>

PESSERS V LYCOS DUTCH RULING (25 NOVEMBER 2005)	
	<ol style="list-style-type: none"> <li>2) When the third party has a real interest in obtaining the personal data;</li> <li>3) When it is likely that in the specific case no less drastic option exists to obtain the personal data; and</li> <li>4) When the balance between the interests of the Notifier, the ISP and the website owner involved (as far as known) implies that the interest of the Notifier should prevail.</li> </ol>
Dutch Supreme Court Decision	<ul style="list-style-type: none"> <li>▪ In the context of a dispute between Pessers (a well-known seller of stamps in eBay) and Lycos (a Dutch provider hosting a website containing information criticising Pesser), Pessers contacted Lycos asking for the name and address of the person who had included material that was allegedly defamatory towards him. Lycos refused to do so, and this led to a Court ruling for Pessers against Lycos for the purpose of obtaining the name and address of the wrongdoer in order to recover damages.</li> <li>▪ In this regard, Lycos claimed that the disclosure of the personal data requested was unlawful as it was not made clear that the content of the website was illegal, so they did not have to provide such contact details.</li> <li>▪ Moreover, this Dutch Supreme Court ruling is key as it also provides a list of four (4) situations when the provider acts unlawfully by the non-provision of the personal data of the Content Provider to the Notifier: <ol style="list-style-type: none"> <li>1) When the possibility that the information is unlawful and harmful vis-à-vis the third party is sufficiently likely;</li> <li>2) When the third party has a real interest in obtaining the personal data;</li> <li>3) When it is likely that in the specific case that no less drastic option exists to obtain the personal data; and</li> <li>4) When the balance between the interests of the Notifier, the ISP and the website owner involved (as far as knowable) implies that the interest of the Notifier should prevail.</li> </ol> </li> </ul>

TELEATLAS V PLANET INTERNET DUTCH RULING (9 JULY 2002)	
Parties	<ul style="list-style-type: none"> <li>▪ Teleatlas</li> <li>▪ Planet Internet</li> </ul>
Facts	<ul style="list-style-type: none"> <li>▪ Teleatlas is a company offering navigational software and in this case the issue was in relation to taking judicial action against Internet users selling illegal copies of Teleatlas-software on auction websites such as eBay. In this respect, Teleatlas asked for the names and addresses of these persons using the Dutch ISP Planet Internet. Planet Internet is a Dutch ISP that offers, inter alia, email addresses to its subscribers.</li> <li>▪ Nonetheless, the latter refused to provide such contact details claiming it was unlawful in terms of its clients and that there was no legitimate ground to demand them.</li> </ul>
District Court of Utrecht Decision	<ul style="list-style-type: none"> <li>▪ The Court agreed with Planet Internet on not realising the personal data since this request should be dealt with in light of Article 8 of the PDPA, which highlights the processing of personal data is exclusively permitted when it appears strictly</li> </ul>

#### TELEATLAS V PLANET INTERNET DUTCH RULING (9 JULY 2002)

	<p>necessary to fulfil the interests of the responsible person regarding this data and when the interests of the person whose data will be processed do not prevail. Additionally, the Court stressed that one should also take other paths to retrieve the person's data, thus, in this case Teleatlas could have contacted the website in which the illegal copies were sold in the first place. As a consequence, Planet Internet did not disclose the personal data of its clients.</p>
--	---

#### SCIENTOLOGY V XS4ALL13 DUTCH RULING (4 SEPTEMBER 2003)

Parties	<ul style="list-style-type: none"> <li>▪ Scientology</li> <li>▪ XS4ALL13</li> </ul>
Facts	<ul style="list-style-type: none"> <li>▪ There are three (3) significant controversies within the scope of copyright infringement: whether displaying a link to copyright infringing information constitutes a copyright infringement itself, whether an ISP can be held liable if it refuses to reveal the name and address of its clients who happen to be the alleged wrongdoer and whether an ISP will be deemed to be acting unlawfully if it, upon a previous complaint, does not remove the link.</li> <li>▪ In this case, Scientology claimed that XS4ALL, having a link online to a website with unlawful content, constituted copyright infringement.</li> </ul>
Court of the Hague Decision	<ul style="list-style-type: none"> <li>▪ The Court stated that ISPs are not publishing information themselves but simply provide the means for other parties to publish and therefore are not themselves infringing any copyright. Nonetheless, the Court clarifies that, in the event a client has provided information online which is illegal, an ISP has the duty to take the necessary steps to solve this.</li> </ul>

#### BREIN VS. KPN (5 JANUARY 2007)

Parties	<ul style="list-style-type: none"> <li>▪ BREIN</li> <li>▪ KPN</li> </ul>
Preliminary Relief Judge The Hague District Court Decision	Being the hosting provider of the unlawful website dutchtorrent.org which structurally facilitates copyright infringement, KPN is ordered to provide the Name and Address Info of the operator and to close down said website.

#### BREIN VS. LEASEWEB (25 NOVEMBER 2005)

Parties	<ul style="list-style-type: none"> <li>▪ BREIN</li> <li>▪ Leaseweb</li> </ul>
Amsterdam Appeal Court Decision	The Court rules that notifications of BREIN comply with the requirement to provide data on which Leaseweb could estimate whether site holders' conduct is unlawful or not, without unreasonably extensive research.

#### BREIN VS. KPN (5TH JANUARY 2007)

Parties	<ul style="list-style-type: none"> <li>▪ BREIN</li> <li>▪ KPN</li> </ul>
Preliminary Relief Judge The Hague District Court Decision	Being the hosting provider of the unlawful website dutchtorrent.org which structurally facilitates copyright infringement, KPN is ordered to provide the Name and Address Info of the operator and to close down said website.

#### BREIN VS. EUROACCESS (8 JULY 2008)

Parties	<ul style="list-style-type: none"> <li>▪ BREIN</li> <li>▪ Euroaccess</li> </ul>
Den Bosch District Court Decision	Being the hosting provider of an unlawful website which structurally facilitates copyright infringement, Euroaccess is ordered to provide the Name and Address Info of the operator of torrent.to. Euroaccess must also make an effort to retrieve the identity. Order to pay full legal costs.

#### BREIN VS. KPN (5 JANUARY 2007)

Parties	<ul style="list-style-type: none"> <li>▪ BREIN</li> <li>▪ KPN</li> </ul>
Preliminary Relief Judge The Hague District Court Decision	Being the hosting provider of the unlawful website dutchtorrent.org which structurally facilitates copyright infringement, KPN is ordered to provide the Name and Address Info of the operator and to close down said website.



EKSMO VS. ECATEL (1 NOVEMBER 2013)	
Parties	<ul style="list-style-type: none"> <li>▪ BREIN</li> <li>▪ Ecatel</li> </ul>
Preliminary Relief Judge The Hague District Court Decision	The hosting provider Ecatel acted unlawfully by not promptly blocking the IP address of illegal sites after notification. One of the sites had returned to the same IP address at Ecatel after finding temporary accommodation elsewhere. This was contrary to the allegation of Ecatel that a returning site would automatically get a different IP address.

## CJEU case law

PROMUSICAE CJEU RULING (29 JANUARY 2008)	
Parties	<ul style="list-style-type: none"> <li>▪ Productores de Música de España (hereinafter, 'Promusicae').</li> <li>▪ Telefónica de España, S.A.U. (hereinafter, 'Telefónica').</li> </ul>
Facts	<ul style="list-style-type: none"> <li>▪ PROMUSICAE is a Spanish non-profit-making organisation of producers and publishers of musical and audio-visual recordings.</li> <li>▪ TELEFONICA is a Spanish commercial company whose activities include the provision of internet access services.</li> <li>▪ PROMUSICAE asked for TELEFONICA to be ordered to disclose the identities and physical addresses of certain persons to whom it provided with internet access services, whose IP address and date and time of connection were known. According to PROMUSICAE, those persons used a file exchange program (peer-to-peer) and provided access in shared files of personal computers to phonograms in which the members of PROMUSICAE held the exploitation rights.</li> <li>▪ The Spanish Judge ordered the preliminary measures requested by PROMUSICAE. TELEFONICA appealed against that order, arguing that under the Spanish Law implementing the E-Commerce Directive, communications of data required by PROMUSICAE were authorised only in a criminal investigation or for the purpose of safeguarding public security and national defence, not in civil proceedings including for preliminary measures.</li> <li>▪ PROMUSICAE argued that the Spanish Law implementing the E-Commerce Directive must be interpreted in accordance with various provisions of the E-Commerce Directive, the InfoSoc Directive and the Enforcement Directive and with Articles 17.2 ('Right to Property') and 47 ('Right to an effective remedy and to a fair trial') of the Charter of Fundamental Rights. Such provisions do not allow a Member State to limit solely to the purposes expressly mentioned in that law the obligations to communicate the data in question</li> </ul>
Preliminary Ruling	<ul style="list-style-type: none"> <li>▪ By its questions, the national Court asked essentially whether Community law, in particular the E-Commerce Directive, the InfoSoc Directive and the Enforcement Directive read also in the light of Articles 17 ('Right to Property') and 47 ('Right to an effective remedy and to a fair trial') of the Charter of Fundamental Rights, must be interpreted as requiring Member States to lay down, in order to ensure effective protection of copyright, an obligation to communicate personal data in the context of civil proceedings.</li> </ul>
CJEU Decision	<ul style="list-style-type: none"> <li>▪ The CJEU has established that the E-Commerce Directive, the InfoSoc Directive, the Electronic Communications Directive, the Enforcement Directive and the E-</li> </ul>

PROMUSICAE CJEU RULING (29 JANUARY 2008)	
	<p>Commerce Directive do not require Member States to lay down an obligation to communicate personal data in order to ensure effective protection of copyright in the context of a civil proceeding.</p> <ul style="list-style-type: none"> <li>▪ However, according to the CJEU, European law requires that, when incorporating those Directives into national laws, Member States shall take care to rely on an interpretation of them which allows a fair balance between the various fundamental rights protected by the European legal order, namely, on the one hand the protection of personal data and, on the other the protection of property (including intellectual property) and the right to an effective remedy.</li> <li>▪ The mechanisms allowing those different rights and interests to be balanced are contained in the Electronic Commerce Directive, in that it provides for rules which determine in what circumstances and to what extent the processing of personal data is lawful and what safeguards must be provided for, and in the E-Commerce Directive, the InfoSoc Directive and the Enforcement Directive which reserve the cases in which the measures adopted to protect the rights they regulate affect the protection of personal data. Moreover, they result from the adoption by Member States of national provisions transposing those Directives and their application by national authorities.</li> <li>▪ Further, when implementing those Directives, the Authorities and Courts of the Member States must not only interpret their national law in a manner consistent with those Directives but also make sure that they do not rely on an interpretation of them which would be in conflict with those fundamental rights or with the other general principles of European law, such as the principle of proportionality.</li> </ul>
BONNIER CJEU RULING (19 APRIL 2012)	
Parties	<ul style="list-style-type: none"> <li>▪ Bonnier Audio AB</li> <li>▪ Earbooks AB</li> <li>▪ Norstedts Förlagsgrupp AB</li> <li>▪ Piratförlaget AB</li> <li>▪ Storyside AB</li> <li>▪ Perfect Communication Sweden AB</li> </ul>
Facts	<p>Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB and Storyside AB are publishing companies which hold, inter alia, exclusive rights to the reproduction, publishing and distribution to the public of copyright works. In this specific case, they had the right of reproducing, publishing and distributing 27 works in the form of audio books. Perfect Communication Sweden AB through the platform 'ePhone' was the ISP through which an alleged illegal file exchange of the referred to 27 works took place.</p>
Preliminary Ruling	<p>The main concern is the interpretation of Articles 3 to 5 and 11 of Directive 2006/24/EC of the European Parliament and of the Council on 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54), and of Article 8 of Directive 2004/48/EC of the European</p>

BONNIER CJEU RULING (19 APRIL 2012)	
	Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights <sup>369</sup> .
CJEU Decision	Being the hosting provider of an unlawful website which structurally facilitates copyright infringement, Euroaccess is ordered to provide the Name and Address Info of the operator of torrent.to. Euroaccess must also make an effort to retrieve the identity. Order to pay full legal costs.

<sup>369</sup> <http://curia.europa.eu/juris/document/document.jsf?text=&docid=121743&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=437217>.

## **CHAPTER 5: DANISH CODE OF CONDUCT FOR MANAGEMENT OF RULINGS ON BLOCKING TO INFRINGEMENTS OF RIGHTS**



## Chapter 5: Glossary of terms

For the purposes of this Chapter 5, the following definitions apply:

- **Art. 29 WP:** the Article 29 Data Protection Working Party that was set up under the Data Protection Directive. It has advisory status and acts independently and it is composed of a representative of the supervisory authority(ies) designated by each European Union country, a representative of the authority(ies) established by the European Union institutions and bodies and representatives of the European Commission<sup>370</sup>.
- **BASCAP:** Business Action to Stop Counterfeiting and Piracy, a subgroup of the International Chamber of Commerce<sup>371</sup>.
- **BEUC:** the *Bureau Européen des Unions de Consommateurs*<sup>372</sup>, the European consumer organisation.
- **Case C-160/15**<sup>373</sup>: the Advocate General's Opinion of 07/04/2016, C-160/15, GS Media, EU:C:2016:221.
- **Code of Conduct:** the Teleindustrien Code of Conduct for the management of rulings on blocking related to the infringement of rights (*Code of Conduct for håndtering af afgørelser om spærring i forbindelse med ret-tighedskrænkelser*)<sup>374</sup>.
- **Copyright Package:** the eight initiatives launched on 20 June 2012 by the Danish Ministry of Culture that aimed, on the one hand, to support initiatives combating piracy on the internet and, on the other hand, to encourage consumers to use legal alternatives available on the internet thereby promoting more legal content on the internet (*Ophavsretspakken*)<sup>375</sup>.
- **Danish Administration of Justice Law:** the consolidated version of the Danish Administration of Justice Law, 25 June 2014 (*Retsplejeloven*)<sup>376</sup>.
- **Danish Copyright Law:** consolidated Danish law No. 1144 of 23 October 2014 on copyright (*Ophavsretsloven*)<sup>377</sup>.
- **Danish Data Protection Law:** law No. 429 of 31 May 2000 on the processing of personal data, which entered into force on 01 July 2000<sup>378</sup>.
- **Danish E-Commerce Law:** law No. 227 of 22 April 2002 on certain legal aspects of information society services, in particular electronic commerce<sup>379</sup>.
- **Data Protection Directive:** the Directive of 24 October 1995 on Data Protection<sup>380</sup>. At the moment of the drafting of this Study, the Data Protection Directive was in force. This Directive **has been repealed** by the General Data Protection Regulation on May 2016.
- **Declaration of Intent:** the Danish code of conduct to promote lawful behaviour on the internet, signed 08 May 2015 by trade associations, companies and rightholders<sup>381</sup>.
- **DNS:** the domain name system.

<sup>370</sup> [http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/index\\_en.htm](http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/index_en.htm).

<sup>371</sup> <http://www.iccwbo.org/advocacy-codes-and-rules/bascap/welcome-to-bascap/>.

<sup>372</sup> <http://www.beuc.eu/>.

<sup>373</sup> <http://curia.europa.eu/juris/document/document.jsf?text=&docid=175626&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=827402>.

<sup>374</sup> An English version of the Code of Conduct is attached in Annex 1 of this Chapter 5. This document has been provided by Teleindustrien.

<sup>375</sup> An English version of the Copyright Package is attached in Annex 2 of this Chapter 5. This document has been provided by the Danish Ministry of Culture.

<sup>376</sup> See Annex 6 of this Chapter 5.

<sup>377</sup> Law No. 202 of 27 February 2010 on Copyright.

<sup>378</sup> See Annex 6 of this Chapter 5.

<sup>379</sup> Law No. 227 of 22 April 2002 on certain legal aspects of information society services, in particular electronic commerce.

<sup>380</sup> Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23/11/1995 pp 0031 – 0050.

<sup>381</sup> Code of Conduct to promote lawful behaviour on the internet,  
<http://www.authorsocieties.eu/uploads/DK%20Declaration%20of%20intent.pdf>.

- **CJEU**: the Court of Justice of the European Union<sup>382</sup>.
- **E-Commerce Directive**: the European Union Directive of 8 June 2000 on electronic commerce<sup>383</sup>.
- **Enforcement Directive**: the Directive of 29 April 2004 on the enforcement of intellectual property rights<sup>384</sup>.
- **IFPI**: the International Federation of the Phonographic Industry<sup>385</sup>.
- **InfoSoc Directive**: the Directive of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society<sup>386</sup>.
- **IP address**: a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the internet protocol for communication.
- **ISP**: internet service providers, the companies that provide access to the internet.
- **Kino.to CJEU Ruling**: the Ruling issued on 27 March 2014 by the CJEU in case C-314/12, UPC Telekabel Wien, EU:C:2013:781<sup>387</sup>.
- **Open Internet Access Regulation**<sup>388</sup>: the regulation laying down measures concerning open internet access.
- **Promusicae CJEU Ruling**: the Ruling issued on 29 January 2008 by the CJEU in case C-275/06, Promusicae, EU:C:2008:54<sup>389</sup>.
- **RettighedsAlliancen**: the Danish rightholder alliance<sup>390</sup>.
- **Rightholder**: any individual or organisation acting on behalf of the owner of a copyright, design or trade mark<sup>391</sup>.
- **Signatories**: all the parties who have signed the Code of Conduct<sup>392</sup>.
- **SWC**: 'Share with Care', a campaign result of the joint initiative between the Danish internet service providers, Teleindustrien, the Danish Ministry of Culture and RettighedsAlliancen.
- **TDC A/S**: a telephone company in Denmark<sup>393</sup>.
- **Teleindustrien**: the Danish telecom industry association<sup>394</sup>.
- **UBVA**: the Danish Committee for the protection of scientific work, a committee of academics with interests in copyright and patent law (*Udvalget til Beskyttelse af Videnskabeligt Arbejde*<sup>395</sup>).
- **VCP**: 'voluntary collaboration practices' developed by industry, public bodies and/or third parties, such as non-governmental organisations, and then adhered to by the respective industry in order to address the infringement of trade mark rights, design rights, copyright and rights related to copyright over the

<sup>382</sup> [http://curia.europa.eu/jcms/jcms/i\\_6/](http://curia.europa.eu/jcms/jcms/i_6/).

<sup>383</sup> Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ L 178, <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32000L0031>.

<sup>384</sup> Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, OJ L 157, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:195:0016:0025:en:PDF>.

<sup>385</sup> <http://ifpi.org/>.

<sup>386</sup> Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167, <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32001L0029>.

<sup>387</sup> <http://curia.europa.eu/juris/liste.jsf?num=C-314/12>.

<sup>388</sup> Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015, laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union. <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R2120&from=EN>.

<sup>389</sup> <http://curia.europa.eu/juris/liste.jsf?language=en&num=C-275/06>.

<sup>390</sup> <http://www.rettighedsalliancen.dk/>.

<sup>391</sup> The Rightholders interviewed for this Chapter 5 are a sampling of those involved in the VCP.

<sup>392</sup> See complete list of Signatories in Annex 4 of this Chapter 5.

<sup>393</sup> <http://tdc.com/>.

<sup>394</sup> <http://www.teleindustrien.dk/>.

<sup>395</sup> <http://www.ubva.dk/>.

internet. With regard to the present Chapter 5, 'VCP' comprises in particular the Teleindustrien Code of Conduct for the management of ruling on blocking related to the infringement of rights.

- **Workgroups:** the result of an initiative from the Dialogue Forum where the aim is to reach voluntary agreements between all parties intervening on the internet in order to fight against copyright infringement.



## Chapter 5: Structure and content

This Chapter 5 analyses the Code of Conduct in depth by assessing the following elements:

- Role of signatories and third parties involved in the Code of Conduct;
- Analysis of the duties and procedures prescribed by the Code of Conduct;
- Coexistence of the measures provided for under the Code of Conduct with the European Union and Danish legal frameworks and related case law;
- Role of technologies used in implementing the duties and procedures as set forth by the Code of Conduct;
- Costs assumed by the parties involved in the implementation of the Code of Conduct;
- Role of educational activities of the parties involved in promoting the Code of Conduct;
- Effectiveness of the measures envisaged by the Code of Conduct.

This Chapter 5 initially involved exhaustive desk research to identify the signatories and third parties involved in the Code of Conduct. A sample of them were then interviewed for the purposes of this Chapter 5.

The statements contained in the Chapter 5 on the signatories and third parties' position regarding the Code of Conduct and their day-to-day procedure are based on the feedback and supporting documentation provided by those stakeholders that agreed to participate in the Chapter 5.

## 1. Introduction

The Code of Conduct, adopted in September 2014, is one of the initiatives that resulted from political debates, considerations and suggestions in Denmark as to how rightholders could confront the problems of unauthorised content distribution.

The Danish Ministry of Culture was aware of the advantages the internet provided to the creative industries, allowing direct and quick access to all kinds of creative content. However, the Ministry of Culture was concerned about the proliferation of unauthorised copies of creative content protected by copyright, which threatened not only intellectual property rights, but also the development of digital businesses.

On 20 June 2012, the Danish Ministry of Culture enhanced the protection of intellectual property rights through the launch of the Copyright Package, a range of legal initiatives directed at all stakeholders, businesses and users in order to fight against the unauthorised sharing of creative content on the internet. This Copyright Package, published by the Danish Ministry of Culture, encourages users to use legal alternatives and fight against unauthorised content, thereby reducing its internet distribution and contributing to the growth of the creation sector<sup>396</sup>.

The Copyright Package contains a total of eight<sup>397</sup> initiatives that have been gradually implemented<sup>398</sup>. Two initiatives resulted in two written Codes of Conduct<sup>399</sup>, (1) the first, concerning the management of court decisions on the blocking of websites due to rights infringements, and (2) the second, concerning the promotion of lawful behaviour on the internet.

The Danish Ministry of Culture invited Teleindustrien to adopt the first of the abovementioned codes, the Code of Conduct<sup>400</sup>, as one of the Copyright Package initiatives ('Guidelines for the blocking of illegal services on the internet'). Communication operators and copyright owners agreed on the procedures that follow regarding blocking access to illegal services on the internet.

The Code of Conduct was adopted with the main aim of simplifying and ensuring that court rulings on DNS website blocking are implemented<sup>401</sup>. The Code of Conduct adheres to the efficiency of the rulings on DNS blocking by implementing a period of seven working days from the day that the court orders the blocking. For this purpose, rightholders and ISPs collaborate closely to reduce the

---

<sup>396</sup> Danish Ministry of Culture, 20 June 2012, 'Initiatives to boost the creation of legal content on the internet'.

<sup>397</sup> **Copyright Package: 1) Innovation Forum:** This forum focuses on identifying possible barriers and exchanging good practices for the development of digital business models within the different creative fields. **2) A common informative campaign directed to users:** The Ministry of Culture, representatives of the television sector, copyright owners and the Danish Consumer Council (*Forbrugerrådet*) engaged together in an informative campaign in 2012 in order to contribute to the awareness of legal services among consumers. **3) Concrete information and users' dialogue:** Copyright owners created an operative informative group by establishing user dialogue with those downloading and making use of illegal content on the internet. **4) Dialogue Forum:** The Ministry of Culture started up a voluntary dialogue forum among copyright owners and online service providers which distribute creative content. These dialogues focus on guaranteeing that these owners are allowed to withdraw illegal contents by themselves. **5) Guidelines for the blocking of illegal services on the internet:** Communications operators and copyright owners concluded an agreement on the procedures to be followed in relation to the blocking of access to illegal services on the Internet. This is formalised in the form of the Code of Conduct which stipulates that operators will respect court judgments concerning blocking of their clients' access to illegal content. **6) Measures aimed at the diffusion of a secure usage of internet connections:** Telephone operators' representatives elaborated guidelines for new devices, due to the existence of the Wireless connection to the internet. The aim of these guidelines is to use protective measures like private passwords, or alternative forms of encryption, so that it becomes impossible to make use of it with no authorisation. **7) Information of telephone operators:** It is permitted that Telephone operators' send the bills to their clients, enclosing informative literature concerning the importance of protecting their internet connection against illicit uses and the importance of using legal alternatives. **8) Evaluation of current and future initiatives:** The Committee on Copyright on the internet proposed in its report a possible model referred to as 'model letter'. This model involves telephone operators, on behalf of copyright owners, providing informative letters to their clients operating on the internet, in the event their connection can be related to any copyright infringement on the internet.

<sup>398</sup> A copy of the Danish Ministry of Culture, 20 June 2012, 'Initiatives to boost the creation of legal content on the internet', is enclosed as Annex 2 of this Chapter 5.

<sup>399</sup> [http://www.wipo.int/edocs/mdocs/enforcement/en/wipo\\_ace\\_10/wipo\\_ace\\_10\\_23.pdf](http://www.wipo.int/edocs/mdocs/enforcement/en/wipo_ace_10/wipo_ace_10_23.pdf).

<sup>400</sup> A copy of the Code of Conduct is enclosed as Annex 1 of this Chapter 5.

<sup>401</sup> A further study regarding DNS blocking is detailed in Section 3 of this Chapter 5 ('Duties and Procedures').

infringement of online intellectual property rights. The Code of Conduct is in two parts, comprising (i) a brief background summary, (ii) its development, (iii) its purpose, in the first part and an Annex with a procedure to follow in the second part.

According to the Code of Conduct, rightholders start a procedure by filing a claim before a Danish court in order to obtain a resolution to block a website where intellectual property rights are being infringed. Once the court has resolved in favour of the rightholders, the decision is communicated to all Teleindustrien members who block the conflictive website as soon as possible. In this respect, Teleindustrien members commit to implement the procedure set out in the abovementioned Code of Conduct and ensure its compliance.

As will be explained further in Section 3 of this Chapter 5 ('Duties and Procedures'), in March 2015 the Code of Conduct was amended <sup>402</sup> by Teleindustrien based on particular experiences previously discussed with RettighedsAlliancen. This amendment defined how blocking should be dealt with when the unauthorised content has moved to other websites. In this event, if the rightholders report such movement to another domain, this new page will also be blocked under the proviso that it is exactly the same content as that covered by the prior court ruling.

Likewise, the Code of Conduct as part of one of the initiatives of the Copyright Package also interacts with other initiatives such as the SWC campaign, which displays a communication on the blocked website informing users about the block and redirecting them to legal alternatives of the creative content they are interested in.

Denmark has notable experience in taking measures for the protection of online intellectual property rights. Danish Courts not only ordered one of the first rulings for website blocking within the European Union in 2006 <sup>403</sup> but also the Danish Supreme Court, in 2010 <sup>404</sup>, was one of the first national courts to issue a website blocking order based on the provisions of the InfoSoc Directive <sup>405</sup>.

---

<sup>402</sup> The amendment of the Code of Conduct was performed on 19 March 2015.

<sup>403</sup> Copenhagen City Court, 25 October 2006, case No. FI-15124/2006 IFPI Denmark v Tele2 A/S.

<sup>404</sup> Supreme Court of Denmark, 27 May 2010, case No. 153/2009, IFPI v Sonofon, the so-called 'thepiratebay.org' case.

<sup>405</sup> Maria Fredenslund, 24 October 2014, 'Denmark: Code of Conduct on website blocking',  
<http://kluwercopyrightblog.com/2014/10/24/denmark-code-of-conduct-on-website-blocking/>.

## 2. Signatories of the Code of Conduct and third parties

In recent times, ISPs have been challenged by rightholders, enforcement authorities and relevant stakeholders to adopt practical and accessible measures to fight against copyright-infringing activity on the internet<sup>406</sup>.

This Code of Conduct is signed by members of the Danish Telecommunications Industry (ISPs) and rightholders. Public authorities, such as the Danish Ministry of Culture, are not current signatories of the Code of Conduct but encourage preliminary meetings and dialogues between rightholders and ISPs.

This Section of Chapter 5 explains the specific roles regarding the VCP played by the four main categories of stakeholders addressed (i.e., rightholders, ISPs, public authorities and civil society).

### 2.1. Role of the RettighedsAlliancen<sup>407</sup>

The RettighedsAlliancen is the Danish Rightholder Alliance, an important body in the implementation of this Code of Conduct. This association is formed by different organisations belonging to the creative industries such as film, music, text and design, which represent more than eighty-five thousand Danish rightholders. Their aims are the improvement and protection of cultural content on the internet<sup>408</sup>.

rightholders have an important role in the application of the Code of Conduct. They report the existence of infringing activity on the internet and request its removal. Rightholders, or representatives of the RettighedsAlliancen, start the procedure as established within the Code of Conduct by filing claims before the court for the blocking of a specific website.

The role of the RettighedsAlliancen in this Code of Conduct comprises the initiation of the blocking procedure, as this body is, in most cases, the one in charge of notifying Teleindustrien of the specific website/domains that have to be blocked according to court resolutions.

Currently, its main function is to collect evidence and go to court on behalf of the rightholders it represents. Also, the RettighedsAlliancen holds regular meetings with rightholders and ISPs in order to discuss the development and use of the Code of Conduct and take account of the strengths and weaknesses of its practice.

It is also important to note the RettighedsAlliancen's participation in the SWC, which is laid out in Section 7 of this Chapter 5 ('Education'), as it also contributes to (i) the strengthening of partnerships between interested parties, (ii) increasing and disseminating the knowledge of legal services for consumers, and (iii) looking out for new methods to influence young people's digital behaviour.

### 2.2. Role of the Danish Ministry of Culture (*Kulturministeriet*)

The Danish Ministry of Culture is a public body devoted to the development of cultural institutions and cultural policy in Denmark.

Regarding the VCP examined, the Danish Ministry of Culture is a relevant stakeholder since, as mentioned above, it launched in 2012 a Copyright Package of eight distinct initiatives, further consolidated in a campaign created with Teleindustrien and the copyright industry. Nonetheless, this body does not play an active role within this practice, as it only took part in the proposal and worked upon the invitation of drafting a Code of Conduct.

The Ministry of Culture also participated in the creation of the SWC.

---

<sup>406</sup> BASCAP report 'Roles and responsibilities of Intermediaries: fighting counterfeiting and piracy in the supply chain', page 69.

<sup>407</sup> The Rightholders interviewed for this Chapter 5 are a sampling of those involved in the VCP.

<sup>408</sup> Rettighedsalliancen. <http://www.rettighedsalliancen.dk/>.

## 2.3. Role of intermediaries

### 2.3.1. Teleindustrien

Teleindustrien is an essential body in the functioning of this Code of Conduct, not only for its role in the drafting of it, but also because it acts as the nucleus between all parties implicated in the practice. This body is in charge of receiving claims from rightholders that have entered into judicial proceedings regarding intellectual property infringements on the internet, in which the court determines which specific ISP should block a certain homepage.

The rightholders communicate the court order to Teleindustrien, who inform its members to arrange the blocking of infringing websites, with a text saying: 'according to the Code of Conduct, we now ask you to also implement this court order within seven working days and we advise you to use this stand up text on the blocking page that we block where we say this page is blocked and if you are interested in finding legal content please go to this home page'. The homepage has legal content. Likewise, Teleindustrien keeps a track record of all blockings implemented.

It is essential to clarify that Teleindustrien's role does not imply a ruling or judgment, it does not even analyse whether an action committed implies an infringement: 'that's up to the court's evaluation and discretion'.

It is, however, important to address that this VCP is not exclusive to Teleindustrien's members. In the event that a court order is sent to this body, it is distributed not only to all its members but also to other operators. Pursuant to the information obtained by Teleindustrien, telecom operators that are not members of this organisation also follow this Code of Conduct in practice.

### 2.3.2. ISPs

Danish telecommunication companies<sup>409</sup> provide internet services. Pursuant to the information obtained from Teleindustrien, all its members<sup>410</sup> comply with the Code of Conduct and other operators who are not members of Teleindustrien follow the Code of Conduct. As stated in the Code of Conduct, whenever a court decision establishes a blocking, Teleindustrien communicates this decision to all its members internally as they are committed to implement the court order within seven days. This means that their role is blocking those addresses the court has ordered to be blocked.

## 2.4. Role of civil society

### 2.4.1. Danish Consumer Council (*Forbrugerrådet*)<sup>411</sup>

The Danish Consumer Council is an independent organisation representing the interests of consumers. This consumer council belongs to more than two hundred committees. Its main goal is to defend consumer rights and strengthen their role in the market. For this purpose the Danish Consumer Council encourages dialogue with the business community from various sectors.

---

<sup>409</sup> For the execution of this report, we have interviewed TDC Group A/S and Telia.

<sup>410</sup> This is a list of all the members of Teleindustrien who complies with the Code of Conduct, <http://www.teleindu.dk/om-ti/medlemmer-af-ti/>.

<sup>411</sup> [http://www.consumersinternational.org/our-members/member-directory/The%20Danish%20Consumer%20Council%20-%20Forbrugerr%C3%A5det%20\(Council\)](http://www.consumersinternational.org/our-members/member-directory/The%20Danish%20Consumer%20Council%20-%20Forbrugerr%C3%A5det%20(Council)).

### 3. Duties and procedures

Before the launch of the Code of Conduct, the main stakeholders, Teleindustrien members and the RettighedsAlliancen had a non-written practice in which they acted according to what was required in the Code of Conduct. In this sense, relevant stakeholders affirmed that the procedure set forth in the Code of Conduct already existed and was applied by the relevant parties of the sector but until the Code of Conduct was launched this practice was not formalised in a written document. The Code of Conduct is a voluntary agreement between the members of Teleindustrien<sup>412</sup> and other relevant Danish ISPs, but in a particular case it will not prevent an ISP from conducting the procedure by itself if necessary<sup>413</sup>.

In this Section we will analyse the procedure established by the Code of Conduct, including details regarding its territorial application, the technical issues related to the blocking of websites and the consequences of non-fulfilment of its dispositions.

#### 3.1. Scope of application of the VCP

The Code of Conduct's territorial limit is Denmark and Danish ISPs. Therefore, to comply with the Code of Conduct, ISPs will only follow Danish court resolutions.

In spite of this, it can occur that a Danish Court orders the blocking of a website with a domain name from another country as long as the rightholder (natural person or legal entity), whose intellectual property rights are infringed, is Danish, and as long as the website can be accessed from Denmark. The Interior Addict case from the Maritime and Commercial Court in Copenhagen, on 11 December 2014<sup>414</sup>, was resolved in favour of Danish designers who detected that copies of their works were being sold through the online store Interior Addict<sup>415</sup>, a website based in England, by distributing illegally copied furniture and lamps in Denmark<sup>416</sup>. These days, one of the main challenges for rightholders is fighting against piracy from websites based outside the jurisdiction in which the infringement takes place<sup>417</sup>.

#### 3.2. Procedure

The Code of Conduct protects rightholders against all types of intellectual property infringements, with copyright and trade mark infringements appearing to be the most common cases.

The procedure set forth in the Code of Conduct starts with the presentation of the claim before the corresponding Danish court in order to request the blocking of a website that infringes intellectual property rights<sup>418</sup>. Although, according to the terms of the Code of Conduct, rightholders are entitled to file the claim, in practice the RettighedsAlliancen files the claims in representation of the majority of Danish rightholders. Once the claim has been filed, the RettighedsAlliancen informs Teleindustrien so they are aware of the procedure from the beginning.

---

<sup>412</sup> The list of Teleindustrien's members is enclosed as Annex 4 of this Chapter 5.

<sup>413</sup> Paragraphs 5 to 8, page 2 of the Code of Conduct clarifies that 'The present [Code of Conduct] represents a voluntary agreement between the members of [Teleindustrien] who will endeavour to comply with the agreement. [Code of Conduct], nevertheless, do not prevent an [Teleindustrien] member from reserving the right to separately try the case if he or she so finds it necessary for whatever special reason'.

<sup>414</sup> Maritime and Commercial Court in Copenhagen, 11 December 2014, Fritz Hansen A/S, Louis Poulsen Lighting A/S, Carl Hansen & Son Mobelfabrik A/S, Fredericia Furniture A/S, Erik Jorgensen Mobelfabrik A/S v Telia Danmark. <http://kluwercopyrightblog.com/files/2015/01/IA11122014EN.pdf>.

<sup>415</sup> [www.interioraddict.co.uk](http://www.interioraddict.co.uk).

<sup>416</sup> This court case will be further studied in Annex 7 of this Chapter 5.

<sup>417</sup> BASCAP report 'Roles and responsibilities of Intermediaries: fighting counterfeiting and piracy in the supply chain', page 74.

<sup>418</sup> The Annex exempt from Official Publication of the Code of Conduct establishes in its point 1 that 'Subsidiary it could be another authority which based on specific legislation can issue such an order', meaning that any authority could order a DNS blocking. Nevertheless, relevant stakeholders appointed that in practice blocking orders only are issued by Danish courts and no other authority participates in this process at the moment. We understand this is only a provision established by the Code of Conduct for the event that new Danish legislation entitles other authorities apart from courts to issue orders to block websites.

A court order is required to implement the blocking. Without one, the blocking would have no basis to influence ISPs. As seen from the experiences of Teleindustrien and the RettighedsAlliancen, these court procedures are generally uncomplicated and do not last more than a couple of months.

When the procedure starts, the court assesses the infringement alleged by the rightholder, and the people or entities responsible for the conflictive website are informed by RettighedsAlliancen about the court process and invited to be involved.

If the court resolves in favour of the rightholder, RettighedsAlliancen sends the court ruling by email to Teleindustrien and provides a list indicating the particular websites/domains that ought to be blocked. In the event the rightholder has not been represented by RettighedsAlliancen during the court procedure, it is not RettighedsAlliancen but the rightholder who has to communicate the court order to Teleindustrien<sup>419</sup>.

Afterwards, both the court ruling and the list of websites/domains to be blocked are distributed by email from Teleindustrien to all of its members together with a request to block the infringing websites as soon as possible but within a maximum term of seven working days from reception of the information by Teleindustrien<sup>420</sup>.

Once the website is blocked, the Code of Conduct establishes that a communication from SWC will be displayed in order to redirect consumers to legal alternatives. This communication will be further detailed in Section 3.2.3 ('Redirection to legal content through SWC') and in Section 7 ('Education').

After the Code of Conduct launched, stakeholders observed that once a blocking injunction is implemented by ISPs, the infringing content sometimes appears again on the internet but with a different website address or domain. To combat this, in 2015 they decided to amend the Code of Conduct to entitle Teleindustrien members to also block these new websites on the basis of the previous court ruling that had already ordered the original website blocking<sup>421</sup>. As soon as the RettighedsAlliancen or the rightholder are aware of a situation, the RettighedsAlliancen sends the information regarding the new website to Teleindustrien who distributes it among its members so they can block the conflictive websites. The term established in the Code of Conduct to perform the new blockings is two working days<sup>422</sup>.

Finally, the Code of Conduct envisages the indemnification of ISPs by the RettighedsAlliancen, in the event that 'the blocking of further homepages leads to legal actions and if, for example, claims for damages are brought forward against ISP(s). The RettighedsAlliancen simultaneously undertakes the management of the entire case and the communication in relation thereof'<sup>423</sup>. For this, according to the information obtained through interviews with Teleindustrien, the RettighedsAlliancen drafts claims more broadly to get a court order to block any website related to the original website blocked so in the event a website owner changes its address to continue providing unauthorised content, the ISPs are also allowed to block new addresses. In practice, ISPs act in this manner if the RettighedsAlliancen guarantees, by providing them with all the documentation and evidence that they have obtained, in order to demonstrate that the website with the new address is related to the one originally blocked by a court order.

---

<sup>419</sup> According to point 4 of the Annex exempt from Official Publication of the Code of Conduct, the Rightholder shall send the blocking ruling to Teleindustrien per email to the following email address [post@teleindu.dk](mailto:post@teleindu.dk).

<sup>420</sup> In this sense, the Code of Conduct establishes in lines 32 to 36 that 'Teleindustrien will then immediately thereafter pass the ruling on to the Teleindustrien members who a.s.a.p. and at the latest within seven working days up-on receipt of the request from the RettighedsAlliancen, will execute the DNS blocking of the homepage addresses/domains that have been previously identified and processed by the RettighedsAlliancen'.

<sup>421</sup> In this regard, according to point 6 of the Annex exempt from Official Publication of the Code of Conduct: 'In case RettighedsAlliancen in the following finds out that the concerned homepage changes its DNS/IP address so that the specific DNS blocking by the court itself is no longer efficient, and in the case that the owner of a right undertakes judicially/economically to demonstrate that homepages with a changed DNS/IP address are subject to the illegal activities that the ruling on blocking concerns, the RettighedsAlliancen will thereafter send information on this new address to Teleindustrien'.

<sup>422</sup> Point 7 of the Annex exempt from Official Publication of the Code of Conduct.

<sup>423</sup> Code of Conduct, lines 50 to 53 first page, and 1 and 2 second page.



The final decision of the court can be appealed by the website owner to the High Court, as it functions as a civil and criminal appellate court. According to the information received during the course of this study, since the implementation of the Code of Conduct, there have been some appeals to the High Court, such as the Pirate Bay case or the UK furniture company Voga Ltd case.

### 3.2.1. Technical methods of infringement

The Code of Conduct makes reference to the infringement of 'rights on the internet' of any rightholders' intellectual property rights. Pursuant to the interviews undertaken with the different stakeholders, they specified that blocking takes place in the context of intellectual property rights, mainly copyright.

There is no reference to the diverse methods that the website owner can use in order to make protected content available. Those methods are not a matter of importance for the Code of Conduct as long as the unauthorised content is duly made available.

Nevertheless, although the internet is in constant evolution, it is considered that the major methods used by website owners in order to place infringing content on the internet are the following<sup>424</sup>:

- Peer-to-peer<sup>425</sup>: a method used to share and download files. Through this method, content is distributed from one user to another without the need of stable hosts. The benefit for intellectual property rightholders is that this method allows them to obtain the identity of the owner of these websites through their IP address.

Linking: this method concerns all websites which, through 'hyperlinks', redirect internet users to other websites. We should point out the Opinion of the Advocate General in Case C-160/15<sup>426</sup>, which considers that hyperlinks posted on a website that directs to works protected by copyright freely accessible on another website, cannot be classified as an 'act of communication'<sup>427</sup>.

- Streaming: an alternative to downloading. When streaming takes place, it is very hard to identify the users because the IP address is shared only with the website that offers the link and the hosting provider.

### 3.2.2. DNS blocking

In this Section some technical considerations regarding website blockings will be examined and more details in relation to the measures envisaged by the Code of Conduct relevant to the DNS provided:

- Website blockings

Technically there are different ways of implementing website blocking: DNS, IP (Internet Protocol) and URL (Uniform Resource Locator). According to literary sources, between these three forms of blocking there are differences regarding their technical implementation, effectiveness and associated costs<sup>428</sup>:

- DNS blocking: the DNS permits the translations of a domain name into the pertinent IP address. An ISP can block a DNS by making minor configuration amendments to the DNS server. Therefore, the costs of this kind of blocking are very low<sup>429</sup>.

<sup>424</sup> Martin Husberg, 2015, 'Blocking injunctions requisites. The balancing of rights and other aspects of blocking injunctions towards intermediaries'. Graduate Thesis, Master of Laws program, Faculty of Law, Lund University, pages 21 to 22.

<sup>425</sup> Google & PRS for Music commissioned report about the 'six business models for copyright infringement', 2012.  
<http://www.prsformusic.com/aboutus/policyandresearch/researchandeconomics/Documents/TheSixBusinessModelsofCopyrightInfringement.pdf>.

<sup>426</sup> At the time of conducting the study the case is pending before the CJEU.

<sup>427</sup> <http://curia.europa.eu/juris/document/document.jsf?text=&docid=175626&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=827402>

<sup>428</sup> Lukas Feiler, 2012, TTLF Working Papers No.13, 'Website Blocking Injunctions under EU and U.S. Copyright Law – Slow Death of the Global Internet or Emergence of the Rule of National Copyright Law?', Stanford-Vienna Transatlantic Technology Law Forum, pages 6 to 11.

- IP blocking: on the internet there is an IP source address and an IP destination address to route data packets. In order to block a data packet sent to a destination address, all traffic to the IP address can be shut down. In this kind of blocking the costs are also very low. In order to avoid an IP block, users only have to change to a server that is connected to a different ISP. Nevertheless, IP blocking carries with it a significant risk of over-blocking<sup>430</sup>.
- URL blockings: in this case the ISP has to control the IP address details (source and destination) as well as the content of the IP packets. URL blocking is very expensive and ISPs would have to change and invest in an alteration of their infrastructure and restructure their networks for implementing this blocking. At the same time it would be very difficult for users to circumvent URL blocking. It is a very precise method and it has the lowest risk of over-blocking.
- DNS website blocking addressed by the Code of Conduct

The Code of Conduct only applies to DNS blocking. Due to the easy manner in which this blocking can be effected, there was a common understanding, when drafting the Code of Conduct, to only consider it applicable to DNS blockings.

Analysing the position given by courts about blocking methods:

- In the case *IFPI Denmark v Tele2 A/S* decided by the Copenhagen City Court, IFPI as the plaintiff filed a report about the different possibilities of website blocking. In relation to DNS blocking, IFPI explained that it was easier for ISPs to block the access of their customers to a certain website and alternatively redirect them to another address that could warn them about the blocking of the website and its unauthorised content<sup>431</sup>. The Copenhagen City Court ordered Tele2 A/S to block the infringing websites. Although the court estimated that DNS blocking is the most common type of technique used, and carried out without noticeable costs or administrative efforts by ISPs, it issued a general injunction and left it to the ISP to decide which level of website blocking was more appropriate.
- The Maritime and Commercial Court in Copenhagen on 11 December 2014 in the *Interior Addict* case ordered the ISP to block the website expressly at DNS level<sup>432</sup>.

### 3.2.3. Redirection to legal content through SWC

As already mentioned in the previous Section 3.2. ('Procedure'), Teleindustrien members are in charge of redirecting users who attempt to connect to a blocked website to specific legal platforms, through the SWC<sup>433</sup> platform designed by Teleindustrien, the Danish Consumer Council, the Danish Ministry of Culture and the RettighedsAlliancen.

Consequently, the ISPs inform users that the website has been blocked but that they can have access to a legal platform if they click on the link suggested. The particular wording was decided by Teleindustrien and the rightholders, however, ISPs still have some discretion as regards the exact wording they wish to use in order to communicate such a blocking.

<sup>429</sup> BASCAP report 'Roles and responsibilities of intermediaries: fighting counterfeiting and piracy in the supply chain', page 65.

<sup>430</sup> Lukas Feiler, 2012, TTLF Working Papers No. 13, 'Website Blocking Injunctions under EU and U.S. Copyright Law – Slow Death of the Global Internet or Emergence of the Rule of National Copyright Law?', Stanford-Vienna Transatlantic Technology Law Forum, page 9: 'A single IP address is often used to host multiple websites, and indeed often hundreds of them. Thus, when IP blocking is used, the blocking of one website will often automatically result in the blocking of numerous other (typically unrelated) websites. Significantly, it is typically not possible for anyone other than the hosting provider hosting the websites in question to determine with certainty whether an IP address is used by multiple websites, let alone how many of them. The extent of over-blocking can therefore typically not be determined with certainty from an ex ante perspective'.

<sup>431</sup> Copenhagen City Court, 25 October 2006, case No. FI-15124/2006, *IFPI Denmark* Ruling: 'Many ISPs, including TDC, gives DNS access to their customers, and it will here be possible to stop translation of certain addresses to IP addresses, alternatively to pass on the inquiry to an address other than the address intended, and here give the user a warning that he is out on illegal business'.

<sup>432</sup> Maritime and Commercial Court in Copenhagen, 11 December 2014, *Interior Addict* Ruling.

<sup>433</sup> The SWC will be further analysed in Section 7 of this Chapter 5 ('Education').

An example of this display is detailed below:

The message has been translated by RettighedsAlliancen as: 'You have tried to access a website which contains content that violates the artist's copyright. For that reason the internet service provider has been ordered to block access to the website. We encourage you to use some of the many options for legal sharing of movies, music, etc. See an overview on [www.sharewithcare.dk](http://www.sharewithcare.dk)'<sup>434</sup>.



### 3.2.4. Penalties and sanctions

If a signatory of the Code of Conduct does not apply the court order by blocking the conflictive website, no penalty could be applied as it is a voluntary collaboration practice. Despite this, if the non-complying ISP is the one ordered to block the website by the court, this ISP is disobeying a court order and therefore Danish law will impose a sanction, most probably a pecuniary fine. Moreover, the Code of Conduct includes an exemption of responsibility for Teleindustrien in case one of its members does not comply with its directions<sup>435</sup>.

### 3.2.5. The role of the website owners

The Code of Conduct does not involve any form of participation of website owners during the application of the Code of Conduct or the implementation of website blocking.

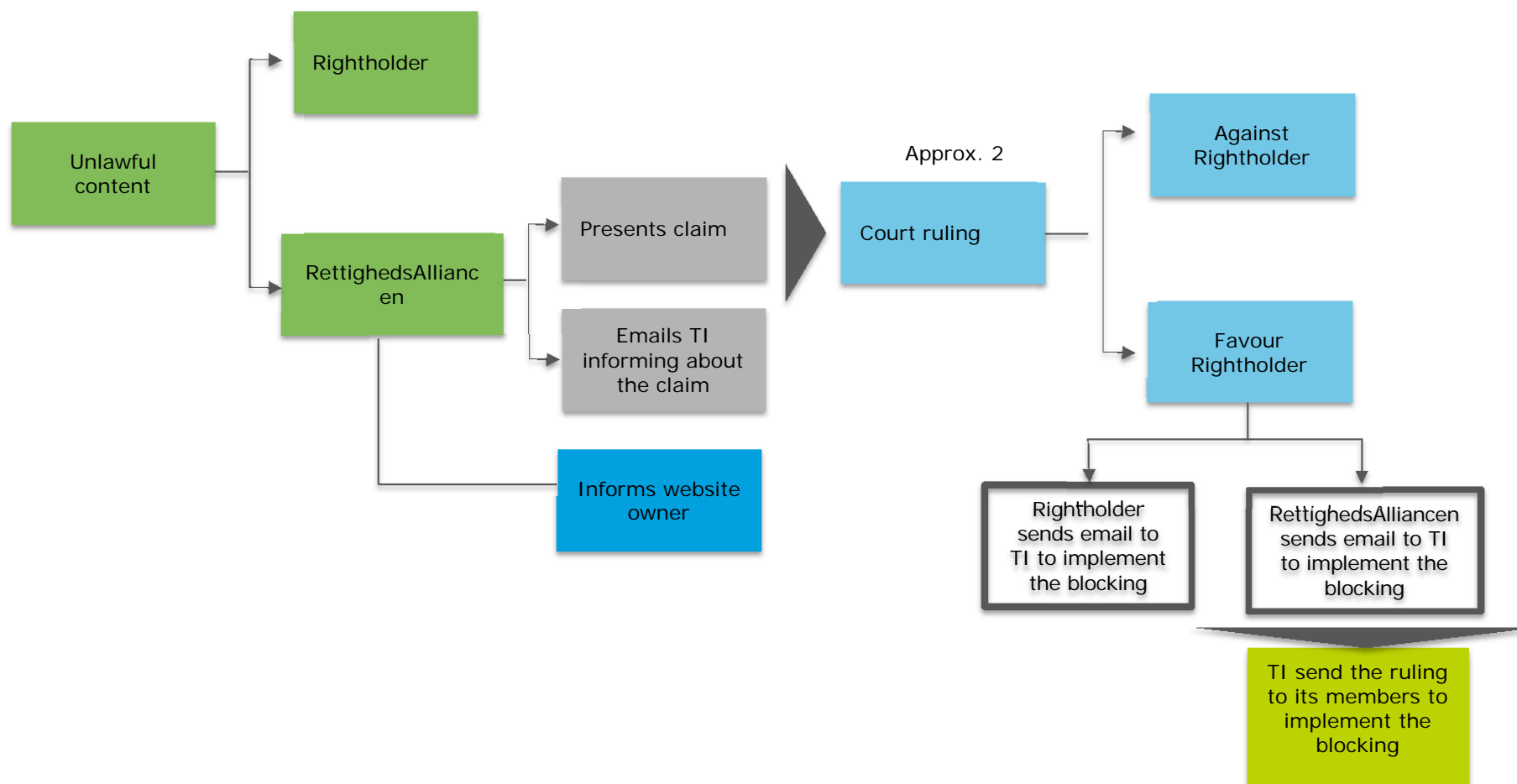
Despite this, according to the information provided by the main stakeholders interviewed, no blocking of a website in Denmark has been executed without involving their website owners, who have always been invited to intervene by RettighedsAlliancen, whenever it is possible to identify the owner.

The fact that neither Teleindustrien nor the ISPs are obliged to inform website owners about the relevant lawsuit does not mean that the website owners are not allowed to intervene. The main stakeholders interviewed explained that a website owner always has the opportunity either to intercede at the trial or request a revision of the resolution ordering the blocking.

<sup>434</sup> Maria Fredenslund, 23 January 2015, Kluwer Copyright Blog, 'Danish Court issues website blocking ruling concerning the illegal distribution of replica products'. <http://kluwercopyrightblog.com/2015/01/23/danish-court-issues-website-blocking-ruling-concerning-the-illegal-distribution-of-replica-products/>.

<sup>435</sup> Paragraphs 8 and 9, page 2 of the Code of Conduct: '[Teleindustrien] cannot be held responsible for the extent of compliance with the agreement on behalf of its members'.

### 3.3 Code of Conduct flowchart



## 4. Coexistence of the measures set forth under the VCP with the European Union, Danish legal frameworks and related case law

This Section of Chapter 5 (*'Coexistence of the measures set forth under the VCP with European Union and Danish legal frameworks and related case law'*) summarises the European Union and Danish legal framework and related case law that may have an impact on the practical application of the Code of Conduct's provisions.

The considerations included in this Section are based upon the following hierarchy of legal sources:

- Charter of Fundamental Rights (Section 4.1.1. of this Chapter 5 ('Charter of Fundamental Rights')).
- European Convention on Human Rights (Section 4.1.2. of this Chapter 5 ('European Convention on Fundamental Rights')).
- European Union Directives (Section 4.2. of this Chapter 5 ('European Union Directives')).
- Constitutional Prerequisites and Fundamental Rights in Denmark (Section 4.3 of this Chapter 5 ('Constitutional prerequisites and fundamental rights in Denmark')).
- Danish Regulations (Section 4.4 of this Chapter 5 ('Danish Regulations')).

### 4.1. Fundamental rights

#### 4.1.1. Charter of Fundamental Rights

Certain measures envisaged by the Code of Conduct may have an impact in the following fundamental rights provided by the Charter of Fundamental Rights<sup>436</sup>:

- Article 8: 'Protection of personal data'. This right generally serves to protect the self-determination of an individual regarding the use of personal data related to him/her.
- Article 11: 'Freedom of expression and information'. This right protects the freedom of every individual to express themselves as well as the freedom to impart and receive ideas and information without interference by public authority and regardless of frontiers.
- Article 16: 'Freedom to conduct a business'. This right includes the freedom to exercise an economic or commercial activity and the freedom of contract.
- Article 17: 'Right to property'. This right stipulates that no one is deprived of their possessions except in the public interest and in cases and under conditions provided for by law, subject to fair compensation being paid in good time for their loss. Protection of intellectual property (including literary and artistic property, as well as patent and trade mark rights and associated rights) is explicitly covered by this right.

The enforceability and acceptability of self-regulatory measures like this Code of Conduct depends, inter alia, on whether the fundamental rights of the persons concerned have been taken into consideration.

#### 4.1.2. European Convention on Human Rights

Certain measures envisaged by the Code of Conduct may have an impact in the following fundamental rights provided by the European Convention on Human Rights<sup>437</sup>:

- Article 8: 'Right to respect for private and family life'. This right protects respect for one's private life and states that it cannot be interfered with by a public authority unless it is required by law and in the benefit of society.

---

<sup>436</sup> See complete wording in Annex 5 of this Chapter 5.

<sup>437</sup> See complete wording in Annex 5 of this Chapter 5.

- Article 10: 'Freedom of expression'. This right states that freedom of expression must be protected and safeguarded. This right includes freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.
- Article 13: 'Right to an effective remedy'. This right ensures the application of effective remedies by national authorities when the rights or freedoms of the citizens are violated.

Considering this, a fair balance between the interests of the parties concerned in this VCP is needed.

## 4.2. European Union Directives and Regulations

Certain measures envisaged by the Code of Conduct may have an impact on the following provisions of the European Union Directives and Regulations<sup>438</sup>:

- Recital 59 of the InfoSoc Directive. This Recital recognises that rightholders should have the possibility to request an injunction against an ISP that carries a third party's infringement of intellectual property rights in a network. Moreover, it considers that in many cases ISPs are the most suitable party to end these infringing activities. The conditions and modalities relating to such injunctions are left to the national law of the Member States.
- Article 2 of the InfoSoc Directive. This Article determines the rightholders that benefit from a right of reproduction in relation to their works and, therefore, have the exclusive right to authorise or prohibit direct or indirect, temporary or permanent reproduction of their works by any means and in any form.
- Article 3 of the InfoSoc Directive. This Article determines the right of the rightholder to communicate the works to the public and to make them available to the public.
- Article 5(1)(a) of the InfoSoc Directive. This Article determines that temporary acts of reproduction of copyrighted content carried out by ISPs, which form an essential part of a technological process and take place in the context of a transmission in a network, are considered technical copies.
- Article 8(3) of the InfoSoc Directive. This Article establishes a legal basis for website blocking as it compels Member States to ensure that rightholders are able to apply for an injunction against ISPs whose services are used by a third party to infringe a copyright or related right.
- Recital 22 of the Enforcement Directive. It remarks on the importance of establishing provisional measures with the aim of immediately terminating the infringements without waiting for a court decision.
- Article 2 of the Enforcement Directive. This Article determines that the provisions of the E-Commerce Directive relating to 'safe-harbors' are independent to the application of injunctions based on the Enforcement Directive dispositions.
- Article 3 of the Enforcement Directive. This Article envisages that the measures and remedies aimed at ensuring the enforcement of the intellectual property rights are (i) fair, (ii) equitable, (iii) not unnecessarily complicated or costly, or entail unreasonable time-limits or unwarranted delays, (iv) effective, (v) proportionate, (vi) dissuasive, and (vii) applied in such a manner as to avoid the creation of barriers to legitimate trade and to provide for safeguards against their abuse.
- Article 11 of the Enforcement Directive. This Article is related to the application of injunctions and extends the legal basis for website blocking, established under Article 8(3) of the InfoSoc Directive to all intellectual property rights.
- Article 15(1) of the E-Commerce Directive. This Article envisages that providers of intermediary services are not subject to an obligation to monitor the information that they send or store, or to a general obligation to actively seek facts or circumstances indicating unauthorised activity.

---

<sup>438</sup> See complete wording in Annex 5 of this Chapter 5.

- Articles 3 and 4 of the Open Internet Access Regulation. These Articles establish that providers of internet access may be subject to measures to comply with national legislation (for example, related to the lawfulness of content, applications or services, or to public safety), including criminal law, requiring, for example, the blocking of specific content, applications or services.
- Article 7(f) of the Data Protection Directive. This Article permits Member States to process personal data when it is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.

The aforementioned European Union Directives have been interpreted, inter alia, in the following CJEU cases<sup>439</sup>:

- Promusicae CJEU Ruling

This Ruling establishes that the protection of intellectual property rights is not of a higher order than other fundamental rights, meaning that the protection of intellectual property rights does not prevail over other rights such as data protection.

- Kino.to CJEU Ruling

Amongst others, this Ruling establishes that where several fundamental rights protected by the European Union legal order are at issue, such legal order and the interpretation thereof will assure a fair balance between the various rights at stake. Namely, in its Ruling the CJEU highlights the need to strike a balance between (1) copyright and related rights, which are intellectual property and are therefore protected by Article 17(2) of the Charter of Fundamental Rights, (2) the freedom to conduct a business, which economic agents enjoy under Article 16 of the Charter of Fundamental Rights and (3) the freedom of information of internet users, whose protection is ensured by Article 11 of the Charter of Fundamental Rights<sup>440</sup>.

### 4.3. Constitutional prerequisites and fundamental rights in Denmark

Certain measures envisaged by the Code of Conduct may have an impact on the following fundamental rights set forth by the Danish Constitution of 5 June 1953 (*Danmarks Riges Grundlov*):

- Section 77 of the Danish Constitution: this Article protects the right to freedom of expression of Danish citizens and prohibits censorship and other preventative measures.

Regarding the freedom to conduct a business and the data protection right laid down in Articles 16 and 8 of the Charter of Fundamental Rights, although they are not referenced in the Danish Constitution, it is understood that they are applicable by implementing or directly applying the Enforcement Directive, the InfoSoc Directive and the E-Commerce Directive<sup>441</sup>.

### 4.4. Danish regulations

As a member of the European Union, Denmark has implemented the European directives analysed previously in this Chapter 5 into national law. Certain measures envisaged by the Code of Conduct may have an impact on the following articles of the Danish regulations:

- Article 2(1) and (2) of Danish Copyright Law, which recognises and regulates the right of reproduction regarding the rightholder's works or creations, as well as the right to make them available to the public.
- Article 11(a)(1) of Danish Copyright Law, which implements the InfoSoc Directive and recognises that it is permitted to make temporary copies.

---

<sup>439</sup> See detailed description in Annex 7 of this Chapter 5.

<sup>440</sup> Kino.to CJEU Ruling paragraph 49 'The freedom to conduct a business includes, inter alia, the right for any business to be able to freely use, within the limits of its liability for its own acts, the economic, technical and financial resources available to it.'

<sup>441</sup> [http://ec.europa.eu/justice/fundamental-rights/charter/index\\_en.htm](http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm).



- Article 411 of the Danish Administration of Justice Law, which entitles Danish courts to issue injunctions by prior application from both private individuals and the Danish state.
- Article 413 of the Danish Administration of Justice Law, which enables Danish courts to issue an injunction. Moreover, this Article determines that Danish courts could refuse to issue the injunction if it determines that it will cause detriment or disadvantage to the opposing party clearly disproportionate to the rightholders' interest in obtaining the injunction.
- Article 6(1) of Danish Data Protection Law, which establishes that personal data may be processed, among others, if processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party to whom the data are disclosed, and these interests are not overridden by the interests of the data subject.

The Danish regulations have been considered by Danish Courts<sup>442</sup> in the following cases:

- Decision of the Copenhagen City Court 25 October 2006, No FI-15124/2006 – IFPI Denmark Ruling

This decision ordered Tele2 A/S to stop making available the copyright protected material on the website [www.allofmp2.com](http://www.allofmp2.com), which was using the network services of Tele2 A/S for making these works available and making copies of sound recordings infringing the IFPI Denmark members intellectual property rights. Moreover, although the Copenhagen City Court estimated that DNS blocking is the most common type of technique used and could be carried out without noticeable costs or administrative effort by ISPs, it issued a general injunction and left it to the ISP to decide which level of website blocking was more appropriate.

- Decision of the Bailiff's Court of Frederiksberg 5 February 2008 — DMT2 A/S Ruling

This decision confirmed that the content available on [www.thepiratebay.org](http://www.thepiratebay.org) through the ISP DMT2 A/S was protected by copyright and made available to the public without authorisation from the corresponding rightholders. The Court held that it was necessary to issue an injunction to be implemented by DMT2 A/S in order to block the website [www.thepiratebay.org](http://www.thepiratebay.org) according to Article 11(a)(1) of Danish Copyright Law and also to the Danish Administration of Justice Law. This Decision was appealed to the High Court and afterwards to the Supreme Court. The Supreme Court issued its Ruling on 22 May 2010 in favour of the rightholders' application for blocking injunction.

- Decision of the Maritime and Commercial Court in Copenhagen 11 December 2014 — Interior Addict Ruling.

This decision held that [www.interioraddict.co.uk](http://www.interioraddict.co.uk) infringed the rightholder's right to reproduce and offer products in Denmark that were identical copies of their designs, without the latter's authorisation or licensing. The Court resolved that the rightholders were entitled to apply for an injunction against Telia Danmark whose service was being used by [www.interioraddict.co.uk](http://www.interioraddict.co.uk) to infringe their rights as established under Article 8(3) of the InfoSoc Directive. The Court provides further detail in recognising that this injunction is also covered by Article 11 of the Enforcement Directive. Also, it determined that the injunction application complied with the requirements established under the Danish Administration of Justice Law.

Therefore, the court ordered Telia Danmark to prevent their customers from accessing [www.interioraddict.co.uk](http://www.interioraddict.co.uk) and associated subpages and subdomains by performing a DNS level website blocking. This decision is remarkable not for issuing a website blocking injunction but for determining that the blocking should be carried out at DNS level.

---

<sup>442</sup> See detailed description in Annex 7 of this Chapter 5.

- Other decisions from Danish Courts:
  - The Bailiff's Court of Frederiksberg's Ruling of 15 August 2007 against Tele2 regarding the Mp3Sparks website.
  - The Bailiff's Court of Frederiksberg's Ruling of 20 February 2012 against Hi3G Denmark regarding the Grooveshark.com website.
  - The City Court of Copenhagen's Ruling of 08 October 2013 against Telia regarding the blocking of 4 websites.
  - The City Court of Frederiksberg's Ruling of 06 March 2015 against TDC regarding the blocking of 15 websites.
  - The City Court of Copenhagen's Ruling of 20 August 2015 against Hi3G regarding the blocking of 19 websites.
  - The Eastern High Court's Ruling (as 2nd instance) of 08 February 2016 against TDC (with intervention from Voga Ltd) regarding the Voga website.

#### 4.5. Analysis of the VCP in relation to the European Union and Danish legal frameworks and case law

In light of the European Union and Danish legal frameworks and related case law discussed in the preceding Sections of this Chapter 5, in the following paragraphs it will be analysed to determine if there is any inconsistency with certain fundamental rights:

- Paragraphs 27 to 36 of the Code of Conduct, which determine that website blocking has to be performed after and on the basis of a court order for a blocking injunction;
- Paragraphs 12 and 13, which determine that the Code of Conduct only applies to website blocking at DNS level;
- Paragraphs 46 to 50, which allow extensive blocking to websites already blocked but which appear on the internet with different addresses;
- Pursuant to the Promusicae CJEU Ruling the protection of intellectual property rights will not be understood as being of a higher interest than other fundamental rights.

Therefore, during the subsequent analysis the impact of the Code of Conduct on the following fundamental rights will be reviewed in detail:

- Right to the protection of personal data related to the website owners;
- Right of freedom of expression and information of the website owners and the consumers/internet users.
- Right of ISPs to conduct a business.

In addition, it is also examined as to whether certain duties established by the Code of Conduct are in line with Article 15 of the E-Commerce Directive, Articles 5(1)(a) and 8(3) of the InfoSoc Directive, and Articles 2, 3 and 11 of the Enforcement Directive as well as Article 11(a)(1) of the Danish Copyright Law and Articles 411 and 413 of the Danish Administration of Justice Law.

As previously explained in this Chapter 5, the Code of Conduct is a voluntary cooperation tool to which ISPs may adhere and which leaves them the freedom to implement corresponding measures for blocking websites that contain copyrighted works or intellectual property related rights content without the authorisation of the rightholder. Therefore, the analysis below is valid in such cases where the Code of Conduct's signatories actually implement the duties and procedures set forth by the Code of Conduct since under alternative scenarios (e.g., signatories not complying with their duties and procedures or complying only partially with them) the analysis performed as well as the conclusions reached would be distorted.

#### 4.5.1. Coexistence of the Code of Conduct with the freedom of expression and information about website owners and internet users

This Section analyses whether certain measures provided for by the Code of Conduct coexist well with the website owners' right to freedom of expression and the right to impart information about website owners and the right to receive information about internet users.

We all have the right to freely express our opinions and the right to defend ourselves whenever this freedom is limited for insubstantial reasons. The right to freedom of expression is established by Article 11 of the Charter of Fundamental Rights (Freedom of expression and information') as well as by Article 10 of the European Convention on Human Rights of 4 November 1950 ('Freedom of expression'). Also, the Danish Constitution covers this freedom in its Section 77.

We also all have the right to provide, receive or access information. The freedom to impart and receive information is established by Article 11 of the Charter of Fundamental Rights ('Freedom of expression and information') as well as in Article 10 of the European Convention on Human Rights of 4 November 1950 ('Freedom of expression'). This freedom includes, inter alia, the right to receive information without interference.

In relation to the Code of Conduct, the duty assumed by the signatory ISPs is that they can only block websites when there is a prior court order. Therefore, it is left to Danish courts to decide whether the content infringes intellectual property rights<sup>443</sup>.

Despite the aforementioned, it could be considered that there is a risk for the ISP in over-blocking legal content in complying with a court order, and therefore this could impact the website owners' freedom of expression, the right to impart information or the internet users' right to receive or access information, in the following cases:

- (a) *The court issues an injunction in generic terms (e.g., leaves the ISP to determine the best manner of website blocking).* In this case, it could happen that the injunction could turn into an intrusive tool putting at risk the website owner's freedom of expression<sup>444</sup>. On the other hand, it could happen that the ISP implements a moderate blocking in favour of the website owner's freedom of expression and their right to impart information, but consequently the ISP could be at risk of a penalty being imposed in the enforcement process if the rightholders found the blocking was not correctly implemented and their rights were still being infringed.
- (b) The website that has been the subject of a blocking order may impact on various website operators when only one of them had made infringing content available. In this case, an injunction to all of the website operators including the ones with legal content would be disproportionate<sup>445</sup> and would affect the right to freedom of expression of the website owners as well as their freedom to impart information without any interference.
- (c) Blocking of further DNS addresses by the ISP if they include the same infringing content already ordered to be blocked by a prior court order. This possibility, included in paragraphs 46 to 50 of the Code of Conduct, only applies if the RettighedsAlliancen argues that these additional DNS addresses would be covered by the prior court order<sup>446</sup>. It seems that if a previous court has declared the illegality of making the content of the conflictive website available, an extensive blocking is appropriate to further addresses containing the same infringing material<sup>447 448</sup>.

---

<sup>443</sup> Lukas Feiler, 2012, TTLF Working Papers No. 13, 'Website Blocking Injunctions under EU and U.S. Copyright Law – Slow Death of the Global Internet or Emergence of the Rule of National Copyright Law?', Stanford-Vienna Transatlantic Technology Law Forum, page 56.

<sup>444</sup> Pekka Savola, 2014, 'Proportionality of Website Blocking: Internet Connectivity Providers as Copyright Enforcers', paragraph 35, page 121 and Advocate Cruz Villalón, 26 November 2013, Opinion on the Case 314/12, UPC Telekabel Wien, EU:C:2013:781, paragraph 89.

<sup>445</sup> Lukas Feiler, 2012, TTLF Working Papers No.13, 'Website Blocking Injunctions under EU and U.S. Copyright Law – Slow Death of the Global Internet or Emergence of the Rule of National Copyright Law?', Stanford-Vienna Transatlantic Technology Law Forum, page 57.

<sup>446</sup> Code of Conduct, paragraphs 46 to 50, page 1.

<sup>447</sup> Pekka Savola, 2014, 'Proportionality of Website Blocking: Internet Connectivity Providers as Copyright Enforcers', paragraph 70, page 126.

In such cases, the Code of Conduct also envisages that in the event that the decision to block further DNS addresses leads to legal actions or claims for damages (i.e., if lawful content has been removed by this reason), the RettighedsAlliancen will indemnify the ISP<sup>449</sup>.

The internet users' freedom to receive information has been considered by the CJEU in relation to injunctions directed to website owners, among others, in the *Kino.to* CJEU Ruling.

In this case, the CJEU determined that for ordering an injunction against the ISP it is necessary to strike a balance namely between '(i) copyright and related rights, which are intellectual property and are therefore protected under Article 17(2) of the Charter, (ii) the freedom to conduct a business, which economic agents such as internet service providers enjoy under Article 16 of the Charter, and (iii) the freedom of information of internet users, whose protection is ensured by Article 11 of the Charter<sup>450</sup>.' And, in compliance with this injunction, the addressee may ensure compliance with the fundamental right of internet users to freedom of information<sup>451</sup>.

Despite the aforementioned, the impact of the Code of Conduct on the website owner's freedom of expression and its freedom to impart information is limited. The following conditions for blocking injunctions according to the Code of Conduct are considered as the main safeguards for the protection of the website owner's freedom of expression and information:

- ISPs will only proceed to block a website at DNS level if there is a court order which determines that the content is infringing intellectual property rights and therefore, orders an injunction to the ISP for blocking the website.
- ISPs will only block further DNS addresses that turn up with the same infringing content if the latter has been discussed in a court proceeding.

#### 4.5.2. Coexistence of the Code of Conduct with the ISPs freedom to conduct a business

This Section analyses whether certain measures provided for by the Code of Conduct are in line with the ISPs freedom to conduct a business.

The freedom to conduct a business is enshrined in Article 16 of the Charter of Fundamental Rights ('Freedom to conduct a business').

This freedom includes, without limitation, the right for any business to be able to freely use within the limits of its liability for its own acts the economic, technical and financial resources available to it.

The freedom to conduct a business has been considered by the CJEU in relation to injunctions directed to ISPs, among others, in the following cases:

- In *Scarlet Extended SA v. Société Belge des auteurs, compositeurs et éditeurs (SABAM)*, the CJEU considered that those injunctions that oblige ISPs to block certain traffic within their nets at their own expense restrict the ISPs fundamental right to conduct a business<sup>452</sup>.

---

<sup>448</sup> The European Digital Rights (EDRi), an association of civil and human rights organisations from across Europe, in commenting on a draft of this document, stated that 'There is no way to ensure proportionality of the second block, even if the first blocking was considered to be proportional by the court'.

<sup>449</sup> EDRi, in commenting on a draft of this document, stated that the fundamental right of internet users to access information should be considered in this context.

<sup>450</sup> *Kino.to* CJEU Ruling, paragraph 47.

<sup>451</sup> *Kino.to* CJEU Ruling, paragraph 55 '[...] when the addressee of an injunction such as that at issue in the main proceedings chooses the measures to be adopted in order to comply with that injunction, he must ensure compliance with the fundamental right of internet users to freedom of information.'

<sup>452</sup> In this case, the ISP was obliged to install at its own cost an entire system that would filter all internet traffic of its users. This was considered by the CJEU as not a fair balance with the protection of intellectual property rights and therefore, considered the injunction disproportionate and violating the ISP freedom to conduct a business. Also, because the filtering system derived by the injunction was considered as a general monitoring prohibited by Article 15 of the E-Commerce Directive.

- In *Kino.to* CJEU Ruling, the CJEU determined that the injunction ordered against the ISP was restricting its freedom to conduct a business as it 'constrains its addressee in a manner in which restricts the free use of the resources at his disposal because it obliges him to take measures which may represent a significant cost for him, have a considerable impact on the organisation of his activities or require difficult and complex technical solutions'<sup>453</sup>. Despite the aforementioned, the Court ruled that the injunction did not infringe the ISPs freedom to conduct the business such as to preclude the compliance with the injunction.

In conclusion, an injunction aimed at protecting intellectual property rights could conflict with the right of freedom to conduct a business of the ISP when the ISP is forced by a court order to implement an injunction the costs of which are very high and which is also time-consuming<sup>454</sup>, limiting the ISPs economic, technical and financial resources available.

The Code of Conduct only involves court orders that require DNS blockings. According to this, the rules in the Code of Conduct do not violate the freedom to conduct business in Denmark.

The following should be considered as safeguards of the right to freedom to conduct a business:

- ISPs will only block a website with infringing content if there is a prior court order which issues the referred injunction. In the event that the court order does not determine which kind of injunction has to perform the blocking, the Code of Conduct establishes that it will apply only to DNS level blockings.
- Website blocking at DNS level is technically more simple and economical than other types of blocking such as blocking at URL level.

Both are factors that speak against an infringement of the freedom to conduct a business of an ISP as the CJEU recently held<sup>455</sup>. For this reason, we could conclude that blocking injunctions performed as a result of the application of the Code of Conduct do not infringe the freedom to conduct a business of the ISP as they can only be performed at DNS level.

#### 4.5.3. Coexistence of the Code of Conduct with the protection of personal data

This Section analyses whether the duties established by the Code of Conduct are in line with Danish Data Protection Law and with the Data Protection Directive.

Citizens have a data privacy right that is covered under Article 8 of the Charter on Fundamental Rights. This Article indicates that the processing of personal data must be fairly executed as well as that the data subject is entitled to access their information and is able to rectify it if needed<sup>456</sup>. Data protection is further regulated at national level through the Danish Data Protection Law implementing the Data Protection Directive<sup>457</sup> which has also been complemented by the Directive on Privacy and Electronic Communications<sup>458</sup>.

In relation to the Code of Conduct, the latter does not envisage the possibility that ISPs will provide the contact details of the website owner to the rightholders. In fact, for compliance with the Code of Conduct there is no need to provide the personal details of the website owner as the main action to be taken by ISPs is to implement a

---

<sup>453</sup> *Kino.to* CJEU Ruling, paragraph 50.

<sup>454</sup> Martin Husberg, 2015, 'Blocking injunctions requisites. The balancing of rights and other aspects of blocking injunctions towards intermediaries'. Graduate Thesis, Master of Laws program, Faculty of Law, Lund University, page 27.

<sup>455</sup> *Kino.to* CJEU Ruling.

<sup>456</sup> Article 8(2) of the Charter on Fundamental Rights 'Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified'.

<sup>457</sup> Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN>.

<sup>458</sup> The Data Protection Directive is complemented by Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communication sector, OJ L 201, (Directive on privacy and electronic communications), <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=en>.

blocking injunction. Moreover, for the implementation of a website blocking it might even not be necessary for ISPs either to (i) obtain the personal data of the website owner or (ii) disclose the personal data of the website owner. Therefore, it is important to determine which information the ISP needs for complying with a blocking injunction. It depends on the type of blocking that has been ordered to implement or the ISP has decided to implement.

According to the opinion of the IT-company Contest A/S which was provided at the Copenhagen City Court decision dated on 25 October 2006 for the case IFPI Denmark Ruling, an ISP needs the following information to block a website: 'If an ISP is to block a site, the only information it needs is the name of the site or the domain to be blocked. This also applies, if blocking is at IP level, as the ISP by so-called DNS references themselves can gain access to the IP address applicable from time to time'.

Thus, in principle, data protection should not interfere with the compliance of the Code of Conduct by the ISPs.

In the event that the Code of Conduct dealt with other types of website blocking, such as blocking at IP addresses level, Article 6(1) of Danish Data Protection Law and the guidelines established by the Art. 29 WP and the Data Protection Directive would have to be taken into account.

The Art. 29 WP in its Opinion 4/2007<sup>459</sup> on the concept of personal data, has considered IP addresses as personal data in the sense of Article 2(a) of the Data Protection Directive<sup>460</sup>. Moreover, the referred Opinion especially puts as an example the cases in which rightholders request a disclosure of the IP address to an ISP for filing a claim against the owner of a website who has placed works protected by copyright or other intellectual property rights without the consent of the rightholder<sup>461</sup>.

Therefore, in the event that ISPs process IP addresses, it will comply with national and European personal data regulation. Article 6(1) of the Danish Data Protection Law and Article 7(f) of the Data Protection Directive determine that personal data processing and its disclosure to third parties is legitimate as long as such processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data is disclosed. The limit of such processing will be defined by taking into account the respect for fundamental rights and freedoms of the data subject.

In order to gauge the scope of the exception established in Article 6(1) of the Danish Data Protection Law, the Opinion of 06/2014 by the Art. 29 WP as regards the notion of legitimate interests of the data controller of Article 7 of Directive 95/46/EC (hereinafter referred to as the 'Opinion of the Data Protection Party') needs to be analysed. This Opinion has developed a number of useful factors to be considered when carrying out the balancing test: (a) assessing the controller's legitimate interest, (b) impact on the data subjects, (c) provisional balance and (d) additional safeguards applied by the controller to prevent any undue impact on the data subjects.

The 'Working document on data protection issues related to intellectual property rights' issued by the Art. 29 WP on January 2005<sup>462</sup> contains the data protection principles to be complied with by rightholders and ISPs in the exercise of their rights against individuals suspected of copyright violation. In this document, the Art. 29 WP highlights the obligation to comply with the information, purpose limitation and compatibility data protection principles when rightholders need to complete the collection of personal information of the author of a possible infringement with additional details that could be found with the help of ISPs and or in other databases, as the Whois database<sup>463</sup>. Furthermore: 'The Working Party insists on the legal restrictions applying to the re-use of

---

<sup>459</sup> Art. 29 WP in its Opinion 4/2007, on the 20 June 2007, on the concept of personal data, pages 16 and 17.

<sup>460</sup> Article 2(a) of the Data Protection Directive includes the definition of 'personal data: shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;'

<sup>461</sup> In this sense, in the Scarlet v SABAM case, the CJEU held that IP addresses of the users have to be considered as personal data 'because they allow those users to be precisely identified'.

<sup>462</sup> 'Working document on data protection issues related to intellectual property rights', 18 January 2005, WP 104.

<sup>463</sup> "(...) The content of databases, be they public or not, can only be processed and further used for a purpose compatible with the one for which they were first collected. As regards the Whois database, the Working party has already emphasised in its opinion of 13 June 2003 (Opinion 02/2003 on the application of data protection principles to the Whois directories. WP 76) that 'from the data protection viewpoint it is essential to determine in very clear terms what is the purpose of the Whois and which purpose(s) can be considered as legitimate and compatible to the original purpose. [...] This is an extremely delicate matter as the purpose of the Whois directories cannot be extended to other purposes just because they are considered desirable by some potential users of the directories'. Some purposes that could raise data



personal information. (...) On the basis of the compatibility principle as well as in compliance with the confidentiality principle included in Directives 2002/58 and 95/46, data retained by ISPs processed for specific purposes including mainly the performance of a telecommunication service cannot be transferred to third parties such as rightholders, except, in defined circumstances provided by law, to public law enforcement authorities’.

In this regard, law enforcement and legal requests can be understood as ‘legitimate interests’ as it is usually necessary to obtain the personal data of a website owner in order to detect or prevent crime or unlawful acts. The Art. 29 WP in its Opinion of 01/2008 on data protection issues related to search engines, explained that ‘Private parties may also try to obtain a court order addressing a search engine provider to hand over user data. When such requests follow valid legal procedures and result in valid legal orders, of course search engine providers will need to comply with them and supply the information if necessary’<sup>464</sup>.

In conclusion, if the Code of Conduct were to deal with other types of website blocking, such as blocking at IP address level, data protection considerations would have to be taken into account. However, in such circumstances, and based on the interpretation of the Article 6(1) of the Danish Data Protection Law and Article 7 of Directive 95/46/EC through the Art. 29 WP’s opinion, it is considered that the Court’s decision will be a sufficient safeguard for a balance of proportionality between the protection of intellectual property rights on the one hand and data protection rights on the other.

#### 4.5.4. Coexistence of the Code of Conduct with the provisions of the InfoSoc Directive, the Enforcement Directive and the E-Commerce Directive as well as with the Danish Copyright Law and the Danish Administration of Justice Law

This Section analyses whether the duties established in the Code of Conduct are in line with the InfoSoc Directive, the Enforcement Directive and the E-Commerce Directive as well as with the Danish Copyright Law and the Danish Administration of Justice Law.

##### 4.5.4.1. *Coexistence of the Code of Conduct with Articles 2, 5(1)(a), 3 of the InfoSoc Directive, Article 11 of the Enforcement Directive and Articles 2(1) and (2) and 11(a)(1) of the Danish Copyright Law as well as Articles 411, 413 and 414 of the Danish Administration of Justice Law*

Article 2 of the InfoSoc Directive recognises the reproduction right of rightholders in relation to their works or creations and therefore, they are the only ones who can ‘authorise or prohibit direct or indirect, temporary or permanent reproduction [of their works] by any means and in any form, in whole or in part’. This reproduction right does not apply to technical copies which according to Article 5(1)(a) of the InfoSoc Directive are temporary acts of reproduction, ‘transient or incidental [and] an integral and essential part of a technological process and whose sole purpose is to enable (a) the transmission in a network between third parties by an intermediary; or (b) a lawful use, of a work or other subject matter to be made, and which have no independent economic significance (...)’.

In addition to this, Article 3 of the InfoSoc Directive recognises the rightholder’s right of making their works available to the public by stating that ‘Member States shall provide authors with the exclusive right to authorise or prohibit any communication to the public of their works, by wire or wireless means, including the making their works available to the public in such a way that members of the public may access them from a place and at a time individually chosen by them’.

These provisions of the InfoSoc Directive have been implemented into Danish law by means of Article 11(a)(1) of the Danish Copyright Law which has to be interpreted jointly with Articles 2(1) and (2) of the Danish Copyright Law. Thus, when an ISP provides access to a website it is considered as a temporary copy of the copyright protected

---

protection (compatibility) issues are for example the use of the data by private sector actors in the framework of self-police activities related to alleged breaches of their rights e.g. in the digital right management field’.

<sup>464</sup> Art. 29 WP in its Opinion 172008, on 4 April 2008, on data protection issues related to search engines, pages 17 and 18.



material. There is an exception to the prohibition to make temporary copies in Article 11(a)(1) of the mentioned law when any of the following circumstances occur '(i) which are transient or incidental; ii) which are an integral and essential part of a technical process; iii) the sole purpose of which is to enable a transmission of a work in a network between third parties by an intermediary, or a lawful use of a work; and iv) which have no independent economic significance'.

In order to protect the rightholders' copyright and intellectual property rights, Article 8(3) of the InfoSoc Directive provides a solid legal basis for website blocking when compelling Member States to 'ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right', while Article 11 of the Enforcement Directive extends the scope of these injunctions to all intellectual property rights<sup>465</sup>. Further, Recital 59 of the InfoSoc Directive determines that the conditions and modalities relating to such injunctions are left to the national law of the Member States.

In compliance with the aforementioned, the Danish legal framework envisages the issuance of injunctions by Danish courts as stated in Articles 411, 413 and 414 of the Danish Administration of Justice Law. The latter contains the provisions regarding application and ordering of injunctions by a Danish court in its Part 40 — Interim Prohibitory and Mandatory Injunctions in Civil Proceedings.

Firstly, Article 411 of the Danish Administration of Justice Law entitles Danish courts to issue injunctions by prior application of both private individuals and the Danish state, regions and municipality for a temporary action, refraining others from doing or tolerating certain actions.

Moreover, according to Article 413 of the referred-to law, Danish courts will issue an injunction on those terms if the party applying for an injunction 'proves on a balance of probabilities or by clear and convincing evidence: (i) that the party holds the right for which the protection by the way of a prohibitory or mandatory injunction is sought; (ii) that the conduct of the opposing party necessitates the granting of the injunction; and (iii) that the ability of the party to enforce his right will be lost if the party has to await a full trial'.

According to the aforementioned Articles, the general rules on temporary injunctions imply the occurrence of illegal activities in the ISPs' network. Furthermore, rightholders when applying for an injunction before a court will present sufficient evidence for proving that they are the rightholders of the intellectual property rights which have been infringed, that the injunction is needed in order stop the infringement or the rightholder will be in risk or enforcing his intellectual property right.

Nevertheless, the previous Article is not absolute as according to Article 414(2) of the Danish Administration of Justice Law, it could happen that the court 'refuse(s) to grant a prohibitory or mandatory injunction if such injunction would cause the opposing party to suffer a detriment or disadvantage which is clearly disproportionate to the party's interest in obtaining the injunction'<sup>466</sup>. Thus, the fundamental right to conduct the business of the ISPs will also be observed by the Danish courts<sup>467</sup>.

In light of the aforementioned, there is no incompatibility of the Code of Conduct regarding these rules as the commitment of its signatories is to apply blocking injunctions issued by a judge. Moreover, blocking injunctions are accepted both at European level as well as in the Danish legal framework, therefore there is no interference by the Code of Conduct with the application of the InfoSoc Directive, the Enforcement Directive as well as the Danish Copyright Law and the Danish Administration of Justice Law.

#### *4.5.4.2. Coexistence of the Code of Conduct with Articles 12 to 14 and Article 15 of the E-Commerce Directive*

The application of blocking injunctions in compliance with the InfoSoc Directive and the Enforcement Directive is without prejudice to the determination of liability for the ISP or its coverage by any of the 'safe-harbors' provided by

---

<sup>465</sup> Lukas Feiler, 2012, TTLF Working Papers No. 13, 'Website Blocking Injunctions under EU and U.S. Copyright Law – Slow Death of the Global Internet or Emergence of the Rule of National Copyright Law?', Stanford-Vienna Transatlantic Technology Law Forum, page 19.

<sup>466</sup> Article 414(2) of the Danish Administration of Justice Law.

<sup>467</sup> EDRI, in commenting on a draft of this document, stated that the interests of the internet users, whose access to information is denied/blocked, should be considered as well in the proportionality assessment.

Articles 12 to 14 of the E-Commerce Directive, implemented into the Danish legal framework by the Danish Law on E-Commerce<sup>468</sup>.

Moving on to consider the application of the E-Commerce Directive and the eventual impact of the Code of Conduct, the latter does not include any mention to the implementation of monitoring techniques which are not allowed within the European framework according to Article 15 of the E-Commerce Directive. As the Code of Conduct is applicable only to DNS blocking injunctions previously ordered by a Danish Court, there is no impact on the Code of Conduct in the application of the E-Commerce Directive as DNS blocking is an injunction that does not involve the general monitoring prohibition as it only concerns traffic data but not the content of the communications<sup>469</sup>.

#### *4.5.4.3. Coexistence of the Code of Conduct with Articles 3 and 4 of the Open Internet Access Regulation*

In order to comply with the Danish legal framework, the Code of Conduct introduces the procedure to carry out DNS blocking injunctions previously ordered by a Danish Court.

These Articles recognise that national legislation, including orders by courts or public authorities vested with relevant powers, will prevail in traffic management measures (for example, related to the lawfulness of content).

### **4.6. Summary of findings relating to the coexistence of the Code of Conduct with the European Union, Danish legal frameworks and case law**

This Section summarises the findings made under Section 4 ('Coexistence of the measures set forth under the VCP with the European Union, Danish legal frameworks and related case law') regarding the coexistence of the Code of Conduct and DNS blocking with the European Union and Danish legal frameworks and case law.

#### **4.6.1. Coexistence of DNS blocking with fundamental rights**

The following conclusions have been reached concerning the coexistence of DNS blocking with certain fundamental rights:

- **Freedom of expression and information**

A blocking injunction will only be implemented by the signatories of the Code of Conduct in the event that there is a prior court order. The court performs the appropriate balancing between the protection of the intellectual property rights infringed and the freedom of expression and information.

In light of the aforementioned, the Code of Conduct does not collide with the fundamental right of freedom of expression and information.

- **Freedom to conduct a business**

- ISPs will only block a website if there is a previous court order. The judge performs a balance of proportionality between the protection of intellectual property rights and this fundamental right.
- The Code of Conduct only applies to injunctions at DNS level. Blocking at DNS level is the simplest and its cost is not of great significance.

Both reasons suggest that the Code of Conduct does not violate the freedom to conduct the business of the ISPs.

---

<sup>468</sup> Act No. 227 of 22 April 2002 on certain legal aspects of information society services, in particular electronic commerce.

<sup>469</sup> Also IP blocking could hardly involve a general monitoring prohibition as it also concerns data traffic and not the content of the communications. Nevertheless, URL blocking has a higher risk of being covered by the general monitoring prohibition as it requires an examination of all data packets to confirm if they are part of a request to a blocked URL.

- **Data protection**

The Code of Conduct does not mention the necessity for the disclosure of the personal data of the website owner either in the context of applying for an injunction or in the implementation of it by the ISPs. Moreover, the fact that the Code of Conduct only relates to injunctions at DNS level limits the risk of fundamental rights collision as this kind of blocking does not need the personal data of the website owner to be duly performed but only the domain or the name of the website.

In the event that the Code of Conduct would deal with IP addresses level blocking, data protection considerations will be applicable. In this event, the court decision will be sufficient safeguard as the court will have performed a balancing of proportionality between the protection of intellectual property rights on the one hand and this fundamental right on the other. Therefore, pursuant to Article 6 of Danish Data Protection Law, and, as long as the disclosure of the website owner's personal data has been ordered by the court, this assignment of data would be permitted.

#### 4.6.2. Coexistence of the Code of Conduct with the Infosoc Directive, the Enforcement Directive, the E-Commerce Directive and Danish Law

Website blocking is one of the measures provided for in Article 8(3) of the Infosoc Directive and Article 11 of the Enforcement Directive, which have been duly transferred to the Danish Copyright Act. In light of the above, the Danish Administration of Justice Law contains in its Article 413 and 414 the provisions regarding the conditions for issuing injunctions by a Danish judge.

As mentioned previously, the application of blocking injunctions is without prejudice to the determination of liability for the ISP or its coverage by any of the 'safe-harbour' protection, established by the E-Commerce Directive and the Danish E-Commerce Act. Finally, prohibition in relation to general monitoring established by Article 15 of the E-Commerce Directive is not applicable as injunctions do not have to deal with this kind of monitoring.

## 5. Technologies

The application of and compliance with the Code of Conduct does not imply the development of any specific technology. In fact, according to the information provided by the main stakeholders interviewed, the communication between Teleindustrien and its members as well as with RettighedsAlliancen is through emails.

Moreover, regarding blocking injunctions, as previously explained in Section 3.2.2 ('DNS Blocking'), there are three different forms of blocking websites, at DNS, IP address or URL level. All these types of blocking have different costs and require different amounts of time for their implementation. The three methods previously mentioned also existed before the launching of the Code of Conduct and none of them has implied the development of further techniques for website blocking.

In the case of the Code of Conduct, DNS blocking is the only relevant form of complying with the court injunctions. As already explained, it is the simplest way of implementing the injunctions and the costs and time for the execution are also lower than with IP and URL blocking.

## 6. Costs

According to the information provided by the stakeholders, each party assumes its own costs, therefore, there is no cost sharing for the application of the Code of Conduct. As we have been informed by Teleindustrien, ISPs already have administrative systems in place to block child pornography in collaboration with the police. As they already have technical and administrative systems to handle the blockings, the costs of DNS blocking should not be very high to handle.

## 7. Education

### 7.1. SWC: objectives and target groups

One of the eight initiatives of the Copyright Package was the mutual information effort between the telecom industry, the copyright industry and the Danish Ministry of Culture. Based on this initiative, in 2012, the Danish Ministry of Culture, Teleindustrien and the RettighedsAlliancen agreed to launch the SWC<sup>470</sup>. SWC has launched a guidebook, distributed among the interested parties, with the purpose of sharing information about digital cultural users, their behaviour and different approaches to positively influencing their conduct. The guidebook comprises the experiences and recommendations in relation to this campaign, acting as a tool to teach and to inform of positive behavioural change.

The guidebook, as well as the SWC's evaluation report, are both addressed to industries dealing with media and cultural consumer's behaviour on the internet.

Since its creation, the campaign has been focused on studying the needs and actions of internet users of cultural content as well as promoting the use of available legal alternatives on the internet. In this regard, SWC's strategy includes providing enough information and influencing consumers, through positive tone messages, to avoid any source of confrontation.

#### 7.1.1. Objectives

The overall objective of the campaign is 'to inform, influence and nudge digital user behaviour towards the use and sharing of legal services, as well as initiating a new understanding of and new collaborations between the interested parties'<sup>471</sup>. The latter can be grouped into three categories:

- One of the main objectives has been to provide adequate advice to consumers in a simple and understandable way, with the purpose of increasing their knowledge and understanding concerning available legal services on the internet.
- Moreover, SWC also studied consumer needs and behaviour in relation to the use of cultural content available on the internet. Principally, their intention has been to gather more information and details regarding young consumers and their digital world. SWC's strategy aims to implement the appropriate actions in accordance with the information obtained, influence consumer behaviour and encourage the use of available legal alternatives through guidance.
- Finally, SWC's objectives also aim to strengthen the growth of culture by limiting unauthorised cultural content on the internet. To that end, SWC has worked on the promotion and development of creative cultural sectors and legal services available on the internet.

#### 7.1.2. Target groups<sup>472</sup>

The three target groups involved in the main purpose of the SWC are: (i) young consumers, (ii) all consumers of services with creative content and (iii) project owners.

- i. In relation to young consumers, these are considered the primary target group and include both current and future consumers of all creative content available on the internet — music, films, books, games, etc.

---

<sup>470</sup> 'The name 'Share With Care' is a further development on the internet pirates' battle cry 'Sharing is Caring'.

'The Guidebook of Digital User Behaviour' SWC. [http://kum.dk/uploads/tx\\_templavoila/SWC\\_guidebook.pdf](http://kum.dk/uploads/tx_templavoila/SWC_guidebook.pdf).

<sup>471</sup> 'The Evaluation of the Information Effort. Share With Care', page 13.

[http://www.sharewithcare.dk/media/20777/SWC\\_evaluation.pdf](http://www.sharewithcare.dk/media/20777/SWC_evaluation.pdf).

<sup>472</sup> 'The Evaluation of the Information Effort. Share With Care'.

[http://www.sharewithcare.dk/media/20777/SWC\\_evaluation.pdf](http://www.sharewithcare.dk/media/20777/SWC_evaluation.pdf).

- ii. Regarding consumers of services with creative content, these are the secondary target group and the main goal has been to influence them in order to prevent the use of unauthorised content, coming up with alternative methods for its accomplishment.
- iii. Lastly, the third target group is identified as the project owners' own support base. The intention was to collaborate with them in positive terms by providing new ideas, switching their view of consumers as opponents.

### 7.1.3. SWC: behavioural design and positive tone as a joint method

SWC is based on the concept that fighting against unauthorised content on the internet through the promotion of legal alternatives can only be accomplished with the consumers' collaboration. Many parties are involved (rightsholders, ISPs, users, etc.) in the fight against online copyright and related rights' infringement. This increases the difficulty of reaching a suitable solution for all parties.

The intention behind SWC's behavioural design is to persuade consumers during the identification and acquiring of digital content through the promotion of a new kind of behaviour. On the one hand, the use of friendly language and a positive tone in all messages in the campaign is considered essential. On the other hand, the campaign consists of addressing direct messages to consumers, but at the same time, it is necessary to help them change their behaviour by indicating the usable legal alternatives available on the internet. SWC believes that it is preferable to provide a service to consumers — such as providing usable legal alternatives — instead of only a message.

The SWC campaign has applied behavioural design methods at the precise moment in which this behaviour takes place, for example, when a consumer accesses a website with unauthorised content. The manner in which behavioural design has been applied in the context of the VCP examined is by blocking the access to the site, displaying a message that informs the consumer about the unauthorised content provided on the site and also offering a list of legal alternatives that could be used by the consumer.

### 7.1.4. Campaign actions

SWC has developed a great number of different activities and actions to accomplish the main objectives of the campaign. Nevertheless, the most noteworthy action that directly affects the Code of Conduct is the display message on websites that have been blocked. This activity is based on the collaboration of SWC with Teleindustrien and is also in compliance with the provisions of the Code of Conduct. It consists of the display of a communication page referred to as 'nudge page' on a website that has been blocked by a Court decision. According to the Code of Conduct, the referred communication 'will be based on and refer to the platform which has been set up in collaboration between the Consumer's Consultative Council, the Ministry of Culture, IT and the Alliance of Rights within the framework of the joint response that goes under the name of Share With Care'<sup>473</sup>.

On this basis, the communication displayed on blocked websites complies with SWC objectives in the following manner:

- i. It promotes public knowledge by providing information to any consumer who accesses the blocked site. Additionally, it doesn't only advise a consumer about the current legal situation of the site but also provides them with the option to learn more about the blocking decision.
- ii. The communication is written in a positive tone and it is structured as a friendly message in order to strengthen consumer collaboration and stimulate behavioural change.
- iii. Following this path, the communication includes a link that redirects consumers to a list of websites containing the legal services they were searching for. This action is a promotion of the use of legal services to the detriment of the illegal services available on the net.

---

<sup>473</sup> The Code of Conduct.



## 7.2. Future actions

The experience of fighting against piracy on the internet has increased the awareness that there has to be a joint force working together in very different ways covering different areas. This is a very dynamic process and therefore everything changes very fast.

In this sense, and with regard to these initiatives, mention should be made of the strategies<sup>474</sup> ‘Follow the money’ and ‘Show the way’<sup>475</sup>:

- **‘Follow the money’**: this strategy targets economic crimes and aims to pursue those benefiting from infringing copyright, thus, ultimately making illegal monetary gains. Similarly, this could be prevented by ensuring that companies and legal services collaborate in initiatives to make profiting from copyright infringement more difficult. Payment services and advertising are the groups working under this strategy.
- **‘Show the way’**: this strategy focuses on redirecting users to legal alternatives promoting legal offers and making illegal services less accessible. This is implemented by targeting main stakeholders: ISPs, search engines, hosters and domain name registrars and the information campaign groups.

Moreover, there are currently six different groups working jointly against intellectual property infringements, each of them with the dual purposes explained above, that would be: (i) payment services, (ii) advertising, (iii) ISPs, (iv) search engines, (v) hosting providers and web domain name registrars and (vi) information campaign groups.

## 7.3. Further voluntary collaboration practices derived from the Copyright Package

Apart from the Code of Conduct, there are also other practices that have been implemented in order to enhance the use of legal content as well as fight against all unauthorised content available on the internet. Such is the case of Dialogue Forum, the aim of which is to encourage users and parties on the internet to reach voluntary agreement in order to fight against copyright infringement and ensure the enforcement of the measures taken.

At the time of the creation of Dialogue Forum, around twenty parties joined the initiative and during their work more parties have been adding to the group. It is a voluntary platform, anyone who wants to participate in their decisions can freely join. Although the Danish Ministry of Culture is not a part of any of the Workgroups, their role is to organise meetings following the main objective of enhancing the collaboration between all the interested parties.

Two practices have been implemented as a result of Dialogue Forum:

### 7.3.1. Code of Conduct to promote lawful behaviour on the internet<sup>476</sup>. Declaration of Intent

On 08 May 2015, trade associations, companies and rightholders signed a Declaration of Intent, named the Code of Conduct, to promote lawful behaviour on the internet. The latter comprises only certain intentions of its participants<sup>477</sup> but does not include actions against copyright infringing individuals or companies.

The Declaration of Intent follows Dialogue Forum’s main objective, namely, to encourage internet users to reach agreements with the aim of helping consumers use legal creative content.

---

<sup>474</sup> Information available in the Ministry of Culture of Denmark:

[http://kum.dk/fileadmin/KUM/Documents/Nyheder%20og%20Presse/Pressemeddelelser/2015/Projektbeskrivelser\\_2\\_.pdf](http://kum.dk/fileadmin/KUM/Documents/Nyheder%20og%20Presse/Pressemeddelelser/2015/Projektbeskrivelser_2_.pdf)

<sup>96</sup> A description of this strategy of working groups has been translated into English and enclosed as Annex 3 of this Chapter 5. Please note that this is not an official translation of the document.

<sup>476</sup> [http://kum.dk/fileadmin/KUM/Documents/Nyheder%20og%20Presse/Pressemeddelelser/2015/Code\\_of\\_Conduct\\_-\\_Engelsk\\_version.pdf](http://kum.dk/fileadmin/KUM/Documents/Nyheder%20og%20Presse/Pressemeddelelser/2015/Code_of_Conduct_-_Engelsk_version.pdf).

<sup>477</sup> According to the article ‘Denmark partners with tech companies to take on piracy’ dated on the 15 May 2015 from Euractiv.com, Microsoft, Koda and Mastercard are companies participating in the Declaration of intent.

The Declaration of Intent contains a total of six principles set down by the contributors in order to create a common framework to stimulate and help consumers in the use of creative legal content and meanwhile, to assist internet businesses to provide legal services on the internet.

Each participant has agreed to make a concerted effort to follow the principles set out in the Declaration of Intent in harmony with their specific function on the internet. Likewise, participants will cooperate in entering into sectorial agreements that can be directed toward encouraging consumers to use legal creative content as well as to limit, interrupt and end illegal activities on the internet by illegal businesses and their promoters.

According to the aforementioned, participants of the Declaration of Intent have agreed to 'make the internet a safe and legitimate platform for consumers and businesses'<sup>478</sup>. Furthermore, being conscious of the importance of copyright, principle 2 of the Declaration of Intent focuses on the essential role copyright has and highlights that the respect thereof will allow participants and rightholders to develop and improve their businesses. Toward this aim, participants have agreed to 'contribute to efficient processes that help to limit copyright infringement and crime associated therewith'<sup>479</sup>.

In improving the environment for the selling and use of creative products on the internet, the Declaration of Intent emphasises its participants' collaboration to 'reduce financial crime, based on copyright infringement' and 'in promoting the spread of legal products'<sup>480</sup>. The aim of the participants in the Declaration of Intent is to ensure compliance with the principles contained in the Code and to avoid contributing to criminal finances as well as, ultimately, to avoid a link between their companies and crimes related to copyright infringement.

In addition to the principles set out in the Declaration of Intent, the Danish Ministry of Culture has announced that six different Workgroups have been created in order to lay out the different voluntary measures that could help with the aims of the Copyright Package. This could also lead to the creation of new initiatives, which will reinforce the principles and objectives of the Copyright Package.

### 7.3.2. Workgroups

The second initiative from Dialogue Forum implemented currently is the creation of six Workgroups with the aim of enhancing cooperation between parties to reach voluntary agreements to fight against copyright infringement and also to promote the use of legal content on the internet. These Workgroups are formed by different parties who work on different areas on the internet.

According to the Copyright Package, Dialogue Forum and its Workgroups are voluntary and open to any party affected.

Many parties intervene at Workgroups that are also signatories of the code, such as ISPs, advertisers, trade unions, search engines, etc. Therefore, the parties who decide voluntarily to join are divided into the following groups according to the online industry they are representing: (i) payment services, (ii) advertising, (iii) ISPs, (iv) search engines, (v) hosting providers, and (vi) campaign groups.

---

<sup>478</sup> Principle 1 Code of Conduct to promote lawful behaviour on the internet, Declaration of Intent.

<sup>479</sup> Principle 5 Code of Conduct to promote lawful behaviour on the internet, Declaration of Intent.

<sup>480</sup> Principles 3 and 4 Code of Conduct to promote lawful behaviour on the internet, Declaration of Intent.

## 8. Effectiveness

According to the information provided by the main stakeholders interviewed, since the implementation of the Code of Conduct at least seventy-six<sup>481</sup> websites have been blocked by ISPs following a court ruling. The effectiveness of website blocking has been partly evidenced by a decrease in the use of blocked websites. In this sense, Denmark experienced a drop of approximately 20 % in P2P file sharing whereas it has increased by approximately 20 % at international level from 2014 to 2015<sup>482</sup>.

At the same time, the SWC has helped to inform and educate on the use of unauthorised illegal content. Moreover, the SWC website experienced between 300-600 visits per day in 2015.

Most ISPs agree with the conclusion that the Code of Conduct achieves its direct goal: to reinforce the application of a court order to block a certain website with unauthorised content, thereby saving time and money in the process of protecting intellectual property rights.

Some critics consider that the blocking of websites is useless. Their reasoning is that as technology is in constant development, legislation and its enforcement will always be one step behind technological improvements. Therefore, infringers will always find a path to avoid their websites being blocked.

In addition to the amount of blocked websites, there has also been a proliferation in the availability of copyright legal services that has resulted in a significant drop in copyright infringement, particularly in relation to music. In light of this, it is difficult to determine which are the definitive grounds that may have influenced this decrease in infringement.

Nevertheless, 'The Guide Book of Digital User Behaviour'<sup>483</sup> from SWC contains data and experiences analysed from the perspective of international behavioural research:

- **'Nudge Communication'**: as detailed in paragraph 3.2.3 ('Redirection to legal content through SWC'), ISPs inform the user that the website has been blocked but they can access a legal platform if they click on a link to a long list of legal services on sharewithcare.dk.

This strategy has resulted in many visits to the 'Share With Care' website. Pursuant to the information provided by SWC, 59 % of all visitors to sharewithcare.dk arrive via the link on the infringing website.

- **'Web nudge campaign'**<sup>484</sup>: the biggest characteristic of this campaign, launched in 2013, was that it focused on 'behavioural design' rather than apply marketing approaches. This activity was tested to ascertain whether nudge communication could help influence young people's digital behaviour. An informative message is displayed on the websites distributing unauthorised content, detailing the availability of websites with legal content. The results of the test were very positive, '(...) all of 84 % of the users chose not to continue onto the illegal website'<sup>485</sup>.

A 'Web nudge' study was performed in order to test if user behaviour can be influenced via a 'nudge' communication. They tested more than four thousand students from two Danish schools, via ten local and popular pirate websites. They inserted a semi-blocking page every time the student tried to access one of the pirate websites, which advised them they could either continue to the illegal website or redirect to a legal website. The intention was to stop the user from accessing the illegal website and check to see if they could also be redirected to a legal website. The result of the study showed that 84 % of users chose not to access the illegal website<sup>486</sup>. The campaign concluded that web nudging could guide consumers' behaviour and help protect them against accessing illegal websites.

<sup>481</sup> An overview of the websites that have been blocked under the Code of Conduct can be found here: <http://www.teleindu.dk/wp-content/uploads/2013/01/oversigt-over-blokeringer-16-marts-2016.pdf>.

<sup>482</sup> Figures are based on Mark Monitor data described it in the annual report 2015 of RettighedsAlliancen.

<sup>483</sup> [http://kum.dk/uploads/tx\\_templavoila/SWC\\_guidebook.pdf](http://kum.dk/uploads/tx_templavoila/SWC_guidebook.pdf).

<sup>484</sup> RettighedsAlliancen Report, Web Nudge Project.

<sup>485</sup> Mette Bom og Mikala Poulsen, Share with Care. 'Evaluation of the Information Effort Share with Care', 2014, p. 15.

<sup>486</sup> SWC monthly report #5.

- The Cultural Barometer is an analytic tool resulting from SWC, launched to investigate objections to the enforcement of intellectual property rights on the internet and to verify whether the ideal of freedom of information was a motivating factor behind illegal file sharing.

The studies carried out by SWC demonstrated that behavioural mechanisms are a good measure to combat against the distribution of unauthorised content on the internet.

## Chapter 5: Annex 1

### The Danish Telecommunications Industry, TI: Code of Conduct for Management of Rulings on Blockings Related to Infringements of Rights<sup>487</sup>

Revision 19 March 2015

Members of the Danish Telecommunications Industry, in the following referred to as TI, upon request from the Danish Ministry of Culture and as part of a number of measures aimed at the reduction of the extent of infringements of rights on the internet, have adopted the present 'Code of Conduct' (CoC) that pursues the simplification and efficiency of the implementation of court rulings on DNS blockings. 'Ruling' in the present CoC means rulings on blocking directed at an internet service provider (ISP) made by an authority, e.g. a court, based on specific legislation.

The Agreement includes an Annex, which in detail describes the procedure established in the CoC, but which has not been published in order to secure the purpose of the Agreement.

The purpose of the CoC is to make sure that the rulings on blockings of homepages directed at one TI member (or perhaps another ISP based in Denmark), through TI in a one-stop-shop procedure will be implemented within seven working days by TI members, among these subsidiary companies and other companies associated with these members. Each step of this one-stop-shop procedure is described in the Annex, which is exempted from publishing in order to secure the purpose of the Agreement.

The basis is thus that an owner of rights (for example, represented by the Alliance of Rights, *RettighedsAlliancen*, approaches the courts/the authorities presenting claims for the blocking of a specific homepage/domain or service with associated homepage(s), for example due to an infringement of rights. In case a court/relevant authority upholds the claim and orders the blocking of a specific TI member (or another Danish ISP), the owner of the right will further pass information of this ruling on to the Secretariat of TI. TI will pass the ruling immediately on to the TI members who, at the latest within seven working days upon receipt of the request from the Alliance of Rights, will execute the DNS blocking of the homepage addresses/domains that have been previously identified and processed by the Alliance of Rights.

The ISP themselves, therefore, do not assess whether or not the DNS addresses concerned are included in the court ruling/decision from the authorities.

The communication on the blocked homepages will be based on and refer to the platform that has been set up in collaboration between the Consumer's Consultative Council, the Ministry of Culture, TI and the Alliance of Rights within the framework of the joint response that goes under the name of 'Share With Care'.

Furthermore, the present CoC implies that when a homepage has been DNS blocked following a ruling as described in the above, TI members will block further DNS addresses if an owner of rights as represented by the Alliance of Rights can vouch that illegal acts take place on these homepages that are covered by the previous said court ruling/decision from the authorities, but for example with a changed address. Such a blocking implies that the Alliance of Rights directly and in writing in all aspects related to the blocking accepts to indemnify the internet service providers (ISPs) economically if for example, the blocking of further homepages leads to legal actions and if for example claims for damages are brought forward against the ISP(s). The Alliance of Rights simultaneously undertakes the management of the entire case and of the communication in relation thereof.

The present CoC represents a voluntary agreement between the members of TI who will endeavour to comply with the agreement. The CoC, nevertheless, does not prevent a TI member from reserving the right to separately try the case if he or she so finds it necessary for whatever special reason. TI cannot be held responsible for the extent of compliance with the agreement on behalf of its members.

The CoC has been entered into as a voluntary agreement with a view, under the present legislation, to promote the enforcement of the law; the agreement will, in the case of changed conditions, be revised or cancelled.

The Telecommunications Industry (TI).

---

<sup>487</sup> Not official translation.

## Chapter 5: Annex 2

### Copyright Package<sup>488</sup>

20 June 2012

#### *Initiatives to boost the creation of legal content on the internet.*

The internet constitutes an important sector of growth within the knowledge economy. The creative industry is nourished by the extent of its products, such as music, cinema, books, games, etc. This requires that a great quantity of attractive services and content are available on the internet for the benefit of all: for companies, institutions, consumers, etc.

Copyright is decisive for the generation of creative content. Copyright also constitutes an important condition to construct an interior digital market whose creative contents can also reach users beyond its frontiers.

Besides constituting a condition for the creation and diffusion of creative content, copyright can also constitute a barrier for those willing to make use of the content, thus, for consumers and content providers.

The challenge consists in how to ensure that respecting content copyright is simple and economically efficient. It is important to find solutions that develop and expand business digital models, ensuring that users have access to the contents they wish, and the price willing to be paid, but also guaranteeing a fair remuneration to artists for their work. The Ministry of Culture will contribute to boost the development of business models within a legal scope.

Copyright owners face a significant challenge, since it has never been so easy to illegally share music, films or other creative content through the internet. The Minister of Culture wants to support all initiatives within the sector that combat illegal copies through the internet and which try to redirect consumers' habits to legal alternatives. This is precisely why the Minister of Culture has decided to implement and encourage the following initiatives, aimed at contributing to the growth of the creation sector and the limitation of illegal copies on the internet.

#### *1. Innovation Forum*

The development and diffusion of business legal models that make music, cinema, and other creative content available to consumers, not only constitute crucial criteria to guarantee the creative industry's growth, but also an important step in the fight against piracy through the internet.

Everything suggests that the individual creative sectors face some challenges in terms of the development of new business models which, on the one hand, offer consumers the content they wish for, at the price willing to be paid, and that, on the other hand, guarantee a fair remuneration for artists.

In order to establish a dialogue between the individual creative sectors and content distributors and suppliers, the Ministry of Culture will promote an innovation forum, which could set the basis for an informal dialogue and mutual inspiration between the major stakeholders. It would focus on identifying possible barriers, and the exchange of 'good practices' for developing digital business models within the various creative fields. The objective is that the innovation forum contributes to create a basis for future transversal collaboration between all sectors and fields, with the common purpose of guaranteeing an easy and legal access for consumers to as much creative content as possible.

---

<sup>488</sup> Not official translation.

## *2. A common informative campaign directed at users*

Nowadays, a large amount of legal services exist that enjoy widespread acceptance among the Danish community. However, there are consumers who still believe that it is hard to distinguish what is legal from what is not. Fortunately, everything indicates that many Danish consumers will choose the legal alternative. As such, it is necessary to promote an informative campaign that contributes to the awareness of legal services among consumers.

For this reason, the Ministry of Culture, representatives of the television sector, copyright owners and the Government Consumption Office, will carry out a common informative campaign in 2012. This campaign will have a positive approach, which focuses on the existence of excellent legal access possibilities to a great diversity of music, cinema, books, etc.

The various sectors involved in the campaign will make their experience and diffusion platforms available. Also, the campaign will be financed by entities linked to the television sector, copyright owners and the Ministry of Culture.

## *3. Concrete information and users' dialogue*

One of the issues of the illegal usage of cultural products, such as the cinema or music, is that many users do not understand its significance and the consequences this brings.

Copyright owners highlight that a specific informative campaign and an established dialogue between the creators and internet users that enhances the awareness of the significance and consequences of illegal consumption, is essential to combat illegal copies.

Copyright owners note that they will create an operative informative group, which will take the initiative of establishing communication and dialogues with internet users for the aforementioned purpose, within websites and related forums. The purpose is to change users' attitude in relation to illegal practices on the internet, making contact (performing legal searches from the contact details that users have provided) and establishing a user dialogue with those downloading and making use of illegal content. It has also been noted that there will be special emphasis on encouraging users to make use of legal alternatives, such as legal distribution services for music, films or other content. Likewise, they state that, whenever possible, illegal content will be withdrawn from forums and cited pages.

## *4. Dialogue Forum to boost the development of new measures based upon dialogue*

Examples of the established dialogue between copyright owners and service providers the internet can be found. These are focused on guaranteeing that these owners are allowed to withdraw illegal content by themselves. This type of solution will contribute to the diffusion of legal services and diminish the scope of illegal copies.

With the purpose of contributing to this development and boosting a voluntary dialogue, the Ministry of Culture will start up a Dialogue Forum among copyright owners and online service providers that distribute creative content.

## *5. Guidelines for the blocking of illegal services on the internet*

When copyright is infringed, its owner can defend this before court. For instance, the communications operator can be accused, demanding its clients' access to an illegal service be blocked. When a court decides that the communications operator must block the access to the service, such decision only has validity for the operator in question.

Communication operators and copyright owners are in agreement regarding the procedures to be followed in relation to the blocking of access to illegal services on the internet. The parties will formalise it in written form under the Code of Conduct. The agreement stipulates that all operators respect court judgments in relation to blocking on the part of operators, of their clients' access to illegal contents. This means that copyright owners will only need to demand an operator and the remaining operators will also comply with the judgment. This process will be automatic, by which copyright owners will only need to get in contact with a company or operator, which will be in charge of communicating the judgment to the other operators.

Also, the parties have indicated that they will promote this idea to other parties involved, for example, among those linking illegal services.



## *6. Measures aimed at the diffusion of a secure usage of internet connections*

Nowadays, many Danish people have a wireless connection in their homes, via cell phones, tablets, etc. Unfortunately, some have not protected their connection in order to avoid use by third parties, for instance, downloading illegal content from the internet (pirate copy) or other criminal purposes.

It seems very easy to take security measures to prevent others from using a wireless internet connection for illegal purposes.

As part of the hardware aimed at the wireless connection to the internet is supplied without protection, the user has to implement it so that their internet connection is safe.

Telephone operator representatives have indicated that they will propose guidelines for the sectors to ensure that new devices with a wireless connection to the internet are already protected by private passwords, or with another form of encryption, so that they are impossible to use without authorisation.

## **7. Information from telephone operators that comes with the bill**

Telephone operator representatives have indicated that the sector will take measures to allow operators to send information to their clients alongside their bills, which details the importance of protecting their connection to the internet against illicit use and the significance of using legal providers of creative content.

The sector will set the details in collaboration with the Ministry of Culture throughout autumn 2012.

## *8. Evaluation of other current initiatives, and, where appropriate, future ones*

As for the measures aimed at combating illegal copies on the internet, diverse alternatives have already been implemented, such as those detailed in the Committee on Copyright on the Internet's report of April 2011.

One of the measures tried to establish an informative campaign specifically addressed towards consumers who infringe copyright. The Committee on Copyright on the Internet proposed a possible model in its report, referred to as the 'model letter'. This model specified that telephone operators, on behalf of copyright owners, send informative letters to their clients when their connection can be related to any internet copyright infringement.

As yet the Ministry of Culture has not implemented a model letter for Denmark. Instead, it prefers to wait and see the results from the rest of the measures that are also fighting against illegal copies on the internet.

The Ministry of Culture will evaluate the evolution of creative content on the internet on an annual basis. The availability of legal content providers will be assessed to value the necessity of undertaking initiatives such as a specific informative campaign, or other measures that could contribute to the defence of copyright on the internet.

## Chapter 5: Annex 3

### Project description<sup>489</sup>

#### Project 1 — ‘Follow the money’

The strategy ‘Follow the money’ focuses on economic crimes and intends to pursue those who ultimately make money by infringing copyright, interrupting the money flow that reaches its services. This can be accomplished, among others, by ensuring that services, companies and legal products collaborate in initiatives aimed at making it difficult to profit from economic crimes related to copyright infringement, arising from illegal services. It covers a wide range of measures, such as access blocking, advertising, payment services, information, etc.

##### *Advertising purchase and sale*

The distribution of advertisements usually takes place through companies that facilitate the purchase, sale and exchange of advertising, or directly from an online platform of advertising selling.

##### *Companies selling advertising space and advertising exchange*

Companies subscribing to this Code will take reasonable measures aimed at preventing support to criminal services and products based on copyright infringement, in relation to the selling of advertising space.

As far as possible, companies will aim to include conditions that can contribute to restricting the money flow towards illegal services in their contracts.

Inasmuch as companies are devoted to the sale of advertising space, reasonable measures will be taken, intended to prevent criminal services being acquired through their platforms.

This can be achieved by implementing processes, manual or automated, that prevent the sale of advertising aimed at websites of criminal services and guarantee that these are not announced on the websites of the companies concerned.

The Danish Association of Mass Media (Danske Medier), the Commercial sections (Handel) and Information Technology (ITEK) of the Confederation of Danish Industry (DI), rightholders Alliance (RettighedsAlliancen), Microsoft and Google, will draft a Code of Conduct of the companies that sell advertising space, on the basis of the preceding description of the issue. The Workgroups can include companies, organisations, etc. that do not take part in the Dialogue Forum. The group participants will complete their work before the end of 2015.

##### *Advertising purchasers*

Advertising purchasers and copyright owners will collaborate to prevent copyright infringement on the internet.

This can be attained by, among others, making the covered advertising purchasers under this Code, implement, in their commercial and technical systems, processes which ensure that the purchase of advertising space complies with the legislation in force, and that advertising purchasers ensure that their commercial activity solely takes place in collaboration with those following the Code of Conduct for the sale of advertising.

The association Kreativitet & Kommunikation of consultancy firms from the advertising creation sector, the Commercial sections (Handel), and Information Technology (ITEK), of the Confederation of Danish Industry (DI), Omnicom Media Group and rightholders Alliance (RettighedsAlliancen), will draft a Code of Conduct of the companies that sell advertising space, on the basis of the preceding description of the issue. The Workgroup will tailor a scheme of the current processes with the aim of analysing the best way to implement measures that respect the procedures and technical solutions currently in place for advertising purchase. The Workgroup can include companies, organisations, etc., that do not take part in the Dialogue Forum. The Workgroup will consider,

---

<sup>489</sup> Not official translation.

among others, the possibility of expanding cooperation to also include services and websites for which there is no established decision concerning their legality, but in which one might speak of a 'manifestly illegal service/website' from the previous defined criteria. The group participants will complete their work before the end of 2015.

#### *Payment services, etc.*

There will be a Workgroup of agents involved in payment services and copyright, that will tailor a scheme of the possibilities that the payment services rely on to block the flow of money towards illegal services with creative content. From this scheme, the group will study the necessity and possibility of taking additional measures. The Workgroup can include companies, organisations, etc., that do not take part in the Dialogue Forum. The group participants will complete their work before the end of 2015.

#### *Hosting providers and web domains*

Hosting providers and web domains offer storage space in the server or in domain names to companies and people. These services can contribute to limit the access to illegal websites taking reasonable measures devoted to eliminating illegal services within their server, or stop offering their services to illegal providers. The activities described do not affect the obligations deriving from the E-Commerce Directive with regards to the deletion of illegal content.

One.Com, Larsen Data, BFIH, DIFO and the rightholders Alliance (RettighedsAlliancen) will elaborate a Code of Conduct for servers of web storage and domain providers on the basis of the preceding description of the issue. The Workgroup will tailor a scheme of the current processes to study the best way to implement measures that respect the procedures and technical solutions currently in place within the web storage services and assignment of domain. The Workgroup can include companies, organisations, etc., that do not take part in the Dialogue Forum. The group participants will complete their work before the end of 2015.

### Project 2 — 'Show the way'

The 'Show the way' strategy focuses on the measures that vary within users' conduct, directing them to a more legally respectful conduct. It is about increasing the visibility of legal offers and hiding illegal ones. 'Show the way' must guarantee that legal services promote a legal offer. Presenting legal pages to the user and encouraging their use should constitute the general rule and not the exception. Therefore, what should be worked upon is mainly the availability and visibility of legal services, as well as the elimination and concealment of links, references, recommendations and popularity ratings related to illegal services. These activities are part of broad and varied efforts to make the internet a market with enhanced legality for users and companies. This will be carried out in the following way:

#### *Internet providers*

In the Code of Conduct, signed by the telecommunications industry in September 2014, Danish internet providers committed to block websites, with the fact that authorities require the DNS blocking of an illegal website. Besides this commitment, telecommunications industry members agreed that in the blocked websites, a text pops up that guides users, in a positive manner, towards legal services. The Telecommunications Industry, the Information Technology section (ITEK) of the Confederation of Danish Industry (DI) and the rightholders Alliance (RettighedsAlliancen) will discuss, from the results, the possibility of developing the commitments contained in the Code of Conduct. The group participants will complete their work before the end of 2015.

## *Search engines*

The search results have an influence on the pace in which the user finds the product or service he is looking for. As a result of the search, it can occur that the user is directed to illegal services, or services that offer illegal products. Microsoft, Google, TIC industry and rightholders Alliance (RettighedsAlliancen), will tailor a scheme of the current processes to study the best way to implement the measures that respect the procedures and technical solutions in place within search engines. The Workgroup will include companies, organisations, etc., that do not take part in the Dialogue Forum. The group participants will complete their work before the end of 2015.

## *Activities that affect consumer behaviour*

The discussions and presentations that have taken place at the Dialogue Forum meetings have demonstrated that there is a need to provide visibility in legal services. An important aspect of the work directed at giving visibility to legal services is that the information given regarding a service's illegal character be accompanied by user guidance to the place where the legal product can be obtained.

The experience acquired in relation to the 'Share With Care' initiative shows that it is possible to induce positive conduct through simple tools. For instance, the pilot tests have demonstrated that a message that stops a user's access to an illegal website, and which also redirects them to legal pages, has a positive effect in more than 80 percent of the users.

On the basis of these debates and experiences, the rights owners, online e-market shops' certification, the Information Technology section (ITEK) of the Confederation of Danish Industry (DI), telecommunications industry, will keep promoting the conduct design and informative activities which, from the instruments offered by the network, enhance the visibility of legal products' usage, together with informative activities that make the difference between legal and illegal activities more visible. The Workgroup participants will present a plan of possible initiatives by the end of 2015.

## Chapter 5: Annex 4

### List of Teleindustrien members

Below is a list of the current members of Teleindustrien<sup>490</sup> and, therefore, signatories of the Code of Conduct:

- Bibob A/S
- Callme A/S
- CBB A/S
- COLT Telecom A/S
- ComX Holding A/S
- Dansk Beredskabskommunikation A/S
- Fullrate A/S
- Føroya Tele
- GlobalConnect A/S
- Global Crossing Pan European Crossing
- M1 A/S
- OCH A/S
- SEAS/NVE
- SE Holding A/S
- Stofa A/S
- TDC A/S
- Telenor A/S
- Telia Danmark
- Telmore A/S
- TT-Netværket
- Wao A/S
- YouSee A/S

---

<sup>490</sup> <http://www.teleindu.dk/om-ti/medlemmer-af-ti/>.

## Chapter 5 : Annex 5

### European Union legal framework

#### 1. Charter on Fundamental Rights of the European Union

- Article 8: protection of personal data.
  - '1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority.'
- Article 11: freedom of expression and information.
  - '1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. 2. The freedom and pluralism of the media shall be respected.'
- Article 16: freedom to conduct a business.
  - 'The freedom to conduct a business in accordance with Community law and national laws and practices is recognised.'
- Article 17: right to property.
  - '2. Intellectual Property shall be protected.'

#### *European Convention on Human Rights*<sup>491</sup>

- Article 8: right to respect for private and family life.
  - '1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'
- Article 10: freedom of expression.
  - '1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises. 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.'

---

<sup>491</sup> European Convention on Fundamental Rights, [https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Convention\\_ENG.pdf](https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Convention_ENG.pdf).

- Article 13: right to an effective remedy.
  - 'Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity.'

### *European Union Directives*

- Article 12 of the E-Commerce Directive: mere conduit.
  1. 'Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member information transmitted, on condition that the provider: does not initiate the transmission; does not select the receiver of the transmission; and does not select or modify the information contained in the transmission.2. The acts of transmission and of provision of access. referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the included exclusively by exchange of electronic mail or by that the information is not stored for any period longer than equivalent individual communications. is reasonably necessary for the transmission. 3. This Article shall not affect the possibility for a court or (b) administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.'
- Article 13 of the E-Commerce Directive: caching.
  1. 'Where an information society service is provided that legal systems, of requiring the service provider to terminate or consists of the transmission in a communication network of prevent an infringement, nor does it affect the possibility for information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other Article 15 recipients of the service upon their request, on condition that: (a) the provider does not modify the information; (b) the provider complies with conditions on access to the information; (c) the provider complies with rules regarding the updating of the information in a manner widely recognised and used by industry; (d) the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and the provider acts expeditiously to remove or to disable information provided by recipients of their service or obligations to communicate to the competent authorities, the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement. 2. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.'
- Article 14 of the E-Commerce Directive: hosting.
  1. 'Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that: the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the activity or information is apparent; or the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider. 3.This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for, Member States of establishing procedures governing the removal or disabling of access to information.'



- Article 15 of the E-Commerce Directive: no general obligation to monitor.
  1. 'Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.
  2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.'
- Recital 59 of the InfoSoc Directive:
  3. 'In the digital environment, in particular, the services of intermediaries may increasingly be used by third parties for infringing activities. In many cases such intermediaries are best placed to bring such infringing activities to an end. Therefore, without prejudice to any other sanctions and remedies available, rightholders should have the possibility of applying for an injunction against an intermediary who carries a third party's infringement of a protected work or other subject-matter in a network. This possibility should be available even where the acts carried out by the intermediary are exempted under Article 5. The conditions and modalities relating to such injunctions should be left to the national law of the Member States.'
- Article 2 of the InfoSoc Directive: reproduction right.
  4. 'Member States shall provide for the exclusive right to authorise or prohibit direct or indirect, temporary or permanent reproduction by any means and in any form, in whole or in part:
    - (a) for authors, of their works;
    - (b) for performers, of fixations of their performances;
    - (c) for phonogram producers, of their phonograms;
    - (d) for the producers of the first fixations of films, in respect of the original and copies of their films;
    - (e) for broadcasting organisations, of fixations of their broadcasts, whether those broadcasts are transmitted by wire or over the air, including by cable or satellite.'
- Article 3 of the InfoSoc Directive: right of communication to the public of works and right of making other subject-matter available to the public.
  1. '11. Member States shall provide authors with the exclusive right to authorise or prohibit any communication to the public of their works, by wire or wireless means, including the making their works available to the public of in such a way that members of the public may access them from a place and at a time individually chosen by them. 2. Member States shall provide for the exclusive right to authorise or prohibit the making available to the public, by wire or wireless means, in such a way that members of the public may access them from a place and at a time individually chosen by them: (a) for performers, of fixations of their performances; (b) for phonogram producers, of their phonograms; (c) for the producers of the first fixations of films, of the original and copies of their films; (d) for broadcasting organisations, of fixations of their broadcasts, whether these broadcasts are transmitted by wire or over the air, including by cable or satellite. 3. The rights referred to in paragraphs 1 and 2 shall not be exhausted by any act of communication to the public or making available to the public as set out in this Article.'

- Article 5(1) of the InfoSoc Directive: exceptions and limitations.
- 1. 'Temporary acts of reproduction referred to in Article 2, which are transient or incidental [and] an integral and essential part of a technological process and whose sole purpose is to enable: (a) a transmission in a network between third parties by an intermediary, or (b) a lawful use of a work or other subject-matter to be made, and which have no independent economic significance, shall be exempted from the reproduction right provided for in Article 2.'
- Article 8(3) of the InfoSoc Directive: sanctions and remedies.
- 2. 'Member States shall ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.'
- Recital 23 of the Enforcement Directive:
 

'Without prejudice to any other measures, procedures and remedies available, rightholders should have the possibility of applying for an injunction against an intermediary whose services are being used by a third party to infringe the rightholder's industrial property right. The conditions and procedures relating to such injunctions should be left to the national law of the Member States. As far as infringements of copyright and related rights are concerned, a comprehensive level of harmonisation is already provided for in Directive 2001/29/EC. Article 8(3) of Directive 2001/29/EC should therefore not be affected by this Directive.'
- Article 2 of the Enforcement Directive: scope.
 

'1. Without prejudice to the means which are or may be provided for in Community or national legislation, in so far as those means may be more favourable for rightholders, the measures, procedures and remedies provided for by this Directive shall apply, in accordance with Article 3, to any infringement of intellectual property rights as provided for by Community law and/or by the national law of the Member State concerned. 2. This Directive shall be without prejudice to the specific provisions on the enforcement of rights and on exceptions contained in Community legislation concerning copyright and rights related to copyright, notably those found in Directive 91/250/EEC and, in particular, Article 7 thereof or in Directive 2001/29/EC and, in particular, Articles 2 to 6 and Article 8 thereof. 3. This Directive shall not affect:

  - (a) the Community provisions governing the substantive law on intellectual property, Directive 95/46/EC, Directive 1999/93/EC or Directive 2000/31/EC, in general, and Articles 12 to 15 of Directive 2000/31/EC in particular;
  - (b) Member States' international obligations and notably the TRIPS Agreement, including those relating to criminal procedures and penalties;
  - (c) any national provisions in Member States relating to criminal procedures or penalties in respect of infringement of intellectual property rights.'
- Article 3 of the Enforcement Directive: general obligation
 

'1. Member States shall provide for the measures, procedures and remedies necessary to ensure the enforcement of the intellectual property rights covered by this Directive. Those measures, procedures and remedies shall be fair and equitable and shall not be unnecessarily complicated or costly, or entail unreasonable time-limits or unwarranted delays. 2. Those measures, procedures and remedies shall also be effective, proportionate and dissuasive and shall be applied in such a manner as to avoid the creation of barriers to legitimate trade and to provide for safeguards against their abuse.'
- Article 11 of the Enforcement Directive: injunctions
 

'This Directive does not aim to establish harmonised rules for judicial cooperation, jurisdiction, the recognition and enforcement of decisions in civil and commercial matters, or deal with applicable law.'

There are Community instruments which govern such matters in general terms and are, in principle, equally applicable to intellectual property.’

- Article 2 of the Data Protection Directive<sup>492</sup>: definitions

‘1. For the purposes of this Directive: (a ) ‘personal data’ shall mean any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified , directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological , mental , economic, cultural or social identity; (b) ‘processing of personal data’ (‘processing’) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction; (c) ‘personal data filing system’ (‘filing system’) shall mean any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis; (d) ‘controller’ shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law; (e ) ‘processor’ shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller; (f) ‘third party’ shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorised to process the data ; (g) ‘recipient’ shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients; (h) ‘the data subject’s consent’ shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.’

- Recital (12) and (13) of the Open Internet Access Regulation:

‘(12) Traffic management measures that go beyond such reasonable traffic management measures may only be applied as necessary and for as long as necessary to comply with the three justified exceptions laid down in this Regulation.

(13) First, situations may arise in which providers of internet access services are subject to Union legislative acts, or national legislation that complies with Union law (for example, related to the lawfulness of content, applications or services, or to public safety), including criminal law, requiring, for example, blocking of specific content, applications or services. In addition, situations may arise in which those providers are subject to measures that comply with Union law, implementing or applying Union legislative acts or national legislation, such as measures of general application, court orders, decisions of public authorities vested with relevant powers, or other measures ensuring compliance with such Union legislative acts or national legislation (for example, obligations to comply with court orders or orders by public authorities requiring to block unlawful content). The requirement to comply with Union law relates, inter alia, to the compliance with the requirements of the Charter of Fundamental Rights of the European Union (‘the Charter’) in relation to limitations on the exercise of fundamental rights and freedoms. As provided in Directive 2002/21/EC of the European Parliament and of the Council (1), any measures liable to restrict those fundamental rights or freedoms are only to be imposed if they are appropriate, proportionate and necessary within a democratic society, and if their implementation is subject to adequate procedural safeguards in conformity with the European Convention for the Protection of Human Rights and Fundamental Freedoms, including its provisions on effective judicial protection and due process’.

---

<sup>492</sup> Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN>.

▪ Article 3 of the Open Internet Access Regulation

11.‘1. End-users shall have the right to access and distribute information and content, use and provide applications and services, and use terminal equipment of their choice, irrespective of the end-user’s or provider’s location or the location, origin or destination of the information, content, application or service, via their internet access service. This paragraph is without prejudice to Union law, or national law that complies with Union law, related to the lawfulness of the content, applications or services. 2. Agreements between providers of internet access services and end-users on commercial and technical conditions and the characteristics of internet access services such as price, data volumes or speed, and any commercial practices conducted by providers of internet access services, shall not limit the exercise of the rights of end-users laid down in paragraph 1.3. Providers of internet access services shall treat all traffic equally, when providing internet access services, without discrimination, restriction or interference, and irrespective of the sender and receiver, the content accessed or distributed, the applications or services used or provided, or the terminal equipment used. The first subparagraph shall not prevent providers of internet access services from implementing reasonable traffic management measures. In order to be deemed to be reasonable, such measures shall be transparent, non-discriminatory and proportionate, and shall not be based on commercial considerations but on objectively different technical quality of service requirements of specific categories of traffic. Such measures shall not monitor the specific content and shall not be maintained for longer than necessary. Providers of internet access services shall not engage in traffic management measures going beyond those set out in the second subparagraph, and in particular shall not block, slow down, alter, restrict, interfere with, degrade or discriminate between specific content, applications or services, or specific categories thereof, except as necessary, and only for as long as necessary, in order to:

- a) comply with Union legislative acts, or national legislation that complies with Union law, to which the provider of internet access services is subject, or with measures that comply with Union law giving effect to such Union legislative acts or national legislation, including with orders by courts or public authorities vested with relevant powers;
- b) preserve the integrity and security of the network, of services provided via that network, and of the terminal equipment of end-users;
- c) prevent impending network congestion and mitigate the effects of exceptional or temporary network congestion, provided that equivalent categories of traffic are treated equally.

12.4. Any traffic management measure may entail processing of personal data only if such processing is necessary and proportionate to achieve the objectives set out in paragraph 3. Such processing shall be carried out in accordance with Directive 95/46/EC of the European Parliament and of the Council (10). Traffic management measures shall also comply with Directive 2002/58/EC of the European Parliament and of the Council (11). 5. Providers of electronic communications to the public, including providers of internet access services, and providers of content, applications and services shall be free to offer services other than internet access services which are optimised for specific content, applications or services, or a combination thereof, where the optimisation is necessary in order to meet requirements of the content, applications or services for a specific level of quality. Providers of electronic communications to the public, including providers of internet access services, may offer or facilitate such services only if the network capacity is sufficient to provide them in addition to any internet access services provided. Such services shall not be usable or offered as a replacement for internet access services, and shall not be to the detriment of the availability or general quality of internet access services for end-users.’

▪ Article 4 of the Open Internet Access Regulation:

13. 'Providers of internet access services shall ensure that any contract which includes internet access services specifies at least the following: a) information on how traffic management measures applied by that provider could impact on the quality of the internet access services, on the privacy of end-users and on the protection of their personal data; b) clear and comprehensible explanation as to how any volume limitation, speed and other quality of service parameters may in practice have an impact on internet access services, and in particular on the use of content, applications and services; c) a clear and comprehensible explanation of how any services referred to in Article 3(5) to which the end-user subscribes might in practice have an impact on the internet access services provided to that end-user; d) a clear and comprehensible explanation of the minimum, normally available, maximum and advertised download and upload speed of the internet access services in the case of fixed networks, or of the estimated maximum and advertised download and upload speed of the internet access services in the case of mobile networks, and how significant deviations from the respective advertised download and upload speeds could impact the exercise of the end-users' rights laid down in Article 3(1); and e) a clear and comprehensible explanation of the remedies available to the consumer in accordance with national law in the event of any continuous or regularly recurring discrepancy between the actual performance of the internet access service regarding speed or other quality of service parameters and the performance indicated in accordance with points (a) to (d). Providers of internet access services shall publish the information referred to in the first subparagraph. 2. Providers of internet access services shall put in place transparent, simple and efficient procedures to address complaints of end-users relating to the rights and obligations laid down in Article 3 and paragraph 1 of this Article 3. The requirements laid down in paragraphs 1 and 2 are in addition to those provided for in Directive 2002/22/EC and shall not prevent Member States from maintaining or introducing additional monitoring, information and transparency requirements, including those concerning the content, form and manner of the information to be published. Those requirements shall comply with this Regulation and the relevant provisions of Directives 2002/21/EC and 2002/22/EC. 4. Any significant discrepancy, continuous or regularly recurring, between the actual performance of the internet access service regarding speed or other quality of service parameters and the performance indicated by the provider of internet access services in accordance with points (a) to (d) of paragraph 1 shall, where the relevant facts are established by a monitoring mechanism certified by the national regulatory authority, be deemed to constitute non-conformity of performance for the purposes of triggering the remedies available to the consumer in accordance with national law. This paragraph shall apply only to contracts concluded or renewed from 29 November 2015.'

## Chapter 5: Annex 6

### Danish legal framework<sup>493</sup>

#### 14. Danish Constitution

- Section 77

'Any person shall be entitled to publish his thoughts in printing, in writing, and in speech, provided that he may be held answerable in a court of justice. Censorship and other preventive measures shall never again be introduced.'

#### 15. Copyright Law

- Article 2: scope of protection

'(1) Within the limitations specified in this Act copyright implies the exclusive right to control the work by reproducing it and by making it available to the public, whether in the original or in an amended form, in translation, adaptation into another literary or artistic form or into another technique. (2) Any direct or indirect, temporary or permanent reproduction, in whole or in part, by any means and in any form shall be considered as reproduction. The recording of the work on devices which can reproduce it, shall also be considered as a reproduction. (3) The work is made available to the public if (i) copies of the work are offered for sale, rental or lending or distribution to the public in some other manner; (ii) copies are exhibited in public; or (iii) the work is performed in public. (4) Public performance within the meaning of subsection (3)(iii) shall include i) communication to the public of works, by wire or wireless means, including broadcasting by radio or television and the making works available to the public in such a way that members of the public may access them from a place and at a time individually chosen by them; and ii) performance at a place of business before a large group, which would otherwise have been considered not public.'

- Article 11(a): temporary reproduction

'1) It is permitted to make temporary copies

i) which are transient or incidental;

ii) which are an integral and essential part of a technical process;

iii) the sole purpose of which is to enable a transmission of a work in a network between third parties by an intermediary, or a lawful use of a work; and

iv) which have no independent economic significance.

(2) The provision of subsection (1) shall not apply to computer programs and databases.'

#### 16. Danish E-Commerce Law

- Article 14: mere conduit

'(1) A service provider who transmits information on a communication network supplied by a recipient of the service is not liable for the information transmitted, on condition that the provider

1) does not initiate the transmission,

2) does not select the receiver of the transmission and

---

<sup>493</sup> Not official translation.

3) does not select or modify the information contained in the transmission.

(2) The acts of transmission referred to in subsection 1 also cover automatic, intermediate and transient storage of the information transmitted, in so far as this takes place for the sole purpose of carrying out the transmission, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.

(3) The provisions of subsections 1 and 2 also apply to a service provider who provides access to a communication network.'

- Article 15: caching

'A service provider who transmits information provided by a recipient of the service on a communication network is not liable for the automatic, intermediate and temporary storage of such information or for the content of such information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that the service provider:

- 1) does not modify the information
- 2) complies with conditions on access to the information
- 3) complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry
- 4) does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information and
- 5) acts expeditiously to remove or to disable access to the information he has stored upon obtaining actual knowledge of the fact that the information has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.'

- Article 16: hosting

'(1) A service provider is not liable for storage of information or for the content of the information stored, where such storage takes place at the request of a recipient of the service who has supplied the information, on condition that the service provider

- 1) does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent, or
- 2) the provider, upon obtaining such knowledge or awareness (cf. point 1), acts expeditiously to remove or to disable access to the information.

(2) Subsection 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.'

## 17. Danish Administration of Justice Law

- Article 411:

'(1) On application, the court may by way of a prohibitory or mandatory injunction under the provisions of this Part order private individuals and representatives of the Danish State, regions and municipalities in their capacity as parties to private legal relationships to temporarily do, refrain from doing or tolerate certain actions.

(2) If the purpose of an application under subsection (1) is to obtain security for the payment of a money claim, an application to this effect must be filed and heard under the provisions of Part 56 on attachment.

(3) If the purpose of an application under subsection (1) is to preserve evidence of an infringement of intellectual property rights etc., an application to this effect must be filed and heard under the provisions of Part 57a on preservation of evidence.



(4) With regard to aircraft, vessels of foreign states and cargoes belonging to foreign states, prohibitory and mandatory injunctions will be available only in accordance with the provisions of other legislation to this effect.'

▪ Article 413:

'(1) A prohibitory or mandatory injunction may be granted if the party applying for the injunction proves on a balance of probabilities or by clear and convincing evidence: 1.(i)that the party holds the right for which protection by way of a prohibitory or mandatory injunction is sought; 2.(ii)that the conduct of the opposing party necessitates the granting of the injunction; and 3.(iii)that the ability of the party to enforce his right will be lost if the party has to await a full trial.'

▪ Article 414:

'(1) No prohibitory or mandatory injunction may be granted if the general provisions of this Act on penalty and compensation and any security offered by the opposing party are deemed to provide adequate protection to the party. (2) The court may refuse to grant a prohibitory or mandatory injunction if such injunction would cause the opposing party to suffer a detriment or disadvantage which is clearly disproportionate to the party's interest in obtaining the injunction.'

## 18. Danish Data Protection Law

▪ Article 6(1):

'Personal data may be processed only if:

1. the data subject has given his explicit consent; or
2. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
3. processing is necessary for compliance with a legal obligation to which the controller is subject; or
4. processing is necessary in order to protect the vital interests of the data subject; or
5. processing is necessary for the performance of a task carried out in the public interest; or
6. processing is necessary for the performance of a task carried out in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
7. processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party to whom the data are disclosed, and these interests are not overridden by the interests of the data subject.'

## Chapter 5: Annex 7

### CJEU and Danish case law

KINO.TO CJEU RULING (27 MARCH 2014)	
Parties	<ul style="list-style-type: none"> <li>UP Telekabel Wien GmbH (hereinafter, 'UP Telekabel Wien').</li> <li>Constantin Film Verleih GmbH (hereinafter, 'Constantin Film').</li> <li>Wega Filmproduktionsgesellschaft GmbH (hereinafter, 'Wega').</li> </ul>
Facts	<ul style="list-style-type: none"> <li>UP Telekabel Wien is one of the largest ISPs in Austria and some of their customers were uploading copyrighted material into the website www.kino.to. This website provided access to a large list of films protected by copyright whose rights were held by Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft GmbH.</li> </ul>
Preliminary Ruling	<ul style="list-style-type: none"> <li>The Handelsregister Wien (Commercial Court of Vienna) ordered UP Telekabel Wien to block the access of their customers to www.kino.to by a DNS blocking of the domain and also by blocking its IP address. The Oberlandesgericht Wien (Higher Regional Court of Vienna) amended the injunction ordered by the lower court as it did not mention the specific measures the ISP had to take. Therefore, the rightholders appealed before the Oberster Gerichtshof (Supreme Court) who suspended the procedure and referred four questions to the CJEU for a preliminary ruling.</li> <li>The third question referred by the Oberster Gerichtshof is the most relevant for analysis for the present study. It was asked if the balance with fundamental rights could preclude the issuance of a blocking injunction, when the latter is a general injunction (without specifying the concrete measures that shall be taken) and when the ISP can avoid incurring coercive penalties for breach of the referred to injunction by proving that it has taken all reasonable measures.</li> </ul>
CJEU Decision	<ul style="list-style-type: none"> <li>The CJEU affirmed that a balance between fundamental rights shall be executed in order to assure the convenience of issuing a blocking injunction. In this particular case, the fundamental rights of intellectual property rights of the rightholders, the freedom to conduct a business of the ISP and the freedom of information of the users needed to be balanced.</li> <li>As regards the freedom to conduct a business, the court defined its scope and affirmed that the injunction issued at the Austrian main proceedings constrained the ISP in a way that the free use of its resources is restricted as the measures it has to take represent a significant cost for it, they have also a high impact on its activities or imply hard and complex technical solutions. Despite the aforementioned, the court concluded that the injunction does not infringe the substance of the freedom to conduct a business of the ISP.</li> <li>As regards the freedom to access of information of the internet users', the court held that the ISP, when implementing a general injunction, has to 'ensure the compliance with the fundamental right of the internet users to freedom of information'. In this sense, it recommends that the measures performed by the ISP have to be directly addressed to end the infringements but not to the access of lawful information by the users.</li> <li>As regards of the protection of intellectual property rights, it has recognised that the injunction may not completely end the infringement as it is the ISPs responsibility to implement an injunction that has 'the effect of preventing unauthorised access to the protected subject-matter or, at least, of making it difficult to achieve and to</li> </ul>

KINO.TO CJEU RULING (27 MARCH 2014)	
	seriously discouraging internet users who are using the services of the addressee of that injunction from accessing the subject-matter made available to them in breach of that fundamental right'.

PROMUSICAE CJEU RULING (29 JANUARY 2008)	
Parties	<ul style="list-style-type: none"> <li>Productores de Música de España (hereinafter, '<b>PROMUSICAE</b>').</li> <li>Telefónica de España, S.A.U. (hereinafter, '<b>TELEFONICA</b>').</li> </ul>

Facts	<ul style="list-style-type: none"> <li>PROMUSICAE is a Spanish non-profit-making organisation of producers and publishers of musical and audio-visual recordings.</li> <li>TELEFONICA is a Spanish commercial company whose activities include the provision of internet access services.</li> <li>PROMUSICAE asked for TELEFONICA to be ordered to disclose the identities and physical addresses of certain persons to whom it provided with internet access services, whose IP address and date and time of connection were known. According to PROMUSICAE, those persons used a file exchange program (peer-to-peer) and provided access in shared files of personal computers to phonograms in which the members of PROMUSICAE held the exploitation rights.</li> <li>The Spanish Judge ordered the preliminary measures requested by PROMUSICAE. TELEFONICA appealed against that order, arguing that under the Spanish Law implementing the E-Commerce Directive, communications of data required by PROMUSICAE were authorised only in a criminal investigation or for the purpose of safeguarding public security and national defence, not in civil proceedings including for preliminary measures.</li> <li>PROMUSICAE argued that the Spanish Law implementing the E-Commerce Directive must be interpreted in accordance with various provisions of the E-Commerce Directive, the InfoSoc Directive and the Enforcement Directive and with Articles 17(2) ('Right to Property') and 47 ('Right to an effective remedy and to a fair trial') of the Charter of Fundamental Rights. Such provisions do not allow a Member State to limit solely to the purposes expressly mentioned in that law the obligations to communicate the data in question.</li> </ul>
Preliminary Ruling	The national court asked essentially whether Community law, in particular the E-Commerce Directive, the InfoSoc Directive and the Enforcement Directive read also in the light of Articles 17 ('Right to Property') and 47 ('Right to an effective remedy and to a fair trial') of the Charter of Fundamental Rights, must be interpreted as requiring Member States to lay down, in order to ensure effective protection of copyright, an obligation to communicate personal data in the context of civil proceedings.
CJEU Decision	<ul style="list-style-type: none"> <li>The CJEU has established that the E-Commerce Directive, the InfoSoc Directive, the Electronic Communications Directive, the Enforcement Directive and the E-Commerce Directive do not require Member States to lay down an obligation to communicate personal data in order to ensure effective protection of copyright in the context of a civil proceeding.</li> <li>However, according to the CJEU, European law requires that, when incorporating those Directives into national laws, Member States shall take care to rely on an interpretation of them which allows a fair balance between the various fundamental</li> </ul>

PROMUSICAE CJEU RULING (29 JANUARY 2008)	
	<p>rights protected by the European legal order, namely, on the one hand the protection of personal data and, on the other the protection of property (including intellectual property) and the right to an effective remedy.</p> <ul style="list-style-type: none"> <li>▪ The mechanisms allowing those different rights and interests to be balanced are contained in the E-Commerce Directive, in that it provides for rules that determine in what circumstances and to what extent the processing of personal data is lawful and what safeguards must be provided for, and in the E-Commerce Directive, the InfoSoc Directive and the Enforcement Directive which reserve the cases in which the measures adopted to protect the rights they regulate affect the protection of personal data. Moreover, they result from the adoption by Member States of national provisions transferring those Directives and their application by national authorities.</li> <li>▪ Furthermore, when implementing those Directives, the Authorities and Courts of the Member States must not only interpret their national law in a manner consistent with those Directives but also make sure that they do not rely on an interpretation of them that would be in conflict with those fundamental rights or with the other general principles of European law, such as the principle of proportionality.</li> </ul>

IFPI DENMARK RULING (25 OCTOBER 2006) <sup>494</sup>	
Parties	<ul style="list-style-type: none"> <li>▪ IFPI Denmark</li> <li>▪ Tele2 A/S</li> </ul>
Facts	<ul style="list-style-type: none"> <li>▪ IFPI Denmark is the Danish branch of the International Federation of the Phonographic Industry (IFPI), representing the majority of the phonograms sales in Denmark that filed a claim before the Copenhagen City Court against Tele2 A/S. The latter is virtual network operator which, inter alia, provides broadband services.</li> <li>▪ The controversy in this case was that the website <a href="http://www.allofmp3.com">www.allofmp3.com</a>, which was using the network services of Tele2 A/S, was making available and making copies of sound recordings infringing the IFPI Denmark members intellectual property rights. The music available on the website was mainly from other countries like UK, the USA or Germany but also included some Danish artists. It is important to note that the music was not free to download but was a lower price than what was legally offered by the rightholders and requested to be paid by <a href="http://www.allofmp2.com">www.allofmp2.com</a>.</li> </ul>
Court Decision	<ul style="list-style-type: none"> <li>▪ The Court considered that <a href="http://www.allofmp2.com">www.allofmp2.com</a> did not have the necessary authorisation from IFPI and their rightholders to make their work available via the internet.</li> <li>▪ The Court also declared that this activity was infringing the copyright of the rightholders in accordance with Article 2 of the Danish Copyright Act and that these copies were not covered by the exception established in Article 11(a) of the same regulation due to the fact that the copies were made from a lawful source.</li> <li>▪ Moreover, the Court estimated that these activities were very likely to be continued so there was a necessity to order an injunction as the conditions established in Article 642 of the Danish Administration of Justice Act were met. The Court also declared that DNS blocking was the</li> </ul>

<sup>494</sup> <http://kluwercopyrightblog.com/files/2015/01/allofmp3-UK.pdf>.

#### IFPI DENMARK RULING (25 OCTOBER 2006)<sup>494</sup>

	<p>best manner of applying the injunction for both costs and administrative reasons.</p> <ul style="list-style-type: none"> <li>Finally, the Court ordered Tele2 A/S to stop making the copyrighted material of the website <a href="http://www.allofmp2.com">www.allofmp2.com</a> available so the exclusive copyright was held by their rightholders. Tele2 A/S was also ordered to 'take the necessary steps suitable to prevent the access of the Defendant's customers to the internet website, <a href="http://allofmp2.com">allofmp2.com</a> and related sub-pages and sub-domains'.</li> </ul>
--	--

#### SONOFON A/S RULING (26 NOVEMBER 2008)<sup>495</sup>

Parties	<ul style="list-style-type: none"> <li>IFPI Denmark</li> <li>Sonofon A/S</li> </ul>
Facts	<ul style="list-style-type: none"> <li>Sonofon A/S (who merged with DMT2 A/S) appealed to the decision of the Bailiff's Court of Frederiksberg claiming that the injunction should be reversed while IFPI and the rightholders the latter was representing defended that the injunction should be maintained.</li> <li>The ISP argued, inter alia, that the injunction was manifestly disproportionate and that the injunction should have been formulated with more clarity by the Bailiff's Court of Frederiksberg. Nevertheless, the Court of Appeals determined that ISP is 'the closest to decide which measures are best and most efficient to use in Appellant's networking' and adds that DNS blocking is 'generally sufficient effective'.</li> </ul>
Court Decision	<ul style="list-style-type: none"> <li>The Court of Appeals stated that DNS blocking as already performed by the ISP should be implemented as it does not contravene the requirement of proportionality of Article 413 of the Danish Administration of Justice Act. Therefore, the Court affirmed the resolution from the Bailiff's Court of Frederiksberg.</li> </ul>

#### TELENOR A/S RULING (27 MAY 2010)<sup>496</sup>

Parties	<ul style="list-style-type: none"> <li>IFPI Denmark</li> <li>Telenor A/S</li> </ul>
Facts	<ul style="list-style-type: none"> <li>The decision of the Bailiff's Court of Frederiksberg affirmed by the Courts of Appeal, prohibited Sonofon (who changed its name to Telenor) to make the works of the rightholders that were protected by copyright available at the website <a href="http://www.thepiratebay.org">www.thepiratebay.org</a>. This prohibition was understood as the obligation on Telenor of assuring that their users did not have access to the website by means of a blocking injunction. As already explained in the previous section, Telenor was entitled to choose the technical manner to perform the blocking and chose to block the website at DNS level.</li> <li>The key issue of the case before the Danish Supreme Court was to determine whether the injunction ordered by the Bailiff's Court of Frederiksberg and afterwards upheld by the Courts of Appeal complied with the requirements established under the Danish Administration of Justice Act. Under the referred law the conditions for</li> </ul>

<sup>495</sup> [http://hssph.net/Sonofon\\_IFPI\\_Cour\\_of\\_Appeals-E.Div26Nov2008\\_PirateBay.pdf](http://hssph.net/Sonofon_IFPI_Cour_of_Appeals-E.Div26Nov2008_PirateBay.pdf).

<sup>496</sup> [http://hssph.net/Sonofon\\_IFPI\\_DK\\_SupremeCourt\\_27May2010\\_PirateBay.pdf](http://hssph.net/Sonofon_IFPI_DK_SupremeCourt_27May2010_PirateBay.pdf).

TELENOR A/S RULING (27 MAY 2010) <sup>496</sup>	
	ordering an injunction are that, in this case, if the ISP has infringed or intends to infringe the rightholders' rights and that the injunction is a proportionate measure (i.e., that the damage generated as regards the ISP for complying with the injunction is not obviously disproportionate in relation to the rightholders interest in the injunction). In relation to the infringement by the ISP it is based on an objective standard, therefore, there is no need for the ISP to have acted intentionally or with negligence to comply with this requirement, it is only needed to infringe a right to comply with it <sup>497</sup> .
Court Decision	<ul style="list-style-type: none"> <li>▪ The Supreme Court affirmed the decision of the Courts of Appeal, and determined that the maintenance of the injunction was proportionate with the following reasoning:</li> <li>▪ 'In light of the given information regarding the costs and disadvantages associated with blocking on DNS level, in connection with the extensive violations of the copyrights administered by the Appellees and as disseminated through the website www.thepiratebay.org and to which the Appellees have a significant protection worthy interest to get terminated or at least reduced significantly, the Supreme Court concur that there is no reason to hold that the prohibition to Telenor will result in damage or inconvenience that is manifestly disproportionate to the Appellees' interest in the issued injunction, see Code of Civil Procedure § 643, paragraph 2. In addition, the Supreme Court holds that the duty to act imposed on Telenor does not exceed the limits outlined in Code of Civil Procedure § 641 paragraph 2.'</li> <li>▪ Therefore, it could be concluded that the Danish Supreme Court of Justice determined that the damages due to rightholders of the infringed copyrighted material, which was available through www.thepiratebay.org, was enough to justify the compliance with the injunction by the ISP. It was confirmed that the requirements under Danish law to issue and maintain the injunction were being fulfilled and affirmed the previous order from the Courts of Appeal.</li> <li>▪ Nevertheless there were some critics of the Supreme Court ruling, in the opinion of EDRI<sup>498</sup> this ruling only undertook a balance of proportionality of economic burdens but not with freedom of speech<sup>499</sup>.</li> </ul>

DMT2 A/S RULING (FEBRUARY 2012) <sup>500</sup>	
Parties	<ul style="list-style-type: none"> <li>▪ IFPI Denmark</li> <li>▪ DMT2 A/S</li> </ul>
Facts	<ul style="list-style-type: none"> <li>▪ In 2007 IFPI filed a claim representing the rightholders before the Bailiff's Court of Frederiksberg requesting an injunction directed to the Danish ISP DMT2 A/S to block the access to www.thepiratebay.org. They argued that the website infringed the rightholders' copyright and that DMT2 A/S was supporting the infringement by making access to the website available to consumers.</li> <li>▪ It was confirmed by the Court that the content available www.thepiratebay.org was</li> </ul>

<sup>497</sup> Søren Sandfeld Jakbosen, IRIS 2010-8:1/24, Denmark 'Danish Supreme Court Upholds Injunction to Block the Pirate Bay', <http://merlin.obs.coe.int/redirect.php?id=12604>.

<sup>498</sup> European Digital Rights' Association. <https://edri.org/>.

<sup>499</sup> <https://edri.org/edrigramnumber8-11piratebay-denmark-supreme-court/>.

<sup>500</sup> Bailiff's Court of Frederiksberg on 29 January 2008, IFPI Danmark v DMT2 A/S – FS 14324/2007. [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1093246](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1093246).

DMT2 A/S RULING (FEBRUARY 2012) <sup>500</sup>	
	<p>protected by copyright, which was administered by the rightholders who did not authorise the website to publish or make their works available. Moreover, it was also determined that the website had a certain distribution in Denmark. In this sense, the court outlined that the sending of the rightholders' works throughout the P2P system of the website constituted a violation of the rightholders' copyright as established in Article 2(1) and (2) of the Danish Copyright Act, even if the website by itself did not upload the copyrighted material.</p> <ul style="list-style-type: none"> <li>As DMT2 A/S was providing access to <a href="http://www.thepiratebay.org">www.thepiratebay.org</a> to their customers, they were sending the copyrighted protected works through their network, which was understood by the court as a temporary reproduction of copies as established in Article 11(a) of the Danish Copyright Act. Nevertheless, due to the fact that the reproduction was not done legally, as they did not have the rightholders' authorisation, the exception provided at the referred Article did not apply in this case.</li> </ul>
Court Decision	<ul style="list-style-type: none"> <li>The Court declared that (i) DMT2 A/S activity was violating the rightholders rights and (ii) the injunction was justified according to Articles 642 and 643 of the Danish Administration of Justice Act.</li> <li>Finally, the court ordered DMT2 A/S to block <a href="http://www.thepiratebay.org">www.thepiratebay.org</a> as it also determined that there was no risk of DMT2 A/S being liable to its customers or third persons by complying with the injunction.</li> </ul>

INTERIOR ADDICT RULING (11 DECEMBER 2014) <sup>501</sup>	
Parties	<ul style="list-style-type: none"> <li>Telia Danmark</li> <li>Fritz Hansen A/S</li> <li>Louis Poulsen Lighting A/S</li> <li>Carl Hansen &amp; Son Mobelfabrik A/S</li> <li>Fredericia Furniture A/S</li> <li>Erik Jorgensen Mobelfabrik A/S.</li> </ul>
Facts	<ul style="list-style-type: none"> <li>The UK based website <a href="http://www.interioraddict.co.uk">www.interioraddict.co.uk</a> was selling copied furniture and other decorative items designed by Danish designers. The plaintiffs were holders of the rights under licensing agreements and filed a claim before the Maritime and Commercial Court in Copenhagen with the aim of ordering <a href="http://www.interioraddict.co.uk">www.interioraddict.co.uk</a> to cease with their activities. Telia Danmark is a Danish ISP who provided access to their customers to the website <a href="http://www.interioraddict.co.uk">www.interioraddict.co.uk</a>.</li> <li>The website was taking advantage of the English regulation regarding industrial design protection, which is substantively shorter than in Denmark, 25 years after the first marketing of the work and 70 years after the death of the author respectively. Due to this situation, some England-based websites started selling replica products of Danish designers.</li> </ul>
Court Decision	<ul style="list-style-type: none"> <li>The Court outlined that <a href="http://www.interioraddict.co.uk">www.interioraddict.co.uk</a> infringed the rightholders right to reproduce and offer products in Denmark that were identical copies of their designs. This was obviously performed without authorisation or licensing from the</li> </ul>

<sup>501</sup> <http://kluwercopyrightblog.com/files/2015/01/IA11122014EN.pdf>.



#### INTERIOR ADDICT RULING (11 DECEMBER 2014)<sup>501</sup>

rightholders.

- In this sense, it was recognised that the rightholders were entitled to apply for an injunction against Telia Danmark whose service was being used by [www.interioraddict.co.uk](http://www.interioraddict.co.uk) to infringe their rights as established at Article 8(3) of the InfoSoc Directive. The court provided further detail in recognising that this injunction was also covered by Article 11 of the Enforcement Directive.
- Moreover, according to Danish law it ensured that the injunction complied with all the requirements established in Articles 413 and 414 of the Danish Administration of Justice Act. In this sense, it declared that as the designers did not approve the reproduction and sell therefore the conditions established in Article 413 (i) and (ii) of the Danish Administration of Justice Act were fulfilled.
- It was particularly relevant in this case that the court determined that, due to the fact [www.interioraddict.co.uk](http://www.interioraddict.co.uk) largely includes the sale of products that infringe the rightholders' rights, Telia Danmark could possibly DNS block the website. It provides further clarification in establishing that 'a block is not deemed to unfairly prevent Internet users from accessing information to which they are legally entitled, a blocking will not contravene the principle of proportionality'.
- Finally, the court orders Telia Danmark to prevent their customers from accessing [www.interioraddict.co.uk](http://www.interioraddict.co.uk) and associated subpages and subdomains by performing a DNS level website blocking. This decision is remarkable not for issuing an injunction of website blocking but also for determining that the blocking should be carried out at DNS level.

## **CHAPTER 6: IACC PAYMENT PROCESSOR INITIATIVE & PORTAL PROGRAM (ROGUEBLOCK)**



## Chapter 6: Glossary of terms

For the purposes of this Chapter 6, the following definitions apply:

- **Acquirer bank:** a financial institution that enables merchants to accept credit card payments (present in open-loop networks only).
- **Betamax ruling:** the decision issued in 1984 by the U.S. Supreme Court (464 U.S. 417 (1984)), *Sony Corp. of America v Universal City Studios, Inc.*
- **Bill of Rights:** the Bill of Rights of the United States of America<sup>502</sup>.
- **Constitution:** the Constitution of the United States of America<sup>503</sup>.
- **Counterfeit goods:** imitation, non-original physical goods manufactured without the consent of the respective rightholder, also referred to as 'trademark-infringing'.
- **Common law:** law made by judges and developed through case law by virtue of the doctrine of precedents.
- **DMCA:** the Digital Millennium Copyright Act, which was adopted in 1998.
- **Federal Trade Commission:** the bipartisan federal agency in the U.S. with the dual mission of (i) protecting consumers and (ii) promoting competition. Created by the Federal Trade Commission Act<sup>504</sup>, this five-member board regulates questionable business practices.
- **Financial Services Modernization Act:** a law signed in 1999 aimed at the partial deregulation of the financial industry. The Financial Services Modernization Act allows companies working in the financial sector to integrate their operations, invest in each other's businesses and consolidate<sup>505</sup>.
- **Global Intellectual Property Center:** the Global Intellectual Property Center established in 2007 as an affiliate of the U.S. Chamber of Commerce. It leads a worldwide effort to champion intellectual property rights<sup>506</sup>.
- **IACC:** the International AntiCounterfeiting Coalition, a non-profit organisation based in Washington, D.C., the main aim of which is to combat product counterfeiting and piracy<sup>507</sup>.
- **IFTA:** the Independent Film & Television Alliance, a non-profit organisation that represents independent production and distribution companies, sales agents, television companies and institutions engaged in film finance<sup>508</sup>.
- **INTA:** the International Trademark Association, an international non-profit association of trade mark owners and professionals that is dedicated to supporting intellectual property<sup>509</sup>.
- **IPEC:** the Intellectual Property Enforcement Coordinator, a government office operating under the U.S. Office of Management and Budget<sup>510</sup>.
- **IPR Center:** the National Intellectual Property Rights Coordinator Center, which is led by the Homeland Security Investigations arm of U.S. Immigration and Customs Enforcement.
- **ISP:** internet service providers.
- **Manila Principles:** baseline safeguards and best practices based on international human rights instruments and other international legal frameworks on intermediary liability proposed by civil society groups from around the world<sup>511</sup>.

---

<sup>502</sup> Bill of Rights of the first Congress of the United States of America in 1789.

<sup>503</sup> United States Federal Constitution of 1787.

<sup>504</sup> <https://www.ftc.gov/>

<sup>505</sup> Title 15 of the U.S. Code, Sections 6801 – 6827

<sup>506</sup> <http://www.theglobalipcenter.com/>.

<sup>507</sup> <http://www.iacc.org/>.

<sup>508</sup> <http://www.ifta-online.org/>.

<sup>509</sup> <http://www.inta.org/Pages/Home.aspx>.

<sup>510</sup> <https://www.whitehouse.gov/omb/intellectualproperty>.

<sup>511</sup> <https://www.manilaprinciples.org/>.

- **Merchant:** the entity or physical person that offers and sells products online and uses any of the Payment Processors as a payment method.
- **MPAA:** the Motion Picture Association of America<sup>512</sup>.
- **NCPC:** the National Crime Prevention Council, which works with the U.S. Department of Justice<sup>513</sup>.
- **Offer:** an online proposal for the sale of physical goods.
- **Payment processors:** credit card, payment and financial services companies and money transfer networks that facilitate online purchases of physical goods.
- **Perfect 10 ruling:** the ruling issued on 3 July 2007 by the U.S. Court of Appeals for the Ninth Circuit under case 494 F.3d 788, *Perfect 10 v Visa Int'l Service Association*.
- **Pirated content:** the non-authorised use or reproduction of content without the consent of the respective rightholder, also referred to as 'copyright-infringing'.
- **RIAA:** the Recording Industry Association of America<sup>514</sup>.
- **Rightholder:** any company owning any intellectual property rights for physical goods that are offered online for sale, based on the explanations of certain stakeholders interviewed for the purpose of this Chapter 6.
- **RogueBlock:** the IACC Payment Processor Initiative & Portal Program, later named RogueBlock<sup>515</sup>.
- **Rogue website:** a website whose primary purpose and mode of operation is obviously in violation of the U.S. intellectual property legal framework.
- **Tiffany ruling:** the ruling issued on 1 April 2010 by the U.S. Court of Appeals for the Second Circuit under case 600 F.3d 93, *Tiffany Inc. v eBay Inc.*
- **Trace message:** a purchase made by credit card (that will be declined) in order to assist card networks in identifying the merchants' accounts.
- **UDHR:** the Universal Declaration of Human Rights<sup>516</sup>.
- **Umbrella portal:** the master IACC portal, where complaints and resolutions are uploaded by the stakeholders involved in RogueBlock.
- **USPTO:** the United States Patent and Trademark Office<sup>517</sup>, the federal agency for granting U.S. patent and registering trade marks.
- **U.S.:** the United States of America.
- **U.S. Copyright Office**<sup>518</sup>: the copyright department of the Library of Congress, created in 1897. Its main functions include: participating on U.S. delegations in meetings with foreign governments or private parties; attending and participating in intergovernmental meetings and other international events; hosting copyright training for copyright officials from developing countries; domestic and international policy analysis; legislative support for Congress; litigation activities; support for the courts and executive branch agencies (including significant efforts on trade and antipiracy initiatives); and providing public information and education.
- **U.S. statutes:** the U.S. Code and related statutes.
- **U.S. Code:** the United States Code<sup>519</sup>.
- **VCR:** videocassette recorder, an electronic device for recording and playing back video images and sound on a videocassette.

<sup>512</sup> <http://www.mpaa.org/>.

<sup>513</sup> <http://www.ncpc.org/>.

<sup>514</sup> <https://www.riaa.com/>.

<sup>515</sup> <http://www.iacc.org/online-initiatives/rogueblock>.

<sup>516</sup> United Nation General Assembly Universal Declaration of Human Rights of 10 December 1948.

<sup>517</sup> <http://www.uspto.gov/>.

<sup>518</sup> <http://copyright.gov/>.

<sup>519</sup> <http://uscode.house.gov/>.

- **VCP:** 'voluntary collaboration practice' developed by industry, public bodies and/or third parties such as non-governmental organisations and then adhered to by the respective industry in addressing infringements of trade mark rights, design rights, copyright and rights related to copyright over the internet. For the purposes of this report also named RogueBlock.

## Chapter 6: Structure and content

This Chapter 6 analyses the RogueBlock in depth, assessing the following elements:

- Role of the parties involved in the implementation of this VCP and third parties.
- Analysis of the duties and procedures prescribed by this VCP.
- Coexistence of the measures established under this VCP with the U.S. legal framework.
- Role of technologies used in implementing the duties and procedures envisaged by this VCP.
- Costs assumed by the parties involved in the implementation of this VCP.
- Role of educational activities of the parties involved in the promotion of this VCP.
- Effectiveness of the measures established by this VCP.

This Chapter 6 initially involved exhaustive desk research to identify the participants and third parties involved in RogueBlock. A sample of them were then contacted and some agreed to be interviewed for the purposes of this Chapter 6, whilst others declined the invitation to participate.

The statements contained in Chapter 6 on the participants and third parties' positions regarding RogueBlock and day-to-day procedure are based on the feedback and supporting documentation provided by those stakeholders that agreed to participate in Chapter 6.

## 1. Introduction

IPEC was set up in 2009 with the objective, inter alia, of fighting against intellectual property infringement in the context of counterfeiting and piracy. Since then, IPEC's strategy has been based on encouraging the private sector to combat acts of infringement effectively and facilitating cooperation in order to reduce intellectual property infringement occurring over the internet<sup>520</sup>.

As a consequence of this strategy, a variety of voluntary practices were adopted among intermediaries in the private sector aimed at curbing the sale of counterfeit goods and reducing online piracy. IPEC's Annual Report on Intellectual Property Enforcement of 2011<sup>521</sup> describes a wide range of the voluntary best practices or measures adopted as a consequence of this approach to fighting online infringement. Examples of these practices were<sup>522</sup>:

- In December 2010, as a result of the Administration's strategy to combat illegal online pharmacies, American Express, Discover, eNom, GoDaddy, Google, MasterCard, Microsoft (Bing), Network Solutions, PayPal, Visa, and Yahoo!, announced that they would form a non-profit group to combat illegal fake online 'pharmacies' selling dangerous illegal drugs over the internet.
- In June 2011, a voluntary agreement (Memorandum of Understanding)<sup>523</sup> was entered into by ISPs, music labels and movie studios under which ISPs notify subscribers, through a series of alerts, when their internet service accounts appear to have been misused for infringement on peer-to-peer networks.
- In June 2011, American Express, Discover, MasterCard, PayPal and Visa—major credit card companies and Payment Processors—reached an agreement to develop voluntary best practices concerning the withdrawal of payment services for sites selling counterfeit goods.
- In July 2011, a voluntary agreement to reduce online piracy was entered into by ISPs, RIAA, A2IM recording companies, MPAA and IFTA movie studios<sup>524</sup>.

The abovementioned agreement of June 2011, entered into by the major payment processors in order to implement voluntary collaboration practices to fight against the sale of counterfeit products, was encouraged and supported by the IPEC<sup>525</sup>. Its main aim was to establish a procedure for rightholders to inform payment processors about the sale of counterfeit goods on the internet so that they could prevent commercial transactions on infringing websites.

In addition, prior to IPEC's reinforcement, these voluntary collaboration practices were already being used by payment processors and rightholders as 'Best Practices for Payment Service Providers' in 2009<sup>526</sup>, with the encouragement of INTA, which submitted them to its board. Due to this agreement, payment processors should have a procedure to enable trade mark owners to report websites that use payment processors' networks for processing payments for the sale of counterfeit goods. Based on the interviews held with relevant stakeholders for the purpose of this Chapter 6 it can be stated that, within the procedure:

- (i) rightholders had to contact each payment processor mentioned in the offer of counterfeited goods in order to report online intellectual property infringements, which ended up as a very lengthy process, and
- (ii) rightholders had to visit multiple websites and go through various procedures to submit complaints, because each payment processor had its own complaint system.

<sup>520</sup> As specified in IPEC's first Joint Strategic Plan in 2010.

<sup>521</sup> [https://www.whitehouse.gov/sites/default/files/omb/assets/intellectualproperty/intellectualproperty\\_strategic\\_plan.pdf](https://www.whitehouse.gov/sites/default/files/omb/assets/intellectualproperty/intellectualproperty_strategic_plan.pdf)

<sup>522</sup> [https://www.iprcenter.gov/reports/ipr-center-reports/copy\\_of\\_2011-ipecc-annual-report/](https://www.iprcenter.gov/reports/ipr-center-reports/copy_of_2011-ipecc-annual-report/).

<sup>523</sup> [https://www.whitehouse.gov/sites/default/files/omb/IPEC/spotlight/ipecc\\_spotlight\\_july\\_august\\_2011.pdf](https://www.whitehouse.gov/sites/default/files/omb/IPEC/spotlight/ipecc_spotlight_july_august_2011.pdf).

<sup>524</sup> <http://www.copyrightinformation.org/wp-content/uploads/2013/02/Memorandum-of-Understanding.pdf>.

<sup>525</sup> <https://www.whitehouse.gov/blog/2011/07/07/working-together-stop-internet-piracy>.

<sup>526</sup> Testimony of Denise Yee, Visa Inc. 'Hearing on Targeting Websites Dedicated To Stealing American Intellectual property'. The United States Senate Committee on the Judiciary. Page 14. (<http://www.judiciary.senate.gov/imo/media/doc/11-2-16%20Yee%20Testimony.pdf>).

<sup>527</sup> Candice Li, External Relations Manager – Anti-Counterfeiting. 'Addressing the Sale of Counterfeits on the Internet'. INTA (2009) (<http://www.inta.org/Advocacy/Documents/INTA%20Best%20Practices%20for%20Addressing%20the%20Sale%20of%20Counterfeits%20on%20the%20Internet.pdf>).



In parallel, in 2010 and 2011, the U.S. Congress, with the same aim of fighting against intellectual property infringement, launched three legislative proposal bills: (1) Combating Online Infringement and Counterfeits Act (COICA); (2) Preventing Real Online Threats to Economic Creativity and Theft of Intellectual property Act (PIPA); and (3) Stop Online Piracy Act (SOPA). The three bills proposed were unsuccessful due to controversy in relation to the domain name system<sup>527</sup>. They did not have the support of payment processors as some of the major payment processors opposed the new legislation (e.g., Discover, Paypal and American Express)<sup>528</sup>.

During the debates in relation to the SOPA and the PIPA, the IACC launched the anti-counterfeiting program initiative<sup>529</sup> 'Payment Processor Initiative & Portal Program', which was later named RogueBlock<sup>530</sup>.

RogueBlock is a collaborative effort between the IACC and the payment industry aimed at providing a simplified procedure for reporting online merchants of counterfeit goods or pirated content directly to participating payment processors. Stakeholders interviewed for the purpose of this Chapter 6 clarified that RogueBlock not only covers intellectual property rights with regard to physical goods, but that the IACC has also instigated a number of copyright-related claims regarding digital content based on RogueBlock. As the IACC has not participated in this Chapter 6, this information could not be verified. However, for the purposes of Chapter 6 and based on stakeholder feedback, it is assumed to be correct.

As certain stakeholders interviewed in the context of this Chapter 6 pointed out, RogueBlock was a reorganised version of the best practices already adopted that made it easier for rightholders to submit complaints and payment processors to receive them.

RogueBlock is designed to help identify and take remedial action against merchants who are using payment processors' services to conduct illegal transactions in violation of the latter's existing policies and to minimise those merchants' chances of profiting from their illicit sales. The payment processors' policies prohibit merchants from using financial services for illegal transactions, which means that once merchants violated those policies, they would be subject to remedial action by the payment processors, which could include the termination of their accounts<sup>531</sup>.

To implement this VCP, the IACC developed a system to facilitate communication between all the stakeholders involved, allowing rightholders to contact all payment processors at the same time by submitting one single complaint; the system is explained in detail in subsequent Sections of this Chapter 6.

A large part of the initiative is based on the education and awareness of major acquirer banks and payment processors. Therefore, going beyond the immediate impact on the fight against the sale of counterfeit goods, rightholders involved in the VCP have begun to cooperate more closely on training other companies in the financial sector in areas related to intellectual property (i.e., due diligence in the process of bringing on board new merchants who request the provision of these companies' services) and monitoring the compliance of existing merchants with company policies.

---

<sup>527</sup> Annemarie Bridy, 'Internet Payment Blockades'. University of Idaho College of Law; Stanford University Center for Internet and Society (February 2015).

<sup>528</sup> OpenCongress, List of Supporters and Opponents for H.R. 3261, [http://www.opencongress.org/bill/hr3261-112/bill\\_positions](http://www.opencongress.org/bill/hr3261-112/bill_positions) (last visited November, 2015).

<sup>529</sup> [https://oami.europa.eu/tunnel-web/secure/webdav/guest/document\\_library/observatory/documents/Knowledge-building-events/Infringements%20of%20Intellectual%20Property%20Rights%20on%20the%20Internet\\_en.pdf](https://oami.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/Knowledge-building-events/Infringements%20of%20Intellectual%20Property%20Rights%20on%20the%20Internet_en.pdf).

<sup>530</sup> <http://www.iacc.org/online-initiatives/rogueblock>.

<sup>531</sup> Robert C. Barchiesi on behalf of the IACC. 'The Role of Voluntary Agreements in the U.S. Intellectual property System'. United States House of Representatives Committee on the Judiciary Subcommittee on Courts, Intellectual property, and the Internet. (September 2013). (<https://judiciary.house.gov/wp-content/uploads/2016/02/091813-Testimony-of-Robert-Barchiesi.pdf>)

In June 2013, the USPTO, with a view to analysing all voluntary initiatives, issued a request for comments seeking public input on voluntary initiatives to reduce online intellectual property infringement. It received 23 responses from, inter alia, IACC, Visa, MasterCard, American Express, Discover or PayPal. Most of the responses<sup>532</sup> focused on: (i) the importance of the concept of 'collaboration' given that unilateral initiatives may suffer from a lack of stakeholder cooperation, (ii) a unified and streamlined procedure with a centralised reporting system and (iii) mechanisms to reduce the options for rogue websites.

RogueBlock, over the past few years, has significantly increased the number of rightholders participating in the VCP and, to date, has led to the termination of 'over 5 000 individual counterfeiters' merchant accounts, which has impacted over 200 000 websites'<sup>533</sup>. In addition, it seems that the IACC is working on new procedures to fight against intellectual property right infringement. According to information on its website, IACC is, inter alia, developing a data-sharing program that will use participants' claims to suspend and lock down infringers' websites in addition to terminating payment services<sup>534</sup>.

---

<sup>532</sup> <http://www.uspto.gov/ip/officechiefecon/PTO-C-2013-0036.pdf>.

<sup>533</sup> Data obtained from <http://www.iacc.org/online-initiatives/rogueblock>.

<sup>534</sup> <http://www.iacc.org/online-initiatives/rogueblock>.

## 2. RogueBlock participants and third parties

RogueBlock does not specify which categories of stakeholders can participate in it. In practice, the stakeholders that assume a more active role in RogueBlock are rightholders (including rightholders' associations), the IACC and payment processors.

Public authorities such as the IPR Center, do not participate in RogueBlock itself but still have an active role in the VCP, as will be explained in detail in this Section. The IPR Center has the possibility of discontinuing the RogueBlock procedure if it considers a complaint has criminal implications.

Finally, as far as consumers are concerned, they are one of the categories of stakeholders, together with rightholders, that may benefit the most from RogueBlock as one of its main aims is to protect consumers from buying counterfeit products. However, civil society does not participate in RogueBlock.

This Section of Chapter 6 explains the specific roles regarding the VCP played by the four (4) mentioned categories of stakeholders (i.e., rightholders, the IACC and payment processors, public authorities and civil society).

### 2.1. Role of rightholders<sup>535</sup>

Rightholders participating in RogueBlock may own any type of intellectual property right in a variety of sectors (e.g., luxury; fashion; pharmaceutical; electronics; sports; consumer).

Each action within RogueBlock begins with an investigation by the rightholders of the rogue websites that are offering counterfeit goods or pirated content. Currently, the IACC only accepts complaints in the umbrella portal<sup>536</sup> regarding standalone rogue websites, not online marketplace or auction websites.

Initially, as stated by certain stakeholders interviewed for the purposes of this Chapter 6, not all rightholders were entitled to report a complaint to the umbrella portal individually, as only members of the IACC could do that. However, the IACC have recently published on its website that 'Both member and non-member rightholders are eligible to participate',<sup>537</sup>

One of the stakeholders interviewed in the context of this Chapter 6 stated that, once they suspect that a website is offering counterfeit goods, rightholders submit a complaint direct to the umbrella portal, without carrying out any formal investigation (e.g., verifying that the payment methods offered on the website work or doing a test purchase to confirm that the goods offered are counterfeited). However, if the rightholder is a member of any rightholders' association, the association carries out monitoring and preliminary investigations (i.e., a test purchase to confirm that they can buy counterfeited products).

Finally, associations of rightholders participate actively in meeting with payment processors, the IACC and other rightholders to discuss the problems arising in relation with the online sale of counterfeit goods or pirated content and possible ways of remedying the situation.

### 2.2. Role of public authorities (IPR Center)

The main objective of the IPR Center is to combat activities that constitute the theft of intellectual property rights. To achieve this objective, the IPR Center works to enforce intellectual property laws in collaboration with 23 partner agencies, including agencies from other countries, such as the Royal Canadian Mounted Police and the Mexican Revenue Service.

<sup>535</sup> The rightholders interviewed for this Chapter 6 are a sample of those involved in the VCP.

<sup>536</sup> Kristina Montanaro (IACC). 'Executive Summary October 2012. IACC Payment Processor Portal Program: First Year Statistical Review', <http://www.gacg.org/Content/Upload/MemberNewsDocs/October%202012%20Report%20to%20IPEC%20-%20FINAL.pdf> [Document available via the previous link on November 2015].

<sup>537</sup> <http://www.iacc.org/online-initiatives/rogueblock>. This information has not been confirmed by the IACC.

The IPR Center's main activity consists of investigating intellectual property infringement and dismantling criminal organisations through active inspections in order to prevent counterfeit goods from reaching the supply chain.

In relation to RogueBlock, and as stated by an agent of this public body, interviewed in the context of this Chapter 6, the IACC usually forwards the information from the complaints they receive from rightholders in the umbrella portal to the IPR Center. This is done for two main reasons:

- To verify that the complaint has no criminal implications: The IACC is not empowered to carry out criminal investigations in relation to a suspected intellectual property infringer. Therefore, they send all the information provided by rightholders to the IPR Center to verify that the infringer is not committing a criminal offence. If the IPR Center determines that the complaint has a criminal implication, the RogueBlock procedure ends at this stage. If, on the contrary, the IPR Center does not consider that a criminal offence is being carried out, the IACC will continue with the RogueBlock procedure by forwarding the complaint to the payment processors.
- To verify that the IACC is not interfering with any ongoing investigation of the IPR Center. All complaint information is forwarded to the IPR Center to check if any criminal investigation is being carried out in relation to a particular merchant. Where this is the case, the IPR Center will ask the IACC not to interfere and the RogueBlock procedure will end at this stage.

The RogueBlock procedure allows the IPR Center<sup>538</sup> to place a 24-hour hold on claims before they are submitted to payment processors.

## 2.3. Role of the IACC and payment processors

### 2.3.1. The IACC

The IACC is a non-profit organisation, the main aim of which is to protect intellectual property rights and deter counterfeiting. It is made up of not only representatives of all the disciplines related to businesses involving intellectual property, such as the entertainment, software, luxury goods and pharmaceuticals industries, but also intellectual property associations and other companies and institutions indirectly affected by product counterfeiting and piracy, such as government agencies, investigation and product security firms, law firms, etc.<sup>539</sup>. The IACC is partnered with payment processors such as Visa Europe and Visa International, American Express, PayPal and MoneyGram.

In relation to RogueBlock, the IACC plays an intermediary role since RogueBlock and the system created to share information between rightholders and payment processors—through the umbrella portal—is administered and managed by the IACC.

### 2.3.2. Payment processors<sup>540</sup>

Other intermediaries that are relevant stakeholders in RogueBlock are the payment processors. Significant sales of all kinds are made via the internet using online payment-processing services. As a consequence, both legitimate and rogue merchants selling products over the internet depend heavily on electronic payment services.

---

<sup>538</sup> Kristina Montanaro (IACC). 'Executive Summary October 2012. IACC Payment Processor Portal Program: First Year Statistical Review', <http://www.gacg.org/Content/Upload/MemberNewsDocs/October%202012%20Report%20to%20IPEC%20-%20FINAL.pdf> [Document available via this link in November 2015]. However, the IPR Center agent interviewed in the context of this Chapter 6 did not confirm this information.

<sup>539</sup> <http://www.iacc.org/membership/members>.

<sup>540</sup> The payment processors interviewed for this Chapter 6 are a sample of those involved in the VCP.

Counterfeit goods worth more than US\$ 200 billion dollars were sold in 2010 alone, and over US\$2 billion dollars' worth were sold in the U.S. during November and December of 2012. The magnitude of these numbers underscores the importance of the role that payment processors play in the context of illicit internet commerce<sup>541</sup>.

As stated by certain payment processors interviewed in the context of this Chapter 6, payment processors have actively cooperated in this VCP and are aware of the importance of their role.

Furthermore, payment processors sometimes collaborate with third parties when it comes to identifying the merchants. Credit card companies, for example, are divided into two different business models depending on their business relation with the merchant<sup>542</sup>:

- closed-loop networks;
- open-loop networks.

The main difference between these business models is the relationship between the payment processors and the merchants. In open-loop networks, payment processors have, unlike in closed-loop networks, only an indirect relationship with their merchants.

In open-loop networks, the payment processors collaborate with the acquirer bank, that is to say the institution that enables merchants to accept, for example, Visa payments. In such cases, since the payment processor does not have a direct relationship with the merchants, the acquirer bank is the party with the authority to carry out all investigations related to the submission of claims by rightholders. Therefore, acquirer banks participate in this VCP as intermediaries.

In closed-loop networks, on the other hand, payment processors have a direct contractual relationship with their clients (merchants) and acquirer banks do not participate in this VCP procedure.

## 2.4. Role of civil society

One of the main aims of RogueBlock is to protect consumers from buying counterfeit goods online. However, although certain consumer associations have been part of other industry initiatives, they were not invited to participate in the creation of this VCP and do not currently participate in it. This circumstance was highlighted by the stakeholders contacted during the drafting of this Chapter 6.

Notwithstanding this, one civil society association interviewed for the purposes of this Chapter 6 stated that it had been contacted several times by website owners whose payment services had been cut off. In cases where website owners do not have a chance to contest the removal of payment services following a complaint submitted to RogueBlock or directly to the payment processors under another procedure, the civil society association mentioned informs consumers publicly by publishing the cases on its blogs.

---

<sup>541</sup> BASCAP and the ICC. 'Roles and Responsibilities of Intermediaries: Fighting counterfeiting and piracy in the supply chain' (March 2015).

<sup>542</sup> Kristina Montanaro (IACC). 'Executive Summary October 2012. IACC Payment Processor Portal Program: First Year Statistical Review'. <http://www.gacg.org/Content/Upload/MemberNewsDocs/October%202012%20Report%20to%20IPEC%20-%20FINAL.pdf> [Document available via this link in November 2015].

### 3. Duties and procedures<sup>543</sup>

The main objectives of RogueBlock are to provide an efficient procedure that allows rightholders to report merchants who sell counterfeit products online directly to payment processors, the aim being to facilitate action against those merchants' accounts and reduce the likelihood of such merchants profiting from illicit sales.

The RogueBlock procedure is divided into three main phases. Different stakeholders participate in each of these phases. The phases are:

- **Submission of the complaint.** Rightholders may submit a complaint to the IACC through the RogueBlock umbrella portal.
- **Analysis by the IACC.** Once a rightholder submits a complaint, the IACC will analyse it to check whether it complies with all requirements. In this phase, the IPR Center intervenes if it considers that the complaint has criminal implications. If the complaint complies with all requirements, it proceeds and the payment processors are notified.
- **Investigation and Remediation.** Payment processors are notified and access the complaints through the umbrella portal. They carry out investigations in order to take a decision and apply the corresponding remedies. Payment processors submit their resolution of the complaint to the umbrella portal in order to make it accessible to rightholders and the IACC.

#### 3.1. Scope of application of the VCP

RogueBlock is not limited in its territorial scope. Stakeholders interviewed for the purposes of the Chapter 6 confirmed that rightholders may submit claims in relation to any rogue website. The website does not need to be a U.S. website; it can be a website anywhere in the world. Many of the payment processors and rightholders participating in RogueBlock are international companies.

#### 3.2. RogueBlock procedure

##### 3.2.1. Submission of complaints

RogueBlock provides a unified procedure that allows rightholders to submit complaints to the IACC, which are then forwarded to the payment processors. This is done through the medium of a master portal of the IACC, the umbrella portal<sup>544</sup>. Rightholders submit their complaints through the portal, while payment processors access the complaints via the portal and then submit their resolution of those complaints.

In accordance with the procedure detailed in the information made publicly available by the IACC, in order to submit a complaint, rightholders first have to carry out an investigation and collect evidence on those merchants who are offering counterfeit goods or pirated content. However, as stated by certain stakeholders interviewed in the context of this Chapter 6, rightholders do not always carry out such investigations themselves (see Section 2.1 of this Chapter 6). Where rightholders are members of a rightholders' association, the investigations are carried out by the association on behalf of their members. Some associations have full-time staff dedicated exclusively to monitoring of intellectual property infringing activities on the internet.

Once the rightholder or association has collected all the information necessary for submitting a complaint to the umbrella portal, they have to fill in a standardised notification form (one separate notification form for each URL offering counterfeit products).

---

<sup>543</sup> This section was drafted based on publicly available information and interviews with relevant stakeholders. The IACC did not participate in this study; therefore, the description in this section may not accurately reflect actual RogueBlock procedure.

<sup>544</sup> Kristina Montanaro (IACC). 'Executive Summary October 2012. IACC Payment Processor Portal Program: First Year Statistical Review', <http://www.gacg.org/Content/Upload/MemberNewsDocs/October%202012%20Report%20to%20IPEC%20-%20FINAL.pdf> [Document available via this link in November 2015].

There are two limitations on rightholders when it comes to submitting a complaint:

- The IACC currently only accepts complaints regarding standalone rogue websites, not online marketplace or auction websites<sup>545</sup>. However, the IACC has recently published on its website that one of the planned enhancements to the RogueBlock system will be that rightholders will also have be able to submit claims with regard to counterfeits being sold in certain online marketplaces<sup>546</sup>.
- Rightholders can submit no more than 25 complaints per-month<sup>547</sup>.

Rightholders also have the option of carrying out a test purchase, which may serve as further evidence that the product offered is counterfeit. Some stakeholders interviewed for the purposes of this Chapter 6 said that they always made a test purchase before submitting a complaint, while others do not.

Some stakeholders interviewed stated that, before submitting a complaint they usually sent a 'cease and desist letter' to the merchants, notifying them that they were engaged in illegal activity and requesting them to discontinue. If rightholders do not receive a satisfactory response or any response at all, they submit the letter to the IACC's umbrella portal as evidence when submitting the complaint notification form.

The majority of rogue websites do not disclose genuine names or addresses, or at least these details are not easily accessible. As a consequence, when rightholders or associations try to send a 'cease and desist letter', it usually has to be sent to a general email address. This action is voluntary on the part of rightholders, and the stakeholders interviewed stated that their decision on whether or not to send these kind of letters depended on the nature of the website or on how serious the infringement was.

Once all information is collected, the rightholder has to specify in the RogueBlock forms available, inter alia, the URL of the website and the type of intellectual property violation. They may also attach screenshots in which the availability of the payment processor's payment services and the counterfeit goods or pirated content can be seen. Certain stakeholders interviewed in the context of this Chapter 6 explained that rightholders occasionally attach information relating to the genuine goods for comparison with the counterfeit goods offered on the website. Without this information, it is significantly more difficult for payment processors to decide on the rightholder's complaint. In fact, rightholders are encouraged to provide screenshots and visuals<sup>548</sup> to make investigation and remediation easier for the payment processors.

Once the notification form is completed, it is submitted to the IACC, which analyses it and any other information provided in order to decide whether or not to pass it on to the IPR Center.

### 3.2.2. Analysis by the IACC<sup>549</sup>

Once the standardised complaint form has been completed and the corresponding documentation submitted to the umbrella portal, the IACC has to review each complaint for sufficiency and compliance. If the IACC finds the

---

<sup>545</sup> Kristina Montanaro (IACC). 'Executive Summary October 2012. IACC Payment Processor Portal Program: First Year Statistical Review', <http://www.gacg.org/Content/Upload/MemberNewsDocs/October%202012%20Report%20to%20IPEC%20-%20FINAL.pdf> [Document available via this link in November 2015].

<sup>546</sup> <http://www.iacc.org/online-initiatives/rogueblock>.

<sup>547</sup> Annemarie Bridy. 'Internet Payment Blockades'. University of Idaho College of Law; Stanford University Center for Internet and Society (February 2015) (Page 25).

<sup>548</sup> See point 1 of the RogueBlock 'Create Claim' form attached as Annex 1. This screenshot has been extracted from: Kristina Montanaro (IACC). 'Executive Summary October 2012. IACC Payment Processor Portal Program: First Year Statistical Review', <http://www.gacg.org/Content/Upload/MemberNewsDocs/October%202012%20Report%20to%20IPEC%20-%20FINAL.pdf> [Document available via this link in November 2015]. There might be an updated version of this form; however, it is not publicly available.

<sup>549</sup> Section 3.2.2. of this Chapter 6 ('Analysis of IACC') is almost totally based on the RogueBlock information publicly available. The IACC did not participate in this study.



complaint to be incomplete and/or deficient, it can either reject the complaint or send it back to the rightholder that submitted it for completion and/or correction of the deficiencies<sup>550</sup>.

Where a complaint regarding the same URL has already been submitted and is pending, the RogueBlock system will alert the IACC. The pending and the new complaint will then be merged.

After the IACC has reviewed the content of the complaint, an attempt is made to make an online purchase using a card that is valid but set to be declined. As the payment will be declined, no products will be delivered. The purpose of the resulting trace message is to assist the payment processors in identifying the merchant account associated with the URL<sup>551</sup>.

During the negotiations between the IACC and payment processors in 2011, and based on the best practices agreement already existing at that time, it was decided that the payment processors could perform this trace messaging. However, since rightholders started submitting more complaints than expected, the IACC agreed to undertake this task itself. In May 2012, the IACC opened a satellite office for all trace messaging work<sup>552</sup>.

Some of the stakeholders interviewed for the purpose of this Chapter 6 stated that the IACC trace messaging is only for card companies with open-loop networks, as payment networks and card companies with closed-loop networks carry out their own trace messaging.

Once the trace message has been conducted, the information and data obtained from it will be attached to the complaint. Once the standardised complaint form has been filled in and the trace message conducted, the IACC approves the complaint for submission to the IPR Center.

Afterwards, the IACC contacts the IPR Center, which can put a hold on the complaint if it considers that the RogueBlock procedure might interfere with any ongoing investigation or have criminal implications. Once it has obtained the information from the IACC's public documents, the IPR Center has only 24 hours to halt the procedure<sup>553</sup>.

If the IPR Center puts the complaint on hold or decides to start its own investigation because there are criminal implications, the RogueBlock procedure ends at this phase. If, on the contrary, the IPR Center does not put a hold on the complaint, it will be automatically accessible to the payment processors through the umbrella portal. This does not mean that the activity is legal, merely that it is not the subject of an ongoing investigation by the IPR Center.

It used to be the case that, before the complaint was made available to the payment processors, it was forwarded to the company G2<sup>554</sup>. This company would initiate the merchant identification process by comparing the URL against their database of known merchant accounts, which consists of merchant account data — apart from that obtained from the trace message — acquired by G2 from its existing relationships with payment processors. However, based on the information provided by certain stakeholders interviewed in the context of this Chapter 6, G2 is no longer a part of RogueBlock.

Once this phase has been completed and if the IPR Center has not put it on hold, the complaint becomes accessible to payment processors in the umbrella portal.

---

<sup>550</sup> Kristina Montanaro (IACC). 'Executive Summary October 2012. IACC Payment Processor Portal Program: First Year Statistical Review', <http://www.gacg.org/Content/Upload/MemberNewsDocs/October%202012%20Report%20to%20IPEC%20-%20FINAL.pdf> [Document available via this link in November 2015].

<sup>551</sup> Kristina Montanaro (IACC). 'Executive Summary October 2012. IACC Payment Processor Portal Program: First Year Statistical Review', <http://www.gacg.org/Content/Upload/MemberNewsDocs/October%202012%20Report%20to%20IPEC%20-%20FINAL.pdf> [Document available via this link in November 2015].

<sup>552</sup> Kristina Montanaro (IACC). 'Executive Summary October 2012. IACC Payment Processor Portal Program: First Year Statistical Review', <http://www.gacg.org/Content/Upload/MemberNewsDocs/October%202012%20Report%20to%20IPEC%20-%20FINAL.pdf> [Document available via this link in November 2015].

<sup>553</sup> This information could not be confirmed by the stakeholders interviewed in the context of this Chapter 6.

<sup>554</sup> G2 Web Services Inc. <http://www.g2webservices.com/>.

### 3.2.3. Investigation and remediation

Each payment processor has its own access credentials (e.g. username, password)<sup>555</sup> in order to operate in the umbrella portal. Once payment processors have access to the complaint through the umbrella portal, they can resolve it in accordance with their internal operating procedures and policies.

The procedure for handling complaints depends on the business model of each payment processor<sup>556</sup>:

- Closed-loop networks. These payment processors have a direct contractual relationship with their clients (merchants). Once they receive a complaint from a rightholder, they initiate their own merchant identification process and, once they have identified the merchant, may take action against the merchant's account.
- Open-loop networks. These payment processors do not have direct contractual relationships with their clients (merchants). Instead, they must rely on the appropriate third-party acquirer bank to take action against a merchant. Once the payment processor receives a complaint, its teams use the data and information sent by the IACC (gathered from the trace message) to identify the acquirer bank associated with the merchant. The payment processor then passes the findings on to the relevant acquirer bank. The bank conducts its own investigation and reports any remedial action taken against the merchant to the payment processor.
- PayPal. Once a complaint is forwarded to PayPal, its investigation team navigates the reported URL through the checkout process to identify the corresponding PayPal merchant account.
- Discover/PULSE/Diners Club. These companies initiate their own investigations and, depending on the merchants' relationship, relay the findings to the appropriate bank or may take action against the merchant's account themselves.

Since RogueBlock depends on payment processors' policies prohibiting merchants from using card services for illegal transactions, the use of the services offered by payment processors to sell counterfeit goods or pirated content constitutes a breach of these policies, and the merchants' accounts could be terminated.

However, as stakeholders interviewed stated, rightholders do not usually investigate whether there is a real payment account linked to the logo of the payment processor that they find on a rogue website. They assume that consumers can use this payment method to buy counterfeit products.

Therefore, once payment processors receive a complaint through the umbrella portal, their first action is to check whether there is a real payment account on this website or not. Stakeholders interviewed stated that, in the vast majority of cases, there is no real active account for buying counterfeit products, which means that the merchant is just using a payment processor's logo to give the website an appearance of legality. In such cases, the payment processors will contact the merchants in order to stop their use of the payment processors' logos and trade marks.

If there is a real and active payment account, the payment processors analyse the information uploaded by the rightholders in the umbrella portal as their decision will depend on this information. Stakeholders interviewed explained that they usually work only with copyright and trade mark complaints, not design complaints, since it is much more difficult to prove a design infringement. For the latter, payment processors need a higher level of clarification and information. In cases where payment processors receive a complaint based exclusively on the infringement of a design, they will ask the rightholders to obtain a court order to certify that there has been an infringement.

In practice, once an investigation has been carried out, the vast majority of payment processors contact the merchants in order to ask them to take down the counterfeit products as, otherwise, their merchant account will be

---

<sup>555</sup> <https://www.iaccmarketsafe.com/login.php>.

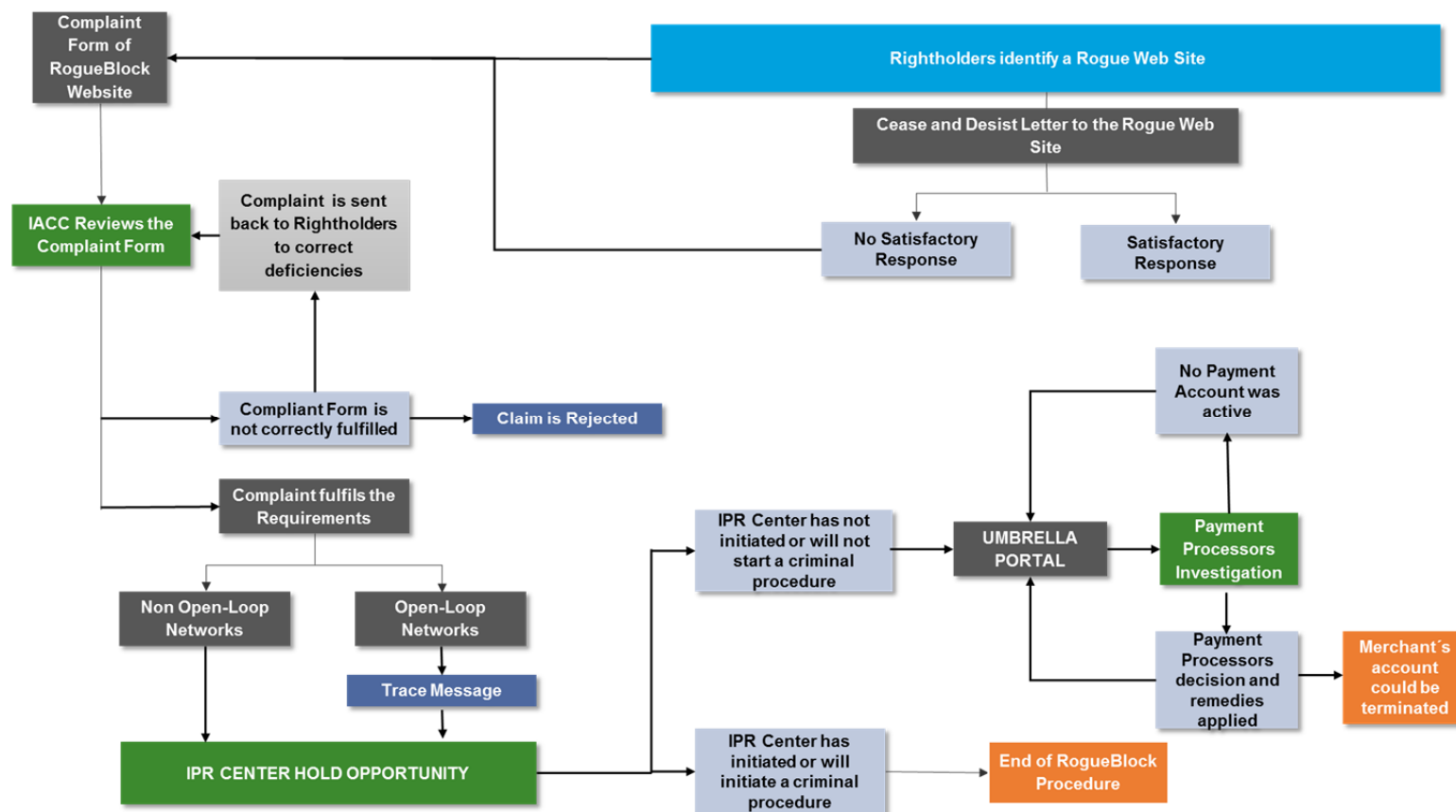
<sup>556</sup> Kristina Montanaro (IACC). 'Executive Summary October 2012. IACC Payment Processor Portal Program: First Year Statistical Review', <http://www.gacg.org/Content/Upload/MemberNewsDocs/October%202012%20Report%20to%20IPEC%20-%20FINAL.pdf> [Document available via this link in November 2015].

terminated. Once notified, merchants can contest the complaint and submit evidence to prove that they are not selling counterfeit products.

Once the payment processors' investigations have been completed, each payment processor notifies its decision and the corresponding remedies to the umbrella portal so that the information is accessible to rightholders.

At no time during the RogueBlock procedure are payment processors and rightholders directly in contact with each other as they submit all the corresponding information through the umbrella portal.

### 3.2.4. VCP Procedure flowchart<sup>557</sup>



<sup>557</sup> Data obtained from publicly available IACC information.

### 3.3. Other payment processor approaches

#### 3.3.1. Payment processors' own procedures

Before the launch of RogueBlock and other best practices subscribed to by payment processors, individual credit card companies had already established certain policies to self-regulate transactions involving illegal drugs and pornography. For example, Visa provided periodic reminders to its member financial institutions of their responsibility to ensure that only legal transactions enter the Visa Payment System. The company also seems to have initiated a regular programme of online monitoring to ensure that its payment services are not used for the sale of certain controlled and regulated substances<sup>558</sup>.

RogueBlock is not the only way for rightholders to submit complaints to payment processors.

Rightholders can also report infringements directly to a payment processor using the latter's own complaint system.

The main differences between RogueBlock and the payment processors' own procedures concern:

- complainants. The umbrella portal is designed for rightholders to prove to payment processors that a website is violating their intellectual property rights. The payment processors' complaint system addresses not only rightholders but also consumers.
- procedure. As certain stakeholders interviewed stated, if payment processors receive the complaint through the umbrella portal, they do not request evidence of ownership of the intellectual property rights in question as the IACC has already checked this. As per the payment processors' own procedures, the complainants have to provide all the documentation that verifies that they are the real rightholders.
- contact between rightholders and payment processors. While in RogueBlock, rightholders and payment processors do not interact with each other but through the umbrella portal, in the payment processors' own procedure, they interact directly with each other.

Under the payment processor's own procedures, once all the information submitted by the complainant has been analysed and verified by the payment processor (i.e., evidence that a brand owner is the real rightholder), the analysis of the complaint itself (i.e., the intellectual property infringement by a merchant) and the decision taken will follow the same procedure as complaints submitted through RogueBlock.

#### 3.3.2. Payment blocking considerations

One of the strengths of RogueBlock lies in the ability of rightholders to reach infringing websites outside the United States, as this VCP is not limited only to U.S. intellectual property laws, but applies to payment processor policies worldwide.

These policies do not allow illegal transactions, that is to say the selling or buying of illegal goods. The problem arises as to what is considered an illegal transaction since legislation varies from country to country.

It is easier for rightholders to get blocking orders under the law of some countries than it is in others. In addition, it may be that neither merchant nor cardholder is in the same country, with the same legal framework, which could result in a claim being submitted before the national courts of the cardholder or merchant, which are different from the payment processor's.

Problems of extraterritoriality were at the fore in the case of AllofMP3.com. In this case, U.S. cardholders were buying unauthorised content from the website (an online music store), which was hosted in Russia and operated

---

<sup>558</sup> BASCAP and the ICC. 'Roles and Responsibilities of Intermediaries: Fighting counterfeiting and piracy in the supply chain'. March 2015. Page 92.

by Russian nationals. Under U.S. copyright law, there was no doubt that the website was operating illegally. However, under Russian regulations, there was no intellectual property infringement.

In order to solve this problem, payment processors included in their policies clauses that require both merchants and cardholders to be in countries where the transactions are legal (i.e., Visa<sup>559</sup> and MasterCard<sup>560</sup>). A transaction that is illegal in the merchant's or cardholder's country will be considered to breach the payment processors' policies<sup>561</sup>.

### 3.3.3. Civil society considerations re payment blocking

In the opinion of the civil society association interviewed in the context of this Chapter 6, such payment-blocking VCPs should involve a public authority, namely a court, in the assessment of any request for taking down content from the internet on the grounds of IP infringement.

The association interviewed believes that these kinds of VCPs are very strong and effective tools for the rightholders, but potentially unfair towards possible users and merchants, given that they may see their relationship with a payment processor terminated unilaterally. The association considers that the Manila Principles<sup>562</sup> should apply to such practices; this would prevent websites from being wrongly targeted.

---

<sup>559</sup> Testimony of Denise Yee, Visa Inc. 'Hearing on Targeting Websites Dedicated To Stealing American Intellectual Property'. The United States Senate Committee on the Judiciary.

<https://www.judiciary.senate.gov/imo/media/doc/11-2-16%20Yee%20Testimony.pdf>

<sup>560</sup> [https://www.mastercard.com/us/wce/PDF/MasterCard\\_Anti-Piracy\\_Policy.pdf](https://www.mastercard.com/us/wce/PDF/MasterCard_Anti-Piracy_Policy.pdf).

<sup>561</sup> In the Visa Online Pharmacy Guide for Acquirers, this solution is referred to as 'dual jurisdictional compliance'.

<https://usa.visa.com/dam/VCOM/download/merchants/Online-Pharmacy-Guide-for-Acquirers-June-2014.pdf>.

<sup>562</sup> <https://www.manilaprinciples.org/>.

'Manila Principles on Intermediaries liability:

1. Intermediaries should be shielded from liability for third-party content.
2. Content must not be required to be restricted without an order by a judicial authority.
3. Requests for restrictions of content must be clear, be unambiguous, and follow due process.
4. Laws and content restriction orders and practices must comply with the tests of necessity and proportionality.
5. Laws and content restriction policies and practices must respect due process.
6. Transparency and accountability must be built into laws and content restriction policies and practices.'

## 4. Coexistence of the measures set forth under the RogueBlock with the U.S. legal framework

Section 4 of the Chapter 6 ('Coexistence of the measures set forth under the RogueBlock with the U.S. legal framework') summarises the U.S. legal framework and case law that is closely related to or may have an impact on the practical application of RogueBlock.

As shown in the previous Sections, RogueBlock proposes a procedure to help participants fight against the sale of counterfeit goods or pirated content on the internet. The implementation of this procedure by its stakeholders, following all the steps previously described, is crucial in determining and analysing the legal grounds that may arise, the remedies applied and the safeguards put in place within the RogueBlock system.

The considerations included in this Section are based upon the following hierarchy of legal sources:

- Fundamental rights in the United States of America (Section 4.1 of this Chapter 6 ('Fundamental rights in the U.S.)).
- U.S. Statutes (Section 4.2 of this Chapter 6 ('U.S. statutes')).
- Online intermediary liability (Section 4.3 of this Chapter 6 ('Online intermediary liability'))

### 4.1. Fundamental rights in the U.S.

In the U.S., the Declaration of Independence, the Constitution and the Bill of Rights<sup>563</sup> provide human rights protection. Many of the rights and freedoms contained in the Constitution correspond to rights enshrined in the UDHR. Furthermore, the U.S. Supreme Court<sup>564</sup>, as the highest legal instance in the U.S., has identified and recognised fundamental rights not explicitly stated in the Constitution (e.g. presumption of innocence in a criminal trial, freedom of movement).

The U.S. Supreme Court recognises fundamental rights, but this recognition is limited to rights concerning individuals and their protection as human beings.

As further analysed in Section 4.4 of this Chapter 6 ('Analysis of the VCP in relation to the U.S. Legal Framework'), it has been concluded that the VCP cannot be considered as colliding with any of the U.S.'s fundamental rights as set out in the Constitution and the Bill of Rights<sup>565</sup>.

The First Amendment to the Constitution recognises freedom of speech. However, none of the Amendments to the Constitution explicitly states that there is a right to privacy.

In addition to this, the Constitution and the Bill of Rights do not recognise all the economic, social, and cultural rights guaranteed in the UDHR. Certain rights can be found in some state statutes but others have not been recognised as fundamental rights. The fact that federal law does not address the protection of certain human rights means that there is a lack of ability to enforce those rights under federal law.

### 4.2. U.S. statutes

Intellectual property in the U.S. embraces, inter alia, copyright, patents and trade marks. Rightholders are afforded a variety of remedies under U.S. law when their intellectual property rights are infringed. Sellers of goods that infringe intellectual property are subject to both criminal and civil penalties.

---

<sup>563</sup> <http://www.humanrights.gov/references/key-us-human-rights-documents.html>.

<sup>564</sup> <http://www.supremecourt.gov/>.

<sup>565</sup> See complete wording in Annex 2 of this Chapter 6.



Moreover, and in relation to a possible conflict between this VCP and U.S. statutes, other statutes and Common Law actions, such as breach of contract, tortious interference with business relationships and data protection laws, should be taken into account. These actions will be analysed in Section 4.4 of this Chapter 6 ('Analysis of the VCP in relation to the U.S. legal framework').

Inter alia, the following provisions of the U.S. statutes and the common law are related to RogueBlock<sup>566</sup> to the extent that they deal with the protection of intellectual property rights and their enforcement:

- Intellectual property statutes:
  - Title 15 of the U.S. Code, Sections 1052 et seq. and Section 1124. These Sections establish federal trade mark registration and protection rights that confer several benefits, such as recording material with the U.S. Customs and Border Protection in order to prevent the importation of foreign counterfeit goods by third party infringers.
  - Title 15 of the U.S. Code, Sections 1116 to 1118. These Sections establish the civil remedies for trade mark infringements, such as injunctions, recovery of infringer's profits, damages for past infringements suffered by the owners of a trade mark, destruction of all materials bearing an infringing mark and costs of such action.
  - Title 18 of the U.S. Code, Sections 2318, 2320 and 2323. These Sections establish the federal criminal remedies for intentionally dealing in goods or services and knowingly using a counterfeit mark, and for trafficking in labels or other packaging or documentation knowing that a counterfeit mark has been applied. These federal criminal remedies include fines, imprisonment, or both. Fines can also be issued to corporations. The infringing enterprise's vehicles, storage facilities and equipment can be seized and articles bearing the infringing marks destroyed.
  - Title 15 of the U.S. Code, Section 1117 and Title 19 of the U.S. Code, Section 1526. These Sections establish the federal civil remedies for trade mark infringement, which include seizure of the goods, counterfeit marks, means of making the marks and relevant business records, mandatory treble damages and recovery of profits, possible prejudgment interest and attorney's fees, and civil fines on infringing imports up to twice the value that the merchandise would have had if it were genuine.
  - Title 18 of the U.S. Code, Sections 2319 and 2323. These Sections make wilful copyright infringement for profit a felony, the penalties for which depend on both the number of copies reproduced or distributed during a given period of time, and whether it is a first or subsequent offence. In addition, a court may order seizure, forfeiture, destruction, restitution or other disposal of all infringing reproductions and all equipment used in their manufacture. Additional penalties apply to trafficking in counterfeit record, film and computer program labels and documentation.
  - Title 17 of the U.S. Code, Sections 501 to 505 and 601-603. These Sections establish the civil remedies available to copyright owners under federal law and include, inter alia, injunctions against future infringements, the seizure, forfeiture, destruction, restitution or other disposal of all infringing reproductions, the seizure of records and information, the actual damages suffered by copyright owners, and civil fines imposed by Customs against importers of counterfeit goods.
  - Title 35 of the U.S. Code, Sections 101 et seq and 171. These Sections establish the right of patent owners to prevent others from making, using, offering for sale or selling an invention within the U.S. or importing it into the U.S. Utility patents are available for processes, business methods, machines, articles of manufacture, and compositions of matter, while design patents are available for a new, original and ornamental design for an article of manufacture.
  - Title 35 of the U.S. Code, Sections 283 to 285. These Sections establish the following civil remedies for patent infringement available under U.S. law: injunctions and compensatory damages.
  - Section 337 of the Tariff Act of 1930 and Title 19 of the U.S. Code, Section 1337. These Sections detail where there has been a violation of the applicable regulations in relation to the importation of

<sup>566</sup> For U.S. legal framework, see Annex 2 of this Chapter 6.

goods that could result in an order excluding counterfeit goods from entry into the U.S. or demanding the cease and desist of certain acts.

- **Agreements between private parties.** Title 41 of the U.S. Code, Section 6503. This Section regulates the obligations established by agreements (express or implied) between private parties.
- **Personal data statutes.** Title 15 of the U.S. Code, Sections 6801 to 6827. These Sections regulate the collection, use and disclosure of financial information.
- **Common law.** RogueBlock is relatively new and no case law has been found with respect to this specific VCP; however, there is some case law concerning intermediaries that may be applicable to RogueBlock too. See Section 4.3 of this Chapter 6 ('Online intermediary liability').

### 4.3. Online intermediary liability

As explained in a study carried out in November 2009 by the European Commission<sup>567</sup>, the DMCA was a legal compromise after the strong lobbying work of both content providers and online service providers. It was a response to concerns that online service providers (i.e., payment processors) would be afraid of incurring secondary liability and therefore would be reluctant to invest in technological experimentation (e.g. a tool that made works available online while guaranteeing their adequate protection).

The DMCA also responded to concerns that copyright holders would decline to make works available online unless they were assured that their work would be adequately protected. It increased the penalties and sanctions for online copyright infringement and addressed issues such as anti-circumvention of protection measures and access restrictions.

Regarding liability, the DMCA introduced a safe harbour for online service providers for copyright claims resulting from the conduct of their customers. Section 512 of the DMCA (i.e., OCILLA)<sup>568</sup> stipulates that the safe harbour was established to ensure that online service providers would have incentives to remove infringing material.

Online service providers would also be protected from lawsuits and judgments based on secondary liability for copyright infringements<sup>569</sup>, as long as the court dismissed any possible vicarious liability arguments raised by the plaintiff.

In this regard, U.S. case law generally recognises two types of secondary liability in the context of copyright infringements:

- contributory infringement. This secondary liability arises when a party with knowledge of another party's infringing conduct has materially contributed to that conduct; and
- vicarious liability. This secondary liability arises when a defendant has enjoyed a financial benefit from the infringing conduct of another person, whose infringing conduct the defendant had the 'right and ability to supervise'<sup>570</sup>.

The following case law is of particular relevance for determining restrictions on secondary liability for intellectual property infringement:

- **Perfect 10 ruling**

Perfect 10 is a publisher of adult magazines and websites. According to Perfect 10, one operator copied images owned by Perfect 10 from the latter's website and displayed them on its own website. Perfect 10 initiated a lawsuit

---

<sup>567</sup> European Commission, Information Society and Media Directorate General. EU Study (SMART 2007/0037) on the 'Legal analysis of a Single Market for the Information Society-Liability of online intermediaries', November 2009.

<sup>568</sup> Entitled the 'Online Copyright Infringement Liability Limitation Act' (OCILLA).

<sup>569</sup> J.M. Urban and L. Quilter, 'Efficient Process or Chilling Effects—Takedown Notices Under Section 512 of the Digital Millennium Copyright Act', 22 Santa Clara Comp. & High Tech. L.J. 621 (2006).

<sup>570</sup> M. Scott, 'Safe harbors under the Digital Millennium Copyright Act', New York University Journal of Legislation and Public Policy, 2005, 9: 99, p. 104; P. Menell and D. Nimmer, 'Legal realism in action: indirect copyright liability's continuing tort framework and Sony's de facto demise', in UC Berkeley Public Law Research Paper, No 966380.

against intermediaries, which included Visa, arguing that they were liable for secondary infringement based on the use of their services by a merchant for facilitating copyright infringement. In 2007, the U.S. Court of Appeals for the Ninth Circuit ruled in favour of Visa. In general terms, this sentence considered that payment processors were not subject to secondary copyright liability for the use of their networks for selling infringing material. Payment processors are considered to be too remote from the infringements not to have the ability to discover or prevent infringements.

- **Betamax ruling**

The Betamax case is a decision by the Supreme Court of the U.S. that ruled that the making of individual copies of complete television shows for time-shifting purposes does not constitute copyright infringement, but is fair use. The Court also ruled that the manufacturers of home video recording devices, such as Betamax or other VCRs, could not be liable for infringement. The case created a legal safe haven for such technology, which also significantly benefited the entertainment industry through the sale of pre-recorded movies. It constituted an important restriction on secondary liability for copyright infringement.

The broader legal consequence of the Court's decision was the establishment of a general test for determining whether a device with copying or recording capabilities runs afoul of copyright law. This test has raised some interpretative challenges for courts when applying the case to more recent file sharing technologies available for use on home computers and over the internet.

- **Tiffany v eBay ruling**

In this case, Tiffany led an action against eBay arguing that a 'significant portion' of the Tiffany jewellery sold on eBay was not genuine, and that the latter was liable for secondary liability. Based on the conclusions of the *Inwood v Ives* case, there are two circumstances that establish secondary liability: (i) intentional inducement, and (ii) continued supply with actual or constructive knowledge of infringement. As Tiffany did not argue that eBay had induced the sale of counterfeit goods, the case was based on 'the second possibility identified in the *Inwood* case'. eBay had implemented certain measures to prevent the sale of counterfeit goods, such as a notice and takedown system that allowed rightholders to submit a notice identifying counterfeited items. Tiffany used this system, listing the counterfeit goods and sending the list to eBay so that the latter could remove the goods from its site. However, eBay continued to sell other items from Tiffany. The latter therefore considered that eBay had reason to know that the sales were of counterfeits as it already had general knowledge that its services were used to sell counterfeit goods due to the listing Tiffany had sent. The Court held eBay not liable, since a service provider must have more than just general knowledge or reason to know that its services are being used to sell counterfeit goods.

#### 4.4. Analysis of the VCP in relation to the U.S. legal framework

In light of the U.S. legal framework discussed in the preceding Sections of this Chapter 6, it cannot be excluded that some procedures envisaged by the VCP might be considered inconsistent with legal provisions.

Since RogueBlock is an extrajudicial and private practice by nature, the applicable body of law is that which relates to private behaviour between individuals. Section 4.4 ('Analysis of the VCP in relation to the U.S. legal framework') will analyse the following:

- In light of the U.S. legal framework discussed in the preceding Sections of this Chapter 6, an analysis should be carried out of whether the VCP contains procedures that may be considered inconsistent with the freedom of speech and the right to privacy mentioned in Section 4.1 of this Chapter 6 ('Fundamental rights in the U.S.'). Section 4.4.1 of this Chapter 6 ('Coexistence of the VCP with the fundamental rights in the U.S.') therefore reviews the procedures in that light.
- A merchant that considers its account to be unjustly terminated could bring a suit under a common law breach of contract. Section 4.4.2 of this Chapter 6 ('Coexistence of the VCP with the right of merchants to bring a suit under a common law breach of contract'), reviews the merchant's right to bring a suit under a breach of contract claim against payment processors.
- A wrongfully terminated merchant account could give rise to claims based on tortious interference with a business relationship. This will be analysed under Section 4.4.3 ('Coexistence of the VCP with the right of merchants to bring a suit under tortious interference with business relationships').

- Finally, while RogueBlock is designed in such a way as to make a data breach unlikely, data protection laws do also apply, as mentioned by certain stakeholders interviewed for the purpose of this Chapter 6. Section 4.4.4 of this Chapter 6 ('Coexistence of the VCP with the protection of merchants' personal data') analyses whether the U.S. data protection statutes may have an impact on RogueBlock.

#### 4.4.1. Coexistence of the VCP with the fundamental rights in the U.S.

As previously stated in Section 4.1 of this Chapter 6 ('Fundamental Rights in the U.S.'), economic, social and cultural issues are not viewed as fundamental rights under U.S. federal law. Therefore, the implementation of RogueBlock as a private and voluntary practice, the purpose of which is to combat intellectual property infringement, cannot be considered as colliding with any of the U.S.'s fundamental rights, as set out in the Constitution and the Bill of Rights.

Consequently, none of the fundamental rights of the stakeholders involved in the VCP are violated by the RogueBlock procedure under U.S. federal law<sup>571</sup>.

#### 4.4.2. Coexistence of the VCP with the right of merchants to bring a suit under a common law breach of contract

In the U.S., the law varies from state to state; there is no nationwide federal contract law, although transactions involving the sale of goods have become highly standardised nationwide.

Contract law is governed by two main sources:

- common law, created by the courts through their interpretation of prior facts and circumstances; and
- specific statutes in each jurisdiction, generally at state level.

As RogueBlock is based on private contracts between merchants and payment processors, whenever a merchant considers that its account has been unfairly suspended, it has the right, in order to protect its interests, to bring a suit under a common law breach of contract claim.

As previously mentioned, and as stated by certain stakeholders interviewed, payment processors have their own administrative procedures for merchants contesting the suspension or termination of their merchant accounts. In this regard, if there is a claim against a merchant, the payment processor will always contact the merchant to inform it about the complaint and try to obtain evidence of the offering for sale of counterfeit products. The payment processor will then analyse the evidence provided by the merchant and take a decision.

In this connection, the contracts entered into by payment processors and merchants all require participating merchants to consent to stringent rules. As stated by certain stakeholders interviewed for the purpose of this Chapter 6, each payment processor has its own administrative procedures for merchants contesting the suspension or termination of their accounts.

Thus with regard to a merchant bringing a suit under common law for breach of contract it may be argued that, even though RogueBlock does not itself make any provision for merchants to contest claims against them, there is a safeguard for merchants through the payment processor's own procedure. Therefore, it is unlikely that these actions could be successful in court. To date, no such cases have been known to be brought against the IACC by any merchant.

---

<sup>571</sup> The impact of this VCP on fundamental rights recognised by U.S. state law has not been analysed.

#### 4.4.3. Coexistence of the VCP with the right of merchants to bring a suit under tortious interference with business relationships

Another relevant action that can be taken under U.S. common law is tortious interference with business relationships. This is taken when someone intentionally damages a business relationship of the plaintiff with the aim of preventing the plaintiff from successfully establishing or maintaining that business relationship. Tortious interference with business relationships occurs where the defendant acts to prevent the plaintiff from successfully establishing or maintaining business relationships.

Tortious interference is broadly divided into two categories, one specific to contractual relationships (irrespective of whether they involve a business), and the other specific to business relationships or activities (irrespective of whether they involve a contract). There is also the possibility to claim tort of negligence in the event of such interference<sup>572</sup>.

A merchant whose payment processor account was wrongfully suspended or terminated may be able to argue that the IACC or its members, through RogueBlock, are liable for damages under the theory of tortious interference.

In such a case the claim of tortious interference requires proof that:

- the defendant acted purposefully and maliciously with intent to injure;
- the defendant acted improperly and without privilege;
- the defendant induced a third party not to enter or continue a business relationship with the plaintiff; and
- the defendant caused the plaintiff some sort of financial injury.

In this sense, if merchants bring a suit under tortious interference with business relationships against RogueBlock, the IACC may be able to argue that, in practice, the acts it carried out through RogueBlock are aimed at preventing an illegal practice, namely the sale of counterfeit products or pirated content, and are not improper or carried out with malicious intent to injure the merchants, but in order to protect rightholders, consumers and civil society. To date, no such cases are known to have been brought by any merchant against the IACC but, for the reasons previously given, it is unlikely that such actions could be successful in court.

#### 4.4.4. Coexistence of the VCP with the protection of merchants' personal data

In the U.S. the collection and use of personal data is not regulated by any single law, but by a large number of federal privacy-related laws. Some of these apply to particular categories of information, such as that concerning children, health care, security breaches, financial information or electronic communications.

In addition, different governmental agencies and industry groups have developed guidelines that, being self-regulatory ('best practices'), are not legally enforceable. Nonetheless, these self-regulatory measures have accountability and enforcement components that are increasingly being used as a tool for enforcement by regulators, such as the Federal Trade Commission<sup>573</sup>. For example, the Financial Services Modernization Act<sup>574</sup> regulates the collection, use and disclosure of financial information. This means that this Act prohibits the disclosure of personal data, such as full credit card information or a person's full name—that is to say, any data that may allow a third party to identify a person. However, this Act applies broadly to financial institutions (i.e., banks, security firms, insurance companies, etc.) and to other businesses that provide financial services and

---

<sup>572</sup> Sandra S. Baron, Hilary Lane, and David A. Schulz, 'Tortious Interference: The Limits of Common Law Liability for Newsgathering', 4 Wm. & Mary Bill Rts. J. 1027 (1996).

<sup>573</sup> <https://www.ftc.gov/es>.

<sup>574</sup> Title 15 of the United States Code, Sections 6801-6827.

products. Consequently, the Financial Services Modernization Act does not govern any of the data flows in which the IACC takes part as this organisation cannot be considered a financial institution<sup>575</sup>.

In relation to the information publicly available about RogueBlock and the statements of certain stakeholders interviewed for the purposes of this Chapter 6, we find two different means of data communication:

1. Rightholder — IACC — merchant

Under the RogueBlock procedure rightholders are not supposed to receive any more of a merchant's data than what a rightholder has discovered and included in the complaint submitted to the umbrella portal. The rightholder does not receive any details of the merchant's account. Similarly, the merchant does not disclose any personal data to third parties.

Consequently, it would be difficult to allege a violation of personal data statutes within the RogueBlock program in this scenario as there is no disclosure of personal data among the parties.

2. Merchant — IACC — payment processors/IPR Center

The merchant data obtained through a trace message is disclosed by the IACC to the payment processors and to the IPR Center. The majority of US data privacy laws deal with non-public consumer information, such as names, social security numbers, etc. Since the IACC's RogueBlock is designed to block transactions coming from merchants (rather than consumers), it would seem that the federal data protection laws 576 would not apply to this disclosure.

Therefore, although U.S. data protection laws at state level may regulate these types of data assignments, RogueBlock does not breach any U.S. federal data protection regulations.

## 4.5. Summary of findings relating to the coexistence of the RogueBlock with the U.S. legal framework

This Section summarises the findings made under Section 4 of this Chapter 6 ('Coexistence of the measures set forth under the RogueBlock with U.S. legal framework') regarding the compatibility of RogueBlock with U.S. federal law.

RogueBlock is a private and voluntary practice, the purpose of which is to combat intellectual property infringement. It does not collide with any of the U.S. fundamental rights comprised in the Constitution and the Bill of Rights.

It would be possible for a merchant to bring a lawsuit against payment processors alleging (i) breach of contract for wrongful suspension/termination or (ii) tortious interference with a business relationship, as it could be alleged that the IACC damages the merchant's contractual or other business relationships. Notwithstanding this possibility, it is unlikely that such actions could be successful, as payment processors' internal administrative procedures, which require merchants' consent to stringent rules and include the possibility of contesting the suspension or termination of a merchant account, minimise the feasibility of a successful lawsuit. The IACC would likely be able to argue successfully that the purpose of acts carried out through RogueBlock to stop counterfeiters are not improper or carried out with malicious intent to injure merchants.

To date, no such cases are known to have been brought by any merchant against the IACC.

Concerning the protection of merchants' personal data, a data protection breach within RogueBlock would not occur between the parties as neither merchants' nor rightholders' privacy is violated.

---

<sup>575</sup> The Financial Services Modernization Act is applicable only to financial institutions, which are defined as: (i) non-bank mortgage lenders, (ii) real estate appraisers, (iii) loan brokers, (iv) certain financial or investment advisers, (v) debt collectors, (vi) tax return preparers, (vii) banks, and (viii) real estate settlement service providers.

<sup>576</sup> U.S. data protection regulations at state level are not covered in this analysis.

## 5. Technologies

As mentioned in the analysis in Section 3 of this Chapter 6 ('Duties and Procedures'), the use of technology is an essential part of the VCP since the sale of counterfeit goods or pirated content is reported through the umbrella portal.

Such reporting is performed by rightholders through the online complaint form available on the RogueBlock website. Each stakeholder involved (i.e., rightholders and payment processors) has its own username and password to access the umbrella portal.

In addition, technologies have played an important role from the very beginning of this VCP. As stated by certain stakeholders interviewed in the context of this Chapter 6, rightholders had to adopt appropriate measures and tools to allow them to identify the selling of counterfeit products (e.g. tools that search for rogue websites). The IACC had to design the umbrella portal that permits it to file and process all information related to the complaints submitted.

According to information on the IACC's website<sup>577</sup>, further developments of the tool are planned, such as (i) reporting tools that will allow participants to measure returns on investment and to generate investigative leads, and (ii) a data-sharing program that will use participants' claims to suspend and lock down rogue websites as well as terminate payment services.

---

<sup>577</sup> <http://www.iacc.org/online-initiatives/rogueblock>.



## 6. Costs

Initially, the rightholders participants of RogueBlock had to pay a fee<sup>578</sup> due to their membership in the IACC.

The IACC assumes some of the costs in taking on the execution of trace messages. Up to October 2011, over five thousand individual trace messages were conducted. The main difficulties lie in the costs associated with executing trace messages, that is to say the labour costs of the trace messages plus the investment in infrastructure for trace messaging (e.g. computers, phones and credit cards)<sup>579</sup>.

The main costs that payment processors have to assume originate from the need to have internal or external staff responsible for dealing with the merchant's accounts investigations.

One of the interviewed payment processors, for example, has internal personnel dedicated to controlling all the complaints submitted in RogueBlock. It also has an external service provider which carries out investigations once it receives the complaint. This stakeholder stated that the costs involved are the same for RogueBlock as for the rest of the complaints received through the forms available on its own website.

Both categories of participants (i.e., rightholders and payment processors) see these costs and expenses as an investment that contributes to the good reputation of their businesses.

---

<sup>578</sup> The annual membership fees at the time of drafting this Chapter 6 are detailed at the following site:  
<http://www.iacc.org/membership/dues>.

<sup>579</sup> Kristina Montanaro (IACC). 'Executive Summary October 2012. IACC Payment Processor Portal Program: First Year Statistical Review',  
<http://www.gacg.org/Content/Upload/MemberNewsDocs/October%202012%20Report%20to%20IPEC%20-%20FINAL.pdf> [Document  
available on the previous link on November 2015].

## 7. Education

In 2013, the IACC launched a consumer education campaign to increase awareness regarding the risks associated with shopping on websites selling counterfeits. This campaign works through the website *designsfauxreal.com*. This website is a 'fake fake-shopping site' that follows the parameters of a rogue website and its main aim is to show users what risks they take when buying counterfeit goods. The website was created by the IACC in collaboration with MasterCard and the IPR Center as a way to educate consumers who actively search for counterfeit goods<sup>580</sup>.

The IACC also organises educational activities for general consumers and users. An example of this is the 'Counterfeit Crimes Gallery' that was displayed at the Washington DC Crime Museum in 2014. The gallery was created as a result of collaboration between the museum, the IACC, the IPR Center and a wide range of industries<sup>581</sup>. The main aim of the gallery is to build awareness among consumers about the damage caused by counterfeiting.

Furthermore, the IACC organises events for industry stakeholders such as the so-called 'Spring Conference' or 'Fall Conference'. The main objective of these conferences is to keep relevant stakeholders updated in relation to industry and best practices and ensure that they are informed about intellectual property trends and solutions<sup>582</sup>.

The IACC collaborates with the payment processor and acquirer banks and trains them in the risks associated with taking on merchants selling counterfeit products<sup>583</sup>.

The training activity of the IACC is not only focused on RogueBlock. The IACC also trains customs agents and other authorities to facilitate enforcement and stop counterfeiting<sup>584</sup>. These training sessions include global events. The IACC has specific training sessions for, among others, Latin-America, mainly focused on activities relating to education, in particular on how to distinguish a counterfeit product from an original one.

Furthermore, the IACC has a partnership with the national government and local associations, the main aim of which is to boost law enforcement and to exchange information about best practices<sup>585</sup>.

More generally, outside the IACC initiatives, the USPTO<sup>586</sup> and the U.S. Copyright Office<sup>587</sup> have learning-focused websites that include learning tools and relevant links. Likewise, the NCPC, in partnership with the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, runs a comprehensive, research-based public awareness campaign against intellectual property theft<sup>588</sup>. This campaign consists of video public service announcements for TV and online use, radio spots, printed signs and brochures.

The Global Intellectual Property Center<sup>589</sup> supports educational campaigns that include documentaries. The Center also publishes an annual international intellectual property report that evaluates and ranks the IP environments in countries and economies. The 2015 Index also includes an annex<sup>590</sup> with data on the correlation between an intellectual property environment and certain socio-economic development factors.

---

<sup>580</sup> Kristina Montanaro (IACC), 'Executive Summary October 2012. IACC Payment Processor Portal Program: First Year Statistical Review'. <http://www.gacg.org/Content/Upload/MemberNewsDocs/October%202012%20Report%20to%20IPEC%20-%20FINAL.pdf> [Document available on the previous link on November 2015].

<sup>581</sup> <http://www.iacc.org/announcements/iacc-crime-museum-unveil-counterfeit-crimes-gallery-first-in-u-s>.

<sup>582</sup> <http://www.iacc.org/conferences/spring-conference>.

<sup>583</sup> Kristina Montanaro (IACC), 'Executive Summary October 2012. IACC Payment Processor Portal Program: First Year Statistical Review', <http://www.gacg.org/Content/Upload/MemberNewsDocs/October%202012%20Report%20to%20IPEC%20-%20FINAL.pdf> [Document available on the previous link on November 2015].

<sup>584</sup> <http://www.iacc.org/training/us>.

<sup>585</sup> <http://www.iacc.org/training/international>.

<sup>586</sup> <http://www.uspto.gov/learning-resources>.

<sup>587</sup> <http://copyright.gov/>.

<sup>588</sup> <http://www.ncpc.org/topics/intellectual-property-theft>.

<sup>589</sup> <http://www.theglobalipcenter.com/>.

<sup>590</sup> [http://www.theglobalipcenter.com/wp-content/uploads/2015/02/GIPC\\_IPIndex\\_Annex\\_final.pdf](http://www.theglobalipcenter.com/wp-content/uploads/2015/02/GIPC_IPIndex_Annex_final.pdf).

## 8. Effectiveness

### 8.1. Numbers and statistics

Since the implementation of RogueBlock in December 2011 the program has terminated over 5 000 individual accounts of merchants selling counterfeit goods, which has impacted over 200 000 rogue websites<sup>591</sup>.

From December 2011 to September 2012, out of a total of 3 140 complaints only 200 were rejected by the IACC and 2 181 investigations were closed. However, in this same time frame, from 9 728 payment channels, 6 716 had actually no account with the payment processors that participate in this VCP. From the 2 680 complaints related to merchants that had an account with a payment processor, 906 finished with the termination of the merchant account<sup>592</sup>.

### 8.2. Challenges<sup>593</sup>

The effectiveness of RogueBlock is subject to certain external elements that pose a challenge for the participants in this VCP:

- Transaction history of credit cards: the trace messages are essential in order to facilitate the identification of the merchants for the open-loop networks as we have seen in Section 3 ('Duties and Procedures'). As explained, trace messaging will always be done using prepaid credit cards because these cards can be purchased anonymously. However, there are not many prepaid credit cards that provide online access to their users regarding the transaction history, which is important to gather all the necessary information to finish the trace message successfully.
- Card numbers and aliases: conducting multiple transactions with the same credit card and alias can trigger the fraud check systems. To avoid blocking the credit cards, aliases and trace messaging cards have to be constantly rotated and changed.
- BIN number: this number consists of six digits listed on the card and is used to identify the issuing bank. When the trace message is conducted, the credit card will always be declined. The main objective of the trace messaging is to establish a connection between the transaction and the merchant. When credit cards of a single issuer are constantly being declined, the merchant may get suspicious and block the transactions of credit cards with that particular issuer. BIN number diversity is therefore necessary.
- Fraud check systems: rogue merchants are beginning to use more fraud check systems to intentionally block the IACC trace messages. Those systems include, among others, IP geo-location, confirmation of residential location of the buyers or blocking the payment with prepaid cards.

Despite the efficiency of RogueBlock in the first years, rogue merchants often choose payment processors that are more difficult to track or find new mechanisms to escape the monitoring of rightholders and payment processors<sup>594</sup>.

---

<sup>591</sup> <http://www.iacc.org/online-initiatives/rogueblock>.

<sup>592</sup> Kristina Montanaro (IACC). 'Executive Summary October 2012. IACC Payment Processor Portal Program: First Year Statistical Review', <http://www.gacg.org/Content/Upload/MemberNewsDocs/October%202012%20Report%20to%20IPEC%20-%20FINAL.pdf> [Document available on the previous link on November 2015].

<sup>593</sup> <http://www.gacg.org/Content/Upload/MemberNewsDocs/October%202012%20Report%20to%20IPEC%20-%20FINAL.pdf>.

<sup>594</sup> BASCAP and the ICC. 'Roles and Responsibilities of Intermediaries: Fighting counterfeiting and piracy in the supply chain'. (March 2015).

## Chapter 6: Annex 1

### Create Claim

Brand

Home Page URL\*

URL of Violation\*

Investigation date\*

Violation types\*

☐ Trademark Counterfeiting
☐ Trademark Counterfeiting - Fragrance
☐ Trade Dress Infringement
☐ Copyright Piracy
☐ Circumvention Device
☐ Trademark Counterfeiting - Pharma
☐ Trademark Counterfeiting - Tobacco
☐ Pharma - No Prescription Required

Screenshots

Choose File

No file chosen

Clear

Enter the URL, where the screenshot was taken.

Add Additional Screenshot

File

Choose File

No file chosen

Clear

Attachments

Add Additional File

No file chosen

Purported payment methods\*

☐ American Express
☐ Discover / PULSE / Diners Club
☐ JCB
☐ MasterCard
☐ Moneybookers
☐ MoneyGram
☐ PayPal
☐ Visa
☐ Western Union

Trademarks and copyrights\*

Legal actions

☐ Cease and Desist - Webhost
☐ Cease and Desist - ISP
☐ Other relevant notifications
☐ Digital Millennium Copyright Act

Description of Investigation and Evidence Sufficient to Prove the Allegation\*

I have a good faith belief that the website or webpage located at the URL(s) listed above sells, offers for sale, or makes available goods and/or services that infringe the IP owner's intellectual property rights.

I am the OWNER or AGENT AUTHORIZED TO ACT ON BEHALF OF THE OWNER of certain intellectual property rights listed above.

Signature\*

Type your signature here...

By submitting this notice, you declare that all of the information contained in this notice is accurate and that the use of your intellectual property described above, in the manner you have complained of, is not authorized by the rights owner, its agent, or the law.

## Chapter 6: Annex 2

### Fundamental rights in the U.S.A.

#### Constitution

- Amendment I
  - 'Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.'
- Amendment III
  - 'No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law.'
- Amendment IV
  - 'The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized'.

### U.S.A. legal system

#### The United States Code<sup>595</sup>

- Title 15 of the U.S. Code, Section 1052
  - No trademark by which the goods of the applicant may be distinguished from the goods of others shall be refused registration on the principal register on account of its nature unless it—
    - (a) Consists of or comprises immoral, deceptive, or scandalous matter; or matter which may disparage or falsely suggest a connection with persons, living or dead, institutions, beliefs, or national symbols, or bring them into contempt, or disrepute; or a geographical indication which, when used on or in connection with wines or spirits, identifies a place other than the origin of the goods and is first used on or in connection with wines or spirits by the applicant on or after one year after the date on which the WTO Agreement (as defined in section 3501(9) of title 19) enters into force with respect to the United States. (b) Consists of or comprises the flag or coat of arms or other insignia of the United States, or of any State or municipality, or of any foreign nation, or any simulation thereof. (c) Consists of or comprises a name, portrait, or signature identifying a particular living individual except by his written consent, or the name, signature, or portrait of a deceased President of the United States during the life of his widow, if any, except by the written consent of the widow. (d) Consists of or comprises a mark which so resembles a mark registered in the Patent and Trademark Office, or a mark or trade name previously used in the United States by another and not abandoned, as to be likely, when used on or in connection with the goods of the applicant, to cause confusion, or to cause mistake, or to deceive: Provided, That if the Director determines that confusion, mistake, or deception is not likely to result from the continued use by more than one person of the same or similar marks under conditions and limitations as to the mode or place of use of the marks or the goods on or in connection with which such marks are used, concurrent registrations may be issued to such persons when they have become entitled to use such marks as a result of their concurrent lawful use in commerce prior to (1)

---

<sup>595</sup> The complete wording of the U.S. Code can be found via the following link:  
<http://uscode.house.gov/browse/prelim@title15/chapter2/subchapter1&edition=prelim>

the earliest of the filing dates of the applications pending or of any registration issued under this chapter; (2) July 5, 1947, in the case of registrations previously issued under the Act of March 3, 1881, or February 20, 1905, and continuing in full force and effect on that date; or (3) July 5, 1947, in the case of applications filed under the Act of February 20, 1905, and registered after July 5, 1947. Use prior to the filing date of any pending application or a registration shall not be required when the owner of such application or registration consents to the grant of a concurrent registration to the applicant. Concurrent registrations may also be issued by the Director when a court of competent jurisdiction has finally determined that more than one person is entitled to use the same or similar marks in commerce. In issuing concurrent registrations, the Director shall prescribe conditions and limitations as to the mode or place of use of the mark or the goods on or in connection with which such mark is registered to the respective persons. (e) Consists of a mark which (1) when used on or in connection with the goods of the applicant is merely descriptive or deceptively misdescriptive of them, (2) when used on or in connection with the goods of the applicant is primarily geographically descriptive of them, except as indications of regional origin may be registrable under section 1054 of this title, (3) when used on or in connection with the goods of the applicant is primarily geographically deceptively misdescriptive of them, (4) is primarily merely a surname, or (5) comprises any matter that, as a whole, is functional.[...]

- Title 15 of the U.S. Code, Section 1124

- 'Except as provided in subsection (d) of section 1526 of title 19, no article of imported merchandise which shall copy or simulate the name of any domestic manufacture, or manufacturer, or trader, or of any manufacturer or trader located in any foreign country which, by treaty, convention, or law affords similar privileges to citizens of the United States, or which shall copy or simulate a trademark registered in accordance with the provisions of this chapter or shall bear a name or mark calculated to induce the public to believe that the article is manufactured in the United States, or that it is manufactured in any foreign country or locality other than the country or locality in which it is in fact manufactured, shall be admitted to entry at any customhouse of the United States; and, in order to aid the officers of the customs in enforcing this prohibition, any domestic manufacturer or trader, and any foreign manufacturer or trader, who is entitled under the provisions of a treaty, convention, declaration, or agreement between the United States and any foreign country to the advantages afforded by law to citizens of the United States in respect to trademarks and commercial names, may require his name and residence, and the name of the locality in which his goods are manufactured, and a copy of the certificate of registration of his trademark, issued in accordance with the provisions of this chapter, to be recorded in books which shall be kept for this purpose in the Department of the Treasury, under such regulations as the Secretary of the Treasury shall prescribe, and may furnish to the Department facsimiles of his name, the name of the locality in which his goods are manufactured, or of his registered trademark, and thereupon the Secretary of the Treasury shall cause one or more copies of the same to be transmitted to each collector or other proper officer of customs.'

- Title 15 of the U.S. Code, Section 1116

- '(a) Jurisdiction; service The several courts vested with jurisdiction of civil actions arising under this chapter shall have power to grant injunctions, according to the principles of equity and upon such terms as the court may deem reasonable, to prevent the violation of any right of the registrant of a mark registered in the Patent and Trademark Office or to prevent a violation under subsection (a), (c), or (d) of section 1125 of this title. [...] (b) Transfer of certified copies of court papers The said courts shall have jurisdiction to enforce said injunction, as provided in this chapter, as fully as if the injunction had been granted by the district court in which it is sought to be enforced. The clerk of the court or judge granting the injunction shall, when required to do so by the court before which application to enforce said injunction is made, transfer without delay to said court a certified copy of all papers on file in his office upon which said injunction was granted. (c) Notice to Director It shall be the duty of the clerks of such courts within one month after the filing of any action, suit, or proceeding involving a mark registered under the provisions of this chapter to give notice thereof in writing to the Director setting forth in order so far as known the names and addresses of the litigants and the designating number or numbers of the registration or registrations upon which the action, suit, or proceeding has been brought [...] (d) Civil actions arising out of use of counterfeit marks (1)(A) In the case of a civil action arising under section 1114(1)(a) of this title or section 220506 of title 36 with respect to a

violation that consists of using a counterfeit mark in connection with the sale, offering for sale, or distribution of goods or services, the court may, upon ex parte application, grant an order under subsection (a) of this section pursuant to this subsection providing for the seizure of goods and counterfeit marks involved in such violation and the means of making such marks, and records documenting the manufacture, sale, or receipt of things involved in such violation. (B) As used in this subsection the term 'counterfeit mark' means- (i) a counterfeit of a mark that is registered on the principal register in the United States Patent and Trademark Office for such goods or services sold, offered for sale, or distributed and that is in use, whether or not the person against whom relief is sought knew such mark was so registered; or (ii) a spurious designation that is identical with, or substantially indistinguishable from, a designation as to which the remedies of this chapter are made available by reason of section 220506 of title 36; but such term does not include any mark or designation used on or in connection with goods or services of which the manufacture<sup>1596</sup> or producer was, at the time of the manufacture or production in question authorized to use the mark or designation for the type of goods or services so manufactured or produced, by the holder of the right to use such mark or designation. (2) The court shall not receive an application under this subsection unless the applicant has given such notice of the application as is reasonable under the circumstances to the United States attorney for the judicial district in which such order is sought. Such attorney may participate in the proceedings arising under such application if such proceedings may affect evidence of an offense against the United States. The court may deny such application if the court determines that the public interest in a potential prosecution so requires. (3) The application for an order under this subsection shall- (A) be based on an affidavit or the verified complaint establishing facts sufficient to support the findings of fact and conclusions of law required for such order; and (B) contain the additional information required by paragraph (5) of this subsection to be set forth in such order. (4) The court shall not grant such an application unless— (A) the person obtaining an order under this subsection provides the security determined adequate by the court for the payment of such damages as any person may be entitled to recover as a result of a wrongful seizure or wrongful attempted seizure under this subsection; and (B) the court finds that it clearly appears from specific facts that (i) an order other than an ex parte seizure order is not adequate to achieve the purposes of section 1114 of this title; (ii) the applicant has not publicized the requested seizure; (iii) the applicant is likely to succeed in showing that the person against whom seizure would be ordered used a counterfeit mark in connection with the sale, offering for sale, or distribution of goods or services; (iv) an immediate and irreparable injury will occur if such seizure is not ordered; (v) the matter to be seized will be located at the place identified in the application; (vi) the harm to the applicant of denying the application outweighs the harm to the legitimate interests of the person against whom seizure would be ordered of granting the application; and (vii) the person against whom seizure would be ordered, or persons acting in concert with such person, would destroy, move, hide, or otherwise make such matter inaccessible to the court, if the applicant were to proceed on notice to such person. (5) An order under this subsection shall set forth- (A) the findings of fact and conclusions of law required for the order; (B) a particular description of the matter to be seized, and a description of each place at which such matter is to be seized; (C) the time period, which shall end not later than seven days after the date on which such order is issued, during which the seizure is to be made; (D) the amount of security required to be provided under this subsection; and (E) a date for the hearing required under paragraph (10) of this subsection. (6) The court shall take appropriate action to protect the person against whom an order under this subsection is directed from publicity, by or at the behest of the plaintiff, about such order and any seizure under such order. (7) Any materials seized under this subsection shall be taken into the custody of the court. For seizures made under this section, the court shall enter an appropriate protective order with respect to discovery and use of any records or information that has been seized. The protective order shall provide for appropriate procedures to ensure that confidential, private, proprietary, or privileged information contained in such records is not improperly disclosed or used. (8) An order under this subsection, together with the supporting documents, shall be sealed until the person against whom the order is directed has an opportunity to contest such order, except that any

---

<sup>596</sup> Typographical error in original, presumably 'manufacturer'.



person against whom such order is issued shall have access to such order and supporting documents after the seizure has been carried out. (9) The court shall order that service of a copy of the order under this subsection shall be made by a federal law enforcement officer (such as a United States marshal or an officer or agent of the United States Customs Service, Secret Service, Federal Bureau of Investigation, or Post Office) or may be made by a State or local law enforcement officer, who, upon making service, shall carry out the seizure under the order. The court shall issue orders, when appropriate, to protect the defendant from undue damage from the disclosure of trade secrets or other confidential information during the course of the seizure, including, when appropriate, orders restricting the access of the applicant (or any agent or employee of the applicant) to such secrets or information. (10)(A) The court shall hold a hearing, unless waived by all the parties, on the date set by the court in the order of seizure. That date shall be not sooner than ten days after the order is issued and not later than fifteen days after the order is issued, unless the applicant for the order shows good cause for another date or unless the party against whom such order is directed consents to another date for such hearing. At such hearing the party obtaining the order shall have the burden to prove that the facts supporting findings of fact and conclusions of law necessary to support such order are still in effect. If that party fails to meet that burden, the seizure order shall be dissolved or modified appropriately. (B) In connection with a hearing under this paragraph, the court may make such orders modifying the time limits for discovery under the Rules of Civil Procedure as may be necessary to prevent the frustration of the purposes of such hearing. (11) A person who suffers damage by reason of a wrongful seizure under this subsection has a cause of action against the applicant for the order under which such seizure was made, and shall be entitled to recover such relief as may be appropriate, including damages for lost profits, cost of materials, loss of good will, and punitive damages in instances where the seizure was sought in bad faith, and, unless the court finds extenuating circumstances, to recover a reasonable attorney's fee. The court in its discretion may award prejudgment interest on relief recovered under this paragraph, at an annual interest rate established under section 6621(a)(2) of title 26, commencing on the date of service of the claimant's pleading setting forth the claim under this paragraph and ending on the date such recovery is granted, or for such shorter time as the court deems appropriate.'

- Title 15 of the U.S. Code, Section 1117

- '(a) Profits; damages and costs; attorney fees When a violation of any right of the registrant of a mark registered in the Patent and Trademark Office, a violation under section 1125(a) or (d) of this title, or a willful violation under section 1125(c) of this title, shall have been established in any civil action arising under this chapter, the plaintiff shall be entitled, subject to the provisions of sections 1111 and 1114 of this title, and subject to the principles of equity, to recover (1) defendant's profits, (2) any damages sustained by the plaintiff, and (3) the costs of the action [...] (b) Treble damages for use of counterfeit mark In assessing damages under subsection (a) for any violation of section 1114(1)(a) of this title or section 220506 of title 36, in a case involving use of a counterfeit mark or designation (as defined in section 1116(d) of this title), the court shall, unless the court finds extenuating circumstances, enter judgment for three times such profits or damages, whichever amount is greater, together with a reasonable attorney's fee, if the violation consists of— (1) intentionally using a mark or designation, knowing such mark or designation is a counterfeit mark (as defined in section 1116(d) of this title), in connection with the sale, offering for sale, or distribution of goods or services; or (2) providing goods or services necessary to the commission of a violation specified in paragraph (1), with the intent that the recipient of the goods or services would put the goods or services to use in committing the violation [...] (c) Statutory damages for use of counterfeit marks In a case involving the use of a counterfeit mark (as defined in section 1116(d) of this title) in connection with the sale, offering for sale, or distribution of goods or services, the plaintiff may elect, at any time before final judgment is rendered by the trial court, to recover, instead of actual damages and profits under subsection (a) of this section, an award of statutory damages for any such use in connection with the sale, offering for sale, or distribution of goods or services in the amount of—(1) not less than \$1,000 or more than \$200,000 per counterfeit mark per type of goods or services sold, offered for sale, or distributed, as the court considers just; or (2) if the court finds that the use of the counterfeit mark was willful, not more than \$2,000,000 per counterfeit mark per type of goods or services sold, offered for sale, or distributed, as

the court considers just. (d) Statutory damages for violation of section 1125(d)(1) [...]. (e) Rebuttable presumption of willful violation [...]

- Title 15 of the U.S. Code, Section 1118

- 'In any action arising under this chapter [...] the court may order that all labels, signs, prints, packages, wrappers, receptacles, and advertisements in the possession of the defendant, bearing the registered mark or, in the case of a violation of section 1125(a) of this title or a willful violation under section 1125(c) of this title, the word, term, name, symbol, device, combination thereof, designation, description, or representation that is the subject of the violation, or any reproduction, counterfeit, copy, or colorable imitation thereof, and all plates, molds, matrices, and other means of making the same, shall be delivered up and destroyed. [...]

- Title 18 of the U.S. Code, Section 2318

- '(a)(1) Whoever, in any of the circumstances described in subsection (c), knowingly traffics in-

(A) a counterfeit label or illicit label affixed to, enclosing, or accompanying, or designed to be affixed to, enclose, or accompany— (i) a phonorecord; (ii) a copy of a computer program; (iii) a copy of a motion picture or other audiovisual work; (iv) a copy of a literary work; (v) a copy of a pictorial, graphic, or sculptural work; (vi) a work of visual art; or (vii) documentation or packaging; or (B) counterfeit documentation or packaging, shall be fined under this title or imprisoned for not more than 5 years, or both. [...] (c) The circumstances referred to in subsection (a) of this section are— (1) the offense is committed within the special maritime and territorial jurisdiction of the United States; or within the special aircraft jurisdiction of the United States (as defined in section 46501 of title 49); (2) the mail or a facility of interstate or foreign commerce is used or intended to be used in the commission of the offense; (3) the counterfeit label or illicit label is affixed to, encloses, or accompanies, or is designed to be affixed to, enclose, or accompany- (A) a phonorecord of a copyrighted sound recording or copyrighted musical work; (B) a copy of a copyrighted computer program; (C) a copy of a copyrighted motion picture or other audiovisual work; (D) a copy of a literary work; (E) a copy of a pictorial, graphic, or sculptural work; (F) a work of visual art; or (G) copyrighted documentation or packaging; or

(4) the counterfeited documentation or packaging is copyrighted. (d) FORFEITURE AND DESTRUCTION OF PROPERTY; RESTITUTION.-Forfeiture, destruction, and restitution relating to this section shall be subject to section 2323, to the extent provided in that section, in addition to any other similar remedies provided by law. (e) CIVIL REMEDIES.— (1) IN GENERAL.—Any copyright owner who is injured, or is threatened with injury, by a violation of subsection (a) may bring a civil action in an appropriate United States district court. [...]

- Title 18 of the U.S. Code, Section 2319

- '(a) Any person who violates section 506(a) (relating to criminal offenses) of title 17 shall be punished as provided in subsections (b), (c), and (d) and such penalties shall be in addition to any other provisions of title 17 or any other law. (b) Any person who commits an offense under section 506(a)(1)(A) of title 17— (1) shall be imprisoned not more than 5 years, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution, including by electronic means, during any 180-day period, of at least 10 copies or phonorecords, of 1 or more copyrighted works, which have a total retail value of more than \$2,500; (2) shall be imprisoned not more than 10 years, or fined in the amount set forth in this title, or both, if the offense is a felony and is a second or subsequent offense under subsection (a); and (3) shall be imprisoned not more than 1 year, or fined in the amount set forth in this title, or both, in any other case. (c) Any person who commits an offense under section 506(a)(1)(B) of title 17— (1) shall be imprisoned not more than 3 years, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution of 10 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of \$2,500 or more; (2) shall be imprisoned not more than 6 years, or fined in the amount set forth in this title, or both, if the offense is a felony and is a second or subsequent offense under subsection (a); and (3) shall be imprisoned not more than 1 year, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than \$1,000. (d)

Any person who commits an offense under section 506(a)(1)(C) of title 17— (1) shall be imprisoned not more than 3 years, fined under this title, or both; (2) shall be imprisoned not more than 5 years, fined under this title, or both, if the offense was committed for purposes of commercial advantage or private financial gain; (3) shall be imprisoned not more than 6 years, fined under this title, or both, if the offense is a felony and is a second or subsequent offense under subsection (a); and (4) shall be imprisoned not more than 10 years, fined under this title, or both, if the offense is a felony and is a second or subsequent offense under paragraph (2). (e)(1) During preparation of the presentence report pursuant to Rule 32(c) of the Federal Rules of Criminal Procedure, victims of the offense shall be permitted to submit, and the probation officer shall receive, a victim impact statement that identifies the victim of the offense and the extent and scope of the injury and loss suffered by the victim, including the estimated economic impact of the offense on that victim. (2) Persons permitted to submit victim impact statements shall include— (A) producers and sellers of legitimate works affected by conduct involved in the offense; (B) holders of intellectual property rights in such works; and (C) the legal representatives of such producers, sellers, and holders. (f) As used in this section— (1) the terms ‘phonorecord’ and ‘copies’ have, respectively, the meanings set forth in section 101 (relating to definitions) of title 17; (2) the terms ‘reproduction’ and ‘distribution’ refer to the exclusive rights of a copyright owner under clauses (1) and (3) respectively of section 106 (relating to exclusive rights in copyrighted works), as limited by sections 107 through 122, of title 17; (3) the term ‘financial gain’ has the meaning given the term in section 101 of title 17; and (4) the term ‘work being prepared for commercial distribution’ has the meaning given the term in section 506(a) of title 17.’

▪ Title 18 of the U.S. Code, Section 2320

- ‘(a) OFFENSES.—Whoever intentionally— (1) traffics in goods or services and knowingly uses a counterfeit mark on or in connection with such goods or services, (2) traffics in labels, patches, stickers, wrappers, badges, emblems, medallions, charms, boxes, containers, cans, cases, hangtags, documentation, or packaging of any type or nature, knowing that a counterfeit mark has been applied thereto, the use of which is likely to cause confusion, to cause mistake, or to deceive, (3) traffics in goods or services knowing that such good or service is a counterfeit military good or service the use, malfunction, or failure of which is likely to cause serious bodily injury or death, the disclosure of classified information, impairment of combat operations, or other significant harm to a combat operation, a member of the Armed Forces, or to national security, or (4) traffics in a counterfeit drug, or attempts or conspires to violate any of paragraphs (1) through (4) shall be punished as provided in subsection (b). (b) PENALTIES.— (1) IN GENERAL.—Whoever commits an offense under subsection (a)— (A) if an individual, shall be fined not more than \$2,000,000 or imprisoned not more than 10 years, or both, and, if a person other than an individual, shall be fined not more than \$5,000,000; and (B) for a second or subsequent offense under subsection (a), if an individual, shall be fined not more than \$5,000,000 or imprisoned not more than 20 years, or both, and if other than an individual, shall be fined not more than \$15,000,000. [...] (c) FORFEITURE AND DESTRUCTION OF PROPERTY; RESTITUTION.— Forfeiture, destruction, and restitution relating to this section shall be subject to section 2323, to the extent provided in that section, in addition to any other similar remedies provided by law. (d) DEFENSES.—All defenses, affirmative defenses, and limitations on remedies that would be applicable in an action under the Lanham Act shall be applicable in a prosecution under this section. In a prosecution under this section, the defendant shall have the burden of proof, by a preponderance of the evidence, of any such affirmative defense. (e) PRESENTENCE REPORT.—(1) During preparation of the presentence report pursuant to Rule 32(c) of the Federal Rules of Criminal Procedure, victims of the offense shall be permitted to submit, and the probation officer shall receive, a victim impact statement that identifies the victim of the offense and the extent and scope of the injury and loss suffered by the victim, including the estimated economic impact of the offense on that victim. [...]

▪ Title 18 of the U.S. Code, Section 2323

- ‘(a) CIVIL FORFEITURE.— (1) PROPERTY SUBJECT TO FORFEITURE.—The following property is subject to forfeiture to the United States Government: (A) Any article, the making or trafficking of which is, prohibited under section 506 of title 17, or section 2318, 2319, 2319A, 2319B, or 2320, or chapter 90, of this title. (B) Any property used, or intended to be used, in any manner or part to commit or facilitate the commission of an offense referred to in subparagraph (A). (C) Any property constituting or derived

from any proceeds obtained directly or indirectly as a result of the commission of an offense referred to in subparagraph (A). (2) PROCEDURES.—The provisions of chapter 46 relating to civil forfeitures shall extend to any seizure or civil forfeiture under this section. For seizures made under this section, the court shall enter an appropriate protective order with respect to discovery and use of any records or information that has been seized. The protective order shall provide for appropriate procedures to ensure that confidential, private, proprietary, or privileged information contained in such records is not improperly disclosed or used. At the conclusion of the forfeiture proceedings, unless otherwise requested by an agency of the United States, the court shall order that any property forfeited under paragraph (1) be destroyed, or otherwise disposed of according to law. (b) CRIMINAL FORFEITURE.— (1) PROPERTY SUBJECT TO FORFEITURE.—The court, in imposing sentence on a person convicted of an [...] (c) RESTITUTION.—When a person is convicted of an offense under section 506 of title 17 or section 2318, 2319, 2319A, 2319B, or 2320, or chapter 90, of this title, the court, pursuant to sections 3556, 3663A, and 3664 of this title, shall order the person to pay restitution to any victim of the offense as an offense against property referred to in section 3663A(c)(1)(A)(ii) of this title [...]

- Title 19 of the U.S. Code, Section 1526

- '(a) Importation prohibited Except as provided in subsection (d) of this section, it shall be unlawful to import into the United States any merchandise of foreign manufacture if such merchandise, or the label, sign, print, package, wrapper, or receptacle, bears a trademark owned by a citizen of, or by a corporation or association created or organized within, the United States, and registered in the Patent and Trademark Office by a person domiciled in the United States, under the provisions of sections 81 to 109 of title 15, and if a copy of the certificate of registration of such trademark is filed with the Secretary of the Treasury, in the manner provided in section 106 of said title 15, unless written consent of the owner of such trademark is produced at the time of making entry. (b) Seizure and forfeiture Any such merchandise imported into the United States in violation of the provisions of this section shall be subject to seizure and forfeiture for violation of the customs laws. (c) Injunction and damages Any person dealing in any such merchandise may be enjoined from dealing therein within the United States or may be required to export or destroy such merchandise or to remove or obliterate such trademark and shall be liable for the same damages and profits provided for wrongful use of a trade-mark, under the provisions of sections 81 to 109 of title 15. (d) Exemptions; publication in Federal Register; forfeitures; rules and regulations [...]. (e) Merchandise bearing counterfeit mark; seizure and forfeiture; disposition of seized goods Any such merchandise bearing a counterfeit mark (within the meaning of section 1127 of title 15) imported into the United States in violation of the provisions of section 1124 of title 15, shall be seized and, in the absence of the written consent of the trademark owner, forfeited for violations of the customs laws. Upon seizure of such merchandise, the Secretary shall notify the owner of the trademark, and shall, after forfeiture, destroy the merchandise. Alternatively, if the merchandise is not unsafe or a hazard to health, and the Secretary has the consent of the trademark owner, the Secretary may obliterate the trademark where feasible and dispose of the goods seized— [...] (f) Civil penalties (1) Any person who directs, assists financially or otherwise, or aids and abets the importation of merchandise for sale or public distribution that is seized under subsection (e) of this section shall be subject to a civil fine. (2) For the first such seizure, the fine shall be not more than the value that the merchandise would have had if it were genuine, according to the manufacturer's suggested retail price, determined under regulations promulgated by the Secretary. (3) For the second seizure and thereafter, the fine shall be not more than twice the value that the merchandise would have had if it were genuine, as determined under regulations promulgated by the Secretary. (4) The imposition of a fine under this subsection shall be within the discretion of the Customs Service, and shall be in addition to any other civil or criminal penalty or other remedy authorized by law.'

- Title 17 of the U.S. Code, Section 501

- '(a) Anyone who violates any of the exclusive rights of the copyright owner [...], or who imports copies or phonorecords into the United States in violation of section 602, is an infringer of the copyright or right of the author, as the case may be. [...]. (b) The legal or beneficial owner of an exclusive right under a copyright is entitled, subject to the requirements of section 411, to institute an action for any infringement of that particular right committed while he or she is the owner of it. [...]

- Title 17 of the U.S. Code, Section 502 et seq.
  - '(a) Any court having jurisdiction of a civil action arising under this title may, subject to the provisions of section 1498 of title 28, grant temporary and final injunctions on such terms as it may deem reasonable to prevent or restrain infringement of a copyright. (b) Any such injunction may be served anywhere in the United States on the person enjoined; [...]'
- Title 17 of the U.S. Code, Section 603
  - '(a) The Secretary of the Treasury and the United States Postal Service shall separately or jointly make regulations for the enforcement of the provisions of this title prohibiting importation. (b) These regulations may require, as a condition for the exclusion of articles under section 602— (1) that the person seeking exclusion obtain a court order enjoining importation of the articles; or (2) that the person seeking exclusion furnish proof, of a specified nature and in accordance with prescribed procedures, that the copyright in which such person claims an interest is valid and that the importation would violate the prohibition in section 602; the person seeking exclusion may also be required to post a surety bond for any injury that may result if the detention or exclusion of the articles proves to be unjustified. (c) Articles imported in violation of the importation prohibitions of this title are subject to seizure and forfeiture in the same manner as property imported in violation of the customs revenue laws. Forfeited articles shall be destroyed as directed by the Secretary of the Treasury or the court, as the case may be.'
- Title 35 of the United States Code, Section 101
  - 'Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.'
- Title 35 of the United States Code, Section 171
  - '(a) IN GENERAL.—Whoever invents any new, original and ornamental design for an article of manufacture may obtain a patent therefor, subject to the conditions and requirements of this title. (b) APPLICABILITY OF THIS TITLE.—The provisions of this title relating to patents for inventions shall apply to patents for designs, except as otherwise provided. (c) FILING DATE.—The filing date of an application for patent for design shall be the date on which the specification as prescribed by section 112 and any required drawings are filed [...]'
- Title 19 of the U.S. Code, Section 1337
  - '(a) Unlawful activities; covered industries; definitions (1) Subject to paragraph (2), the following are unlawful, and when found by the Commission to exist shall be dealt with, in addition to any other provision of law, as provided in this section: (A) Unfair methods of competition and unfair acts in the importation of articles [...]. (B) The importation into the United States, the sale for importation, or the sale within the United States after importation by the owner, importer, or consignee, of articles that— (i) infringe a valid and enforceable United States patent or a valid and enforceable United States copyright registered under title 17; or (ii) are made, produced, processed, or mined under, or by means of, a process covered by the claims of a valid and enforceable United States patent. (C) The importation into the United States, the sale for importation, or the sale within the United States after importation by the owner, importer, or consignee, of articles that infringe a valid and enforceable United States trademark registered under the Trademark Act of 1946 [15 U.S.C. 1051 et seq.]. (D) The importation into the United States, the sale for importation, or the sale within the United States after importation by the owner, importer, or consignee, of a semiconductor chip product in a manner that constitutes infringement of a mask work registered under chapter 9 of title 17. (E) The importation into the United States, the sale for importation, or the sale within the United States after importation by the owner, importer, or consigner, of an article that constitutes infringement of the exclusive rights in a design protected under chapter 13 of title 17 [...]'
- Title 41 of the U.S. Code, Section 6503



- '(a) APPLICABLE BREACH OR VIOLATION.—This section applies in case of breach or violation of a representation or stipulation included in a contract under section 6502 of this title. (b) LIQUIDATED DAMAGES.—In addition to damages for any other breach of the contract, the party responsible for a breach or violation described in subsection (a) is liable to the Federal Government for the following liquidated damages: [...] (c) CANCELLATION AND ALTERNATIVE COMPLETION.—In addition to the Federal Government being entitled to damages described in subsection (b), the agency of the United States that made the contract may cancel the contract and make open-market purchases or make other contracts for the completion of the original contract, charging any additional cost to the original contractor [...]
- Title 15 of the U.S. Code, Section 6801
  - '(a) Privacy obligation policy It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information. (b) Financial institutions safeguards In furtherance of the policy in subsection (a) of this section, each agency or authority described in section 6805(a) of this title, other than the Bureau of Consumer Financial Protection, shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards— (1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.'
- Title 15 of the U.S. Code, Section 6802
  - '(a) Notice requirements Except as otherwise provided in this subchapter, a financial institution may not, directly or through any affiliate, disclose to a nonaffiliated third party any nonpublic personal information, unless such financial institution provides or has provided to the consumer a notice that complies with section 6803 of this title. (b) Opt out (1) In general A financial institution may not disclose nonpublic personal information to a nonaffiliated third party [...] (e) General exceptions Subsections (a) and (b) shall not prohibit the disclosure of nonpublic personal information— (1) as necessary to effect, administer, or enforce a transaction requested or authorized by the consumer, or in connection with— (A) servicing or processing a financial product or service requested or authorized by the consumer; (B) maintaining or servicing the consumer's account with the financial institution, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity; or (C) a proposed or actual securitization, secondary market sale (including sales of servicing rights), or similar transaction related to a transaction of the consumer; (2) with the consent or at the direction of the consumer; (3)(A) to protect the confidentiality or security of the financial institution's records pertaining to the consumer, the service or product, or the transaction therein; (B) to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability; (C) for required institutional risk control, or for resolving customer disputes or inquiries; (D) to persons holding a legal or beneficial interest relating to the consumer; or (E) to persons acting in a fiduciary or representative capacity on behalf of the consumer; (4) to provide information to insurance rate advisory organizations, guaranty funds or agencies, applicable rating agencies of the financial institution, persons assessing the institution's compliance with industry standards, and the institution's attorneys, accountants, and auditors; (5) to the extent specifically permitted or required under other provisions of law and in accordance with the Right to Financial Privacy Act of 1978 [12 U.S.C. 3401 et seq.], to law enforcement agencies (including the Bureau of Consumer Financial Protection<sup>597</sup> a Federal functional regulator, the Secretary of the Treasury with respect to subchapter II of chapter 53 of title 31, and chapter 2 of title I of Public Law 91–508 (12 U.S.C. 1951–1959), a State insurance authority, or the Federal Trade Commission), self-regulatory organizations, or for an investigation on a matter related to public safety; (6)(A) to a consumer reporting agency in accordance with the Fair Credit Reporting Act [15 U.S.C. 1681 et seq.], or (B) from a consumer report reported by a consumer reporting agency; (7) in connection with a proposed or actual sale, merger, transfer, or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal information concerns solely consumers of such business

<sup>597</sup> Probable typographical error in original text. Probably should be followed by a comma.

or unit; or (8) to comply with Federal, State, or local laws, rules, and other applicable legal requirements; to comply with a properly authorized civil, criminal, or regulatory investigation or subpoena or summons by Federal, State, or local authorities; or to respond to judicial process or government regulatory authorities having jurisdiction over the financial institution for examination, compliance, or other purposes as authorized by law.'



## LITERATURE AND SOURCES



## ■ Literature

- French Charter for the fight against the sale of counterfeit goods on the internet between intellectual property rightholders and e-commerce platforms.
- Sirinelli, P., 'Presentation of the French charter on the fight against cyber-counterfeiting of December 16, 2009', WIPO, 2011.
- Business Action to Stop Counterfeiting and Piracy (BASCAP), 'Roles and Responsibilities of intermediaries: Fighting counterfeiting and piracy in the supply chain', *Executive Summary*, March 2015.
- Hyeans, A. (ONDRP researcher) and Guillaneuf, J. (statistician at the ONDRP), 'Counterfeiting in France: Elements for measuring and analysing the problem', June 2011.
- Barbier, J-B., 'Building Respect for IP Online: The French Preventive Tools Against Counterfeiting', *China Intellectual Property*, 2015.
- Castro, D., 'Benefits and Limitations of Industry Self-Regulation for Online Behavioral Advertising', ITIF, December 2011.
- Szoka, B. and Marcus, A., 'The Next Digital Decade. Essays on the Future of the Internet.', Washington: TechFreedom, 2010.
- PriceMinister-Rakuten 2014 balance sheet on the fight against counterfeiting ('Bilan PriceMinister-Rakuten sur la lutte anti-contrefaçon 2014').
- *Signature d'une charte pour lutter contre la contrefaçon sur internet*, Portail du Gouvernement Français, 2009.
- Bird, K., 'Fight against the online sale of counterfeits continues in France', [www.cosmeticsdesign-europe.com](http://www.cosmeticsdesign-europe.com), 2010.
- Rees, M., 'Marques et plateformes signent une charte anti-contrefaçon sans eBay ni Amazon', [www.nextimpact.com](http://www.nextimpact.com), 2009.
- Hinze, G., 'EU Law does not require ISP to hand over customers' identity data in alleged filesharing case', Electronic Frontier Foundation, 2008.
- 'Anti-Counterfeiting Trade Agreement — BEUC Position', BEUC, 2012.
- Letter addressed to Permanent Representation in Europe by BEUC on the Enforcement of Intellectual Property Rights, BEUC, 2014.
- Charter for the Fight Against the Sale of Counterfeit Goods on the Internet. Evaluation of the experimentation process. Application assessment. (*Charte de lutte contre la contrefaçon sur Internet. Evaluation du processus d'expérimentation. Bilan d'application*), INPI, 2012.
- Minutes of the meeting of signatories. French charters on the fight against internet counterfeiting. 22 November 2012 at 2:30 p.m. at the INPI (*Compte-rendu de la réunion des signataires. Chartes françaises de lutte contre la contrefaçon sur Internet. 22 novembre 2012 à 14h30 à l'INPI*), INPI, 2012.
- Usai, A., 'The freedom to conduct a business in the EU, its limitations and its role in the European legal order: a new engine for deeper and stronger economic, social and political integration', *German Law Journal*, 2013.
- Memorandum of Understanding of the European Commission on the Sale of Counterfeit Goods of 4 May 2011.
- Report of the Commission to the European Parliament and the Council on the Functioning of the Memorandum of Understanding of the European Commission on the Sale of Counterfeit Goods of 18 April 2013.
- Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC, of the Article 29 Working Party.
- Working Document on Blacklists, of the Article 29 Working Party.

- French Charter for the Fight against the Sale of Counterfeit Goods on the Internet between Intellectual Property Rightholders and Small Ads Platforms (*Charte de lutte contre la contrefaçon sur Internet entre titulaires de droits de propriété industrielle et plateformes de petites annonces*).
- French Charter for the Fight against the Sale of Counterfeit Goods — Rightholders, Associations representing Rightholders and Postal Operators (*Charte de lutte contre la contrefaçon — Titulaires de droits, associations représentant des titulaires de droits et opérateurs postaux*).
- Danish Ministry of Culture, 2012, 'The Danish Telecommunications Industry, TI: Code of Conduct for Management of Rulings on Blockings Related to Infringements of Rights'.
- Fredenslund, María, Kluwercopyrightblog, 2014, 'Code of Conduct on Website Blocking'.
- Loek Essers, 2012, 'Danish ISPs Agree to Move in Concert to Block Rights-infringing Content', CIO.
- Out-Law.com, 2012, 'All Danish ISPs will Block Content on Single Court Order under Proposed Code'.
- The Legislative Council Secretariat, 2014, 'Creative Industries in Denmark'.
- Berkeley University, 2014, 'Site-blocking Orders in the EU: Justifications and Feasibility'.
- Teleindustrien, 2014, 'Code of Conduct of the Telecommunications Industry Association in Denmark (Teleindustrien)'.
- Eurativ, 2015, 'Denmark Partners with Tech Companies to take on Piracy'.
- Danish Ministry of Culture, 2015, 'Code of Conduct to Promote Lawful Behavior on the Internet. Declaration of Intent'.
- Danish Ministry of Culture, 2015, Press Release 'Broad Support for Joint Action for a Legal and Safe Internet in the Field of Copyright'.
- European Commission, 2001, Press Release 'Commission Welcomes Adoption of the Directive on Copyright in the Information Society by the Council'.
- Torrentfreak.com, 27 March 2015, 'Popular Torrent and Streaming Sites Blocked in Denmark'.
- Torrentfreak.com, 11 May 2015, 'Google, Microsoft, Mastercard & ISPS Sign Anti-piracy Agreement'.
- Maria Fredenslund, 24 October 2014, 'Denmark: Code of Conduct on Website Blocking'.
- Danish Ministry of Culture, 20 June 2012, 'Initiatives to Boost the Creation of Legal Content on the Internet'.
- Mette Bom and Mikala Poulsen, 'Share with Care. The Guidebook of Digital User Behavior (2014)'.
- Martin Husberg, 2015, 'Blocking Injunctions Rerequisites. The Balancing of Rights and other Aspects of Blocking Injunctions Towards Intermediaries'. Graduate Thesis, Master of Laws program, Faculty of Law, Lund University.
- Lukas Feiler, 2012, TTLF Working Papers No 13, 'Website Blocking Injunctions under EU and U.S. Copyright Law'.
- Lukas Feiler, 2012, TTLF Working Papers No 13.
- Maria Fredenslund, 23 January 2015, Kluwer Copyright Blog, 'Danish Court Issues Website Blocking Ruling Concerning the Illegal Distribution of Replica Products'.

- Lukas Feiler, 2012, TTLF Working Papers No 13, 'Website Blocking Injunctions under EU and U.S. Copyright Law – Slow Death of the Global Internet or Emergence of the Rule of National Copyright Law?' Stanford-Vienna Transatlantic Technology Law Forum
- Graeme B. Dinwoodie, 'Secondary Liability for Online Trademark Infringement: The International Landscape'.
- Hjördis Halldórsdóttir, Stockholm Institute for Scandinavian Law, 'Enforcement of Copyright – A Reflection of Injunctions in the Information Society'.
- Pekka Savola, 2014, 'Proportionality of Website Blocking: Internet Connectivity Providers as Copyright Enforcers'.
- Søren Sandfeld Jakbosen, IRIS 2010-8:1/24, Denmark 'Danish Supreme Court Upholds Injunction to Block the Pirate Bay'.
- Mette Bom og Mikala Poulsen, Share with Care. 'Evaluation of the Information Effort Share with Care', 2014.
- Google & PRS for Music, 'The Six Business Models for Copyright Infringement', 2012.
- Code of Ethics of the Austrian advertising industry.
- Rules of Procedure of the Werberat.
- Statutes of the SASR.
- 'Österreichischer Werberat-Europas grösstes Entscheidungsgremium gewählt' (2011), Wirtschaftskammer Österreich.
- 'Branchen — Info-Spezial' (2010), Wirtschaftskammer Österreich.
- 'ÖWR-Qualitätsoffensive' (2014), Werberat.
- 'Umfieldwerbung' (2014), Werberat.
- 'Werberat ruft zu Werbeverzicht auf Online-Seiten mit illegalem Inhalt auf' (2014), Werberat.
- Göschl, Monique A. 'Ad-Industry Self-Regulation in Austria: a European Best Practice' (2014), Verein Anti Piraterie.
- Sery-Froschauer and Müller. 'No advertising on internet sites with illegal content' (2012), Trade Association Film & Music.
- 'ICC Policy statement: Safeguarding against the misplacement of digital advertising' (2014), International Chamber of Commerce.
- 'Behind the cyberlocker door: A report on how shadowy Cyberlocker businesses use credit card companies to make millions', Digital citizens alliance and NetNames.
- 'The six business models for copyright infringement' (2012), PRS for music and Google.
- 'The revenue sources for websites making available copyright content without consent in the EU' (2015), INCOPRO.
- 'USC Annenberg lab ad transparency report' (2013), USC Annenberg Innovation Lab.
- Castro, Daniel. 'Benefits and Limitations of Industry Self-Regulation for Online Behavioral Advertising' (December 2011), ITIF.
- Weatherley MP, Mike. 'Follow the money: financial options to assist in the battle against online IP piracy' (2014).
- Stamhuis, E.F., 'Criminal law on cyber-crime in the Netherlands; general part and country report section I\*', Preparatory Colloquium, Section I - Information Society and Penal Law, Verona (Italy), 28-30 November 2012.
- Brousseau, E., Meryem Marzouki, Cécile Méadel. 'Governance, Regulation and Powers on the Internet', March 2015.
- Milica Antic (SOLV Lawyers, Amsterdam), Arend Lagemaat (DLA Piper Lawyers, Amsterdam Office), Bart van der Sloot (Institute for Information Law, Law Faculty, University of Amsterdam) and Maarten

van Stekelenburg (DLA Piper Lawyers, Amsterdam Office). LIDC Congress in Oxford– Dutch National Report, 2011.

- Olivera Medenica & Kaiser Wahab 'Does Liability enhance credibility? Lessons from the DMCA applies to online Defamation. Article formed the basis of the authors' presentation for a panel at Wikimania 2006, held at the Harvard Law School in August, 2006.
- 'DRILLSTER Terms of Service' (information extracted from <https://www.drillster.com/info/es/tos> used on 3 July 2015).
- Feeley, M. J., 'EU Internet Regulation Policy: The Rise of Self-Regulation', December 1999.
- 'General Terms and Conditions of SAVVIE B.V' (information extracted from <https://www.savvie.eu/terms-conditions/> on 3 July 2015).
- Andy, 'ISP Told to Take Down 'Pirate Site' or Face Money Laundering Issues' (information extracted from <https://torrentfreak.com/isp-told-to-take-down-pirate-site-or-face-money-laundering-action-131220/> on 20 December, 2013)
- Schellekens, M., 'Liability of Internet Intermediaries', 2011.
- 'National CyberSecurity Strategy 2', National Coordinator for Security and Counterterrorism.
- Janssen E., 'Netherlands, Dutch Code for Notice-and-Take-Down', Institute for Information Law (IvIR), University of Amsterdam (<http://merlin.obs.coe.int/iris/2009/1/article28.en.html>), 2009.
- 'New Dutch Notice-and-Take-Down Code raises questions', Digital Civil rights in Europe, number 6.20, (<http://history.edri.org/edri-gram/number6.20/notice-take-down-netherlands>), October 2008.
- De Bruin M.W., 'Notice and Takedown in Dutch Criminal Procedure - A revision of the proposed regime', Master Thesis for the Master Law and Technology Tilburg University, Faculty of Law (<http://arno.uvt.nl/show.cgi?fid=126921>).
- Oerlemans J.J., 'OerlemansBlog – Blog about cybercrime and privacy' (<http://oerlemansblog weblog.leidenuniv.nl/2013/07/18/filtering-the-Internet-for-law-enforcement-purposes/>), 18 July 2013.
- 'Question B: 'To what extent should on-line Intermediaries (such as ISPs and operators of online market places) be responsible for the control or prohibition of unfair competitive practices (in particular sales of products contrary to the law) carried out on their systems?', LIDC Congress in Oxford 2011 - 22-24 September 2011 Dutch National Report (<http://www.ligue.org/uploads/documents/rapportBNL.pdf>), 2011.
- 'SIDN Notice and Take Down Procedure' (information extracted from [https://www.sidn.nl/a/nl-domain-name/complaining-about-the-content-of-a-website?language\\_id=2](https://www.sidn.nl/a/nl-domain-name/complaining-about-the-content-of-a-website?language_id=2) on 3 July 2015).
- Prof. Dr. Gerald Spindler, 'Study on the liability of Internet Intermediaries', 12 November 2007.
- Filippetti A. and Archibugi D., *The Globalization of the Intellectual Property Rights*, The Global Handbook of Science, Technology and Innovation, Wiley Oxford, 2015.
- *The next digital decade. Essays on the future of the internet*, edited by Szoka B. and Marcus A., 2010 by TechFreedom, Washington, D.C.
- Manta I., *The Puzzle of Criminal Sanctions for Intellectual Property Infringement*, September 2010, updated May 2011.
- 'WETRANSFER Notice and Take Down Policy' (<https://www.wetransfer.com/documents/ntd.pdf>), 2013.
- Annexure B- Music Rights Australia submission November 2012.
- 'BREIN review 2014 and preview 2015', (<http://www.anti-piracy.nl/artikelen.php?id=26>), 2015.
- 'BREIN Yearbook', 2011.
- BREIN, letter on the effectiveness of the NTD code since its implementation, July 2015.
- Seng D., *Comparative Analysis Of The National Approaches To The Liability Of Internet Intermediaries*, (Preliminary Version), Section 73, 2010.
- Naylor D., 'European Framework for 'notice and take down' procedure', February 2012.

- 'DMCA Notice-and-Takedown Processes: List of Good, Bad and Situational Practices', Department of Commerce DMCA Multistakeholder Forum.
- eBay Verified Rights Owner (VeRO) takedown requests, visited on 3 July 2015.
- Smith E., 'Lord of the Files: International Secondary Liability for Internet Service Providers', 2011.
- Piper, DLA., 'EU study on the Legal analysis of a Single Market for the Information Society. New rules for a new age?. Liability of online Intermediaries', November 2009.
- Lloyd I., 'Information Technology Law Oct 2014'. Oxford University Press.
- LAYAR Notice and Takedown Code, (information extracted from <https://www.layar.com/legal/notice-takedown/> on 3 July 2015), 2001.
- 'Notice-And-Take-Down Code of Conduct', version 1.04, 9 October 2008.
- Upper House of the Dutch Parliament, '25 892 – Rules for the protection of personal data (Personal Data Protection Act)' (*Wet Bescherming Persoonsgegevens*), Session 1999-2000 No. 92, 1999.
- Hugenholtz P. B., 'Chronicle of the Netherlands Dutch copyright law, 2001-2010', P.
- DTSG UK Good Practice Principles for the Trading of Digital Display Advertising (December 2013).
- 'Verification Submission Form' (9 June 2015), DTSG.
- 'Registration Form' (9 June 2015), DTSG.
- 'Use of verification provider's name and logo' (August 2015), DTSG.
- 'DTSG FAQs' (13 August 2014), DTSG.
- 'Sample Preliminary Agreement' (13 September 2013), DTSG.
- 'Minimising the Risk of Digital Display Advertising Misplacement – A JICWEBS Progress Report' (24 February 2015), JICWEBS.
- '2014 Full Year Digital Adspend Results' (9 April 2015), JICWEBS.
- 'Subscribing information' (27 November 2015), JICWEBS.
- 'City of London Police call on advertising and brand sectors to help tackle cyber-crime' (28 April 2014), PIPCU.
- 'IASH Code of Conduct, V.11.2' (June 2011), IASH.
- 'The Guide to Display Advertising', IAB UK.
- 'Display Trading Buyers Guide', IAB UK.
- 'Factsheet: Copyright and Brand Safety' (September 2015), IAB UK.
- 'Factsheet: Minimising the risk of Advertising Misplacement' (December 2013), IAB UK.
- 'The IAB Believes...in BRAND SAFETY online' (17 August 2015), IAB UK.
- 'DTSG report shows progress of digital ad industry in improving brand safety through JICWEBS' (24 February 2015), IAB UK.
- 'Digital Policy Guide', IAB UK.
- '73 % drop in top UK advertising on illegal sites' (12 August, 2015), IAB UK.
- 'IAB submission: Liberal Democrat Party Creative Industries Review' (October 2015), IAB UK.
- 'DTSG report shows progress of digital ad industry in improving brand safety through JICWEBS' (24 February 2015), IAB UK.
- 'Digital Trading Standards Group agrees new principles for brand safety' (18 April, 2012), ABC.
- 'Guide To Verification. For the DTSG UK Good Practice Principles for the Trading of Digital Display Advertising' (January 2014), ABC.
- 'The value of content verification tools' (28 August 2012), ABC.
- 'Content Verification Certification Programme – Promoting a safer environment for online advertising' (April 2015), ABC.

- 'Content Verification (CV) Technology Q&A Sheet', ABC.
- 'Guidance on the rules on use of cookies and similar technologies' (May 2012), UK Information Commissioner's Office.
- 'UK Police Intellectual Property Crime Unit goes global in its pursuit of illegal websites' – (9 December 2013), BPI.
- 'City of London Police call on advertising and brand sector to help tackle cyber crime' (31 March 2014), IFPI.
- 'Operation Creative sees 73 per cent drop in top UK advertising on illegal sites' (12 August 2015), City of London Police.
- 'Operation Creative and IWL' (3 August 2015), City of London Police.
- Omar Oakes. 'IAB declares five biggest issues in digital advertising' (13 August 2015), Campaign Live Article.
- 'ICC Policy statement: Safeguarding against the misplacement of digital advertising' (2014), ICC.
- 'The application of the EU Charter of Fundamental Rights in the UK: a state of confusion', (26 March 2014), House of Commons' European Scrutiny Committee, Forty-third Report of Session 2013-14.
- Montanaro Kristina. (IACC). 'Executive Summary October 2012. IACC Payment Processor Portal Program: First Year Statistical Review'.
- Espinel, V. 'Intellectual property Spotlight', (July/August 2011).
- Espinel, Victoria. 'Working together to Stop internet Piracy', (7 July 2011).
- Barchiese, Robert C. on behalf of the International AntiCounterfeiting Coalition 'The Role of Voluntary Agreements in the U.S. Intellectual Property System', (September, 2013).
- U.S. Copyright Office Summary 'The Digital Millennium Copyright Act of 1998', (December 1998).
- Castro, Daniel '*PIPA / SOPA*. Responding to Critics and Finding a Path Forward', The Information Technology & Innovation Foundation, (December 2011).
- Testimony of Denise Yee, Visa Inc. 'Hearing on Targeting Websites Dedicated to Stealing American Intellectual Property'. The United States Senate Committee on the Judiciary. (February 2011).
- Bridy, Annemarie. 'Internet Payment Blockades'. University of Idaho College of Law; Stanford University Center for Internet and Society (February 2015).
- Future of Music Coalition, 'Payment Processors Best Practices for Online Copyright Infringement: What it Means for Musicians', (October 2011).
- Europol, 'Infringements of Intellectual Rights on the Internet' (November 2014).
- Pallante, Maria A. 'Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites, Part I', (March 2011).
- International AntiCounterfeiting Coalition, 'IACC 2013 Highlights'.
- International AntiCounterfeiting Coalition, 'IACC: 2014 Highlights & 2015 Initiatives' (February 2015).
- International AntiCounterfeiting Coalition, 'IACC Payment Processor Initiative (RogueBlock)' (March 2015).
- International AntiCounterfeiting Coalition, 'Public Awareness Campaign, Consumer Education Initiative with The DC Crime Museum' (April, 2015).
- U.S. Intellectual Property Enforcement Coordinator, 'Annual Report on Intellectual Property Enforcement', (March 2012).
- **Case-Law**
  - Ruling issued on 12 July 2011 by the CJEU in Case C-324/09, L'Oréal-eBay, EU:C:2011:474.
  - Ruling issued on 29 January 2008 by the CJEU in Case C-275/06, Promusicae, EU:C:2008:54.



- Ruling issued on 14 May 1974 by the CJEU in Case C-4/73, *Nold KG v Commission*, EU:C:1974:51.
- Ruling issued on 8 October 1986 by the CJEU in Case C-234/85, *Keller*, EU:C:1986:377.
- Ruling issued on 30 July 1996 by the CJEU Case C-84/95, *Bosphorus v Minister for Transport, Energy and Communications and Others*, EU:C:1996:312.
- Ruling issued on 4 June 2009 by the CJEU in Case C-8/08, *T-Mobile Netherlands and Others*, EU:C:2009:343.
- Ruling issued by the CJEU under joined Cases C-89/85, C-104/85, C-114/85, C-116/85, C-117/85 and C-125/85 to C-129/85, *Ahlström Osakeyhtiö and Others v Commission*, EU:C:1988:258.
- Ruling issued on 13 February 2014 by the CJEU in Case C-466/12, *Svensson and Others*, EU:C:2014:76.
- Ruling issued on 30 July 1996 by the CJEU in Case C-84/95, *Bosphorus*, EU:C:1996:312.
- French Constitutional Council Decision No 2000-436 DC of 7 December 2000.
- French Constitutional Council Decision No 2010-614 DC of 4 November 2010.
- Ruling issued by the Commercial Court of Paris on 30 June 2008, No 2006-065217 — *Christian Dior/E-Bay*.
- Ruling issued by the Tribunal de Grande Instance of Paris on 10 February 2012.
- Maritime and Commercial Court in Copenhagen, 11 December 2014, *Fritz Hansen A/S, Louis Poulsen Lighting A/S, Carl Hansen & Son Mobelfabrik A/S, Fredericia Furniture A/S, Erik Jorgensen Mobelfabrik A/S v Telia Danmark*.
- Advocate Cruz Villalón, 26 November 2013, Opinion on the Case 314/12 – *UP Telekabel Wien GmbH v. Constantin Fil Verleih GmbH, Wega Filmproduktionsgesellschaft mbH*.
- Judgment of 27/03/2014, C-314/12, *UPC Telekabel Wien*, EU:C:2014:192.
- Judgment of 07/12/2010, joined cases C-585/08 and C-144/09, *Pammer and Hotel Alpenhof*, EU:C:2010:740.
- Decision of the Austrian Supreme Administrative Court No 2011/22/0097 of 31 April 2002.
- Decision of the Austrian Highest Administrative Court No 2012/15/0021 of 19 March 2013.
- Decision of the Austrian Supreme Court No 4 Ob 71/14s of 26 June 2014.
- Decision of the Austrian Supreme Court No 4 Ob 59/00f of 14 March 2000.
- Decision of the Austrian Supreme Court No 4 Ob 64/00s of 14 March 2000.
- Decision of the Austrian Supreme Court No 4 Ob 105/11m of 20 September 2011.
- Decision of the High Court of 17 July 2014 under Case *Comic Enterprise Ltd. V Twentieth Century Fox Film Corp.*
- Decision of the High Court of 17 October 2014 under Case *Cartier International AG & Ors v British Sky Broadcasting Limited*.
- Decision of the High Court of Justice of 23 October 2014 under Case *1967 Ltd & Ors v British Sky Broadcasting Ltd & Ors*.
- Decision of the High Court of 2 March 2015 under Case *Warner-Lambert Co LLC v Actavis Group PTC EHF*.
- Decision of the House of Lords of 6 May 2004 under Case *Campbell v Mirror Group Newspapers Ltd*.
- **Legal Acts**
  - Treaty on the Functioning of the European Union, OJ C 326, 26/10/2012 pp. 000-0390.
  - Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, pp. 391-407.

- Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, OJ C 306, 17.12.2007, pp. 1-271.
- Protocol (No 30) to the Treaty of Lisbon on the application of the Charter of Fundamental Rights of the European Union to Poland and to the United Kingdom, OJ C 306, 17.12.2007, pp. 1-271.
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23/11/1995 pp. 31-50.
- Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ L 178, 17/07/2000 pp. 1-16.
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31.7.2002, pp. 37-47.
- Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, OJ L 157 of 30 April 2004.
- Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167, 22/06/2001 pp. 10-19.
- Commission Decision 78/59/EEC, of 2 December 1977, relating to a proceeding under Article 85 of the EEC Treaty, OJ L 20, 25.1.1978, pp. 18-27.
- The Act of 6 August 2004 on the Protection of Natural Persons regarding the Processing of Personal Data: what changes have been introduced by the Act on 'IT and Freedoms' of 6 January 1978? (*La Loi du 6 Août 2004 relative à la Protection des Personnes Physiques à l'Egard des Traitements de Données à Caractère Personnel: quels changements dans la Loi 'Informatique et Libertés' du 6 Janvier 1978?*), French Data Protection Authority.
- French Law No 78-17, of 6 January 1978, regarding IT, Databases and Liberties (*Loi n° 78-17 relative à l'informatique, aux fichiers et aux libertés*).
- French Law No 2004-575, of 21 June 2004, regarding Confidence in the Digital Economy (*Loi n° 2004-575 pour la confiance dans l'économie numérique*).
- French Law No 2007-1544, of 29 October 2007, regarding the Fight against Counterfeiting (*Loi n° 2007-1544 de Lutte contre la Contrefaçon*).
- Danish E-Commerce Act, 2002.
- Danish Ministry of Culture, 2014, Consolidated Act on Copyright No 1144 of 23 October 2014.
- The Convention for the Protection of Human Rights and Fundamental Freedoms.
- Austrian Constitution of 2 December 1867.
- Austrian State Basic Act of 1867.
- Austrian Civil Code.
- Austrian Federal Law No 111/1936, of 9 April 1936, on Copyright in Works of Literature and Art and on Related Rights (*Bundesgesetz über das Urheberrecht an Werken der Literatur und der Kunst und über verwandte Schutzrechte*).
- UK Copyright, Designs and Patents Act 1988.
- UK Data Protection Act 1998.
- UK Human Rights Act 1998.
- UK Trade Marks Act 1994.
- UK Registered Designs Act 1949.
- UK Companies Act 2006.

- UK Competition Act 1998.
- UK Enterprise Act 2002.
- Bill of Rights of the first Congress of the United States of America in 1789.
- United States Federal Constitution of 1787.
- United States General Assembly Universal Declaration of Human Rights of 10 December 1948.
- The United States Code.

Avenida de Europa, 4,  
E-03008 - Alicante  
Spain

[www.euipo.europa.eu](http://www.euipo.europa.eu)



## STUDY

on voluntary collaboration practices in  
addressing online infringements of  
trade mark rights, design rights,  
copyright and rights related to  
copyright