Moving Towards Balance

A study into duties of care on the Internet

Institute for Information Law (IViR)

Leibniz Center for Law

Prof. Dr. N.A.N.M. van Eijk
Prof. Dr. T.M. van Engers

Mr. C. Wiersma
Mr. C.A. Jasserand
W. Abel LL.M.

University of Amsterdam
2010

Moving Towards Balance

A study into duties of care on the Internet

Institute for Information Law (IViR)
Leibniz Center for Law

Prof. Dr. N.A.N.M. van Eijk
Prof. Dr. T.M. van Engers

Mr. C. Wiersma
Mr. C.A. Jasserand
W. Abel LL.M.

University of Amsterdam
2010

Table of Contents

Summary

Commissioned by the WODC (Wetenschappelijk Onderzoek- en Documentatiecentrum), research has been conducted on duties of care on the Internet, more specifically from the perspective of Internet service providers. Internet service providers currently find themselves in the spotlight, both in a national and international context, with regard to their relationship both with governments and other private parties, on for example questions of (civil) liability. This research focuses on duties of care as concerns the relationship between government and Internet service providers. When such a duty of care does not exist, whether or not duties of care have been developed for others along the value chain between providers of information services and end-users, including Internet service providers, was examined.

The situation in four countries – the Netherlands, the UK, Germany and France – was researched. The (self-) regulation with respect to five separate themes (Internet security and safety, child pornography, copyright, identity fraud and the trade in stolen goods through Internet platforms) was identified. In addition to this, a significant number of interviews with stakeholders were conducted.

The research presents divergent results, which indicates that the related issues are still in a developing stage. Internet security and safety, more specifically the relationship between the Internet service provider and the end-user, has only been dealt with in a preliminary manner. This does not mean that in practice nothing happens, but there is a lack of formal embedding in regulation or self-regulation. With respect to child pornography, an almost identical regime exists in the examined countries. Stakeholders offer far-reaching cooperation in the fight against child pornography. All countries have established a system of hotlines for the notification of child pornography, based on self-regulation or a duty of care defined by legislation. A recurring subject of debate in the context of the fight against the dissemination of child pornography is the applicability of filtering and blocking measures. Copyright attracts a lot of attention, which has led to more stringent regulation of copyright issues in two of the examined countries, providing the possibility of cutting or limiting the access of end-users to the Internet. There is a lot of criticism on these more stringent regulations and, through the conducted interviews, stakeholders have raised clear concerns on the effective enforceability of the new rules. When dealing with identity fraud, the measures are focused on its consequences. There is not a lot of support for criminalizing identity fraud as such (in addition to already existing possibilities to counter identity fraud through other public laws). The sale of stolen goods through platform providers (i.e. auction and trading websites) is considered to be the responsibility of these providers.

The divergent results, which are proof of an ongoing dynamic in these fields and an ongoing search to find a right balance, imply that it is not possible to present proven best

practices. This also implies that on the one hand there is still a lot of insecurity, while on the other a clear challenge is presented for further policy-making. Nevertheless, the collected research results provide interesting information.

The authors present the following conclusions based on the conducted research:

1. Towards a value-chain approach

The examined duties of care cannot be related to one specific party in the value chain between information service providers and end-users. They should be considered as a shared – and balanced – responsibility of all involved stakeholders in the value chain of which, in addition to Internet service providers, providers of information services, platforms, search engines and hosting services are part.

2. Ex ante examination of effectiveness and enforceability

Examination in advance of the effectiveness and enforceability of (planned) legal intervention can contribute to the prevention of symbolic legislation and undesired effects.

3. Usability of "notice and take down" procedures

"Notice and take down" procedures are a widely accepted and applied mechanism. Not only do Internet service providers apply these or similar procedures (when acting as a provider of hosting or caching services), but other parties in the value chain, such as platform providers, do the same. In most of the examined countries, a specific legal ground for this practice is missing. Self- and co-regulatory initiatives exist however. It is recommended to further embed "notice and take down" procedures, for example by implementing a specific legal framework.

4. Clarification of Internet security, safety and privacy

The new provisions on Internet security, safety and privacy (more specifically, Article 4 of the European Directive on privacy and electronic communications) are unclear and demand further clarification on their meaning and impact. Clarification at the European level is desirable to prevent excessive divergences at the national level.

5. Elevation of the knowledge level

The inclination to develop and apply further regulation is partly caused by a lack of sufficient technical and practical knowledge. This lack of knowledge appears to be widespread. It is to be expected that the inclination to regulate will decrease when end-users, regulatory authorities, enforcement authorities and legislators will increase their knowledge level. The importance of education is widely emphasised.

Preface

The Dutch Institute for Information Law (*Instituut voor Informatierecht*, IViR) and the Leibniz Center for Law were commissioned by the Scientific Research and Documentation Centre (*Wetenschappelijk Onderzoeks- en Documentatiecentrum*, WODC) of the Dutch Ministry of Justice to conduct a study into duties of care on the Internet. The study was performed by Prof. Dr Nico van Eijk (IViR) and Prof. Dr Tom van Engers (Leibniz) in collaboration with Wiebke Abel LLM., mr. Catherine Jasserand and mr. Chris Wiersma.

In the context of this study, duties of care relate to the relationship between governments and Internet service providers. Such duties of care may be laid down in legislation or further regulations, but they may also be set out in forms of coregulation or self-regulation.

The position of the Internet service provider was taken as a point of departure in our study of the relevant duties of care. The Internet service provider's role, however, is not an isolated phenomenon; it is rather a link in the wider value chain between the providers of information services and the end-users.

The study was performed in four countries (the Netherlands, France, Germany and the United Kingdom) on the basis of five themes (Internet security, child pornography, copyright, identity fraud and the sale of stolen goods), by means of both a quantitative and a qualitative approach. (Self-)regulatory measures with regard to duties of care have been inventoried and described. Interviews were conducted with the major stakeholders so as to gain the most accurate idea possible of the situation in the countries under study.

The researchers especially wish to thank the interviewees who were so generous as to make time available for the interviews, which often proved to be most informative and frank.

Amsterdam, June/October 2010

Table of Abbreviations

AFA	Association des Fournisseurs d´Accès et de Services Internet
AFOM	Association Française des Opérateurs Mobiles
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ARCEP	Autorité de régulation des communicatons électroniques et des postes
BEFTI	La Brigade d'enquêtes sur les fraudes aux technologies de l'information
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BKA	Bundeskriminalamt
BVerfG	Bundesverfassungsgericht
BW	Burgerlijk Wetboek
CIRCAMP	Cospol Internet Related Child Abusive Material Project (www.circamp.eu)
CNIL	Commission nationale de l'informatique et des libertés
CP	Code Pénal
CPCE	Code des postes et des communications électroniques
CPI	Code de la Propriété Intellectuelle
CPP	Code de Procédure Pénale
CSPLA	Conseil Supérieur de la Propriété Littéraire et Artistique
DADVSI	Loi sur le Droit d'Auteur et les Droits Voisins dans la Société de l'Information
DNS	Domain Name System
ECO	Electronic Commerce Forum (Verband der Deutschen Internetwirtschaft e.V.)
ECP-EPN	ECP-EPN | Platform voor de InformatieSamenleving, (www.ecp.nl)
FCACP	Financial Coalition Against Child Pornography
FSM	Freiwillige Selbstkontrolle Multimedia-Diensteanbieter
HADOPI	Haute Autorité pour la Diffusion des Œuvres et la Protection des Droits sur Internet
INHOPE	International Association of Internet Hotlines
ISPA UK	Internet Services Providers' Association United Kingdom
IWF	Internet Watch Foundation
KLPD	Korps landelijke politiediensten
LCEN	Loi pour la confiance dans l'économie numérique

Loi HADOPI	Loi favorisant la diffusion et la protection de la création sur Internet
Loi HADOPI 2	Loi relative à la protection pénale de la propriété littéraire et artistique sur Internet
Loi Informatique et Libertés	Loi relative à l'informatique, aux fichiers et aux libertés
LOPPSI II	Loi d'Orientation et de Programmation pour la Sécurité Intérieure
NICC	Nederlandse Infrastructuur ter bestrijding van Cybercrime
OCLCTIC	Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication.
OFCOM	Office of Communications
OPTA	Onafhankelijke Post- en Telecommunicatie Autoriteit
PHAROS	Plate-forme d'Harmonisation, d'Analyse, de Recoupement et d'Orientation des Signalements
SOCA	Serious Organised Crime Agency
Sr	Wetboek van Strafrecht
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
Sv	Wetboek van Strafvordering
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
Tw	Telecommunicatiewet
UrhG	Urheberrechtsgesetz
URL	Uniform Resource Locator
VeRO	Verified Right Owner Program
Wbp	Wet bescherming persoonsgegevens
ZugErschwG	Gesetz zur Erschwerung des Zugangs zu kinderpornographischen Inhalten in Kommunikationsnetzen

Glossary

Botnet	Term for a collection of software robots that operate autonomously and automatically. The term is mostly associated with malicious software: botnets are networks of infected computers, also called "zombie PCs".
Caching	Temporary but unmodified storage of information, for instance for Internet traffic processing.
Deep packet inspection	A method for looking inside the data packages that are sent via the Internet.
(Wireless) router	Peripheral converting and sending of (incoming and outgoing) signals from and to a telephone connection for the benefit of a (wireless) Internet connection of a computer.
Fingerprinting	Taking a "fingerprint", for instance of a music file, which results in a so-called sound file by means of which the original files can be recognized.
Grooming	Trying to contact children online with the intention of abusing them sexually online and/or offline.
Hosting/webhosting (provider)	Service that offers space to private individuals or companies for storing information, images or other content that is accessible via a website.
Internet service provider	Market party engaged in providing access to the Internet for end-users. In addition, these parties are often active as providers of so-called hosting and caching services.
Malware	Collective term for malicious and/or harmful software. The word is a contraction of "malicious software".
Mere conduit	The uncut transfer of, or provision of access to, information on the Internet.

Notice and take down	Procedure for handling messages (notice) relating to content on the Internet, where notification is followed by an assessment as to whether the material is to be removed from the Internet (take down) or not.
Peer-to-peer	A computer network on which the users are mutually connected with each other. No servers are used.
Phishing	Practice by which existing websites are copied and a certain reliability of these copies is feigned although the websites are fake.
Spam	Unsolicited communication for commercial, ideological or charity purposes.
Virus	Form of malicious software (malware). It is a computer program that may lodge in a file, for instance an operating system file.
Zombie PC	See “Botnet”.

1 Introduction and problem definition

1.1 Research question

At the request of the Dutch Scientific Research and Documentation Centre (*Wetenschappelijk Onderzoeks- en Documentatiecentrum*, WODC), the Dutch Institute for Information Law (*Instituut voor Informatierecht*, IViR) and the Leibniz Center for Law carried out a study into the duties of care of Internet service providers – who constitute only one of many parties in a complex value chain[1] – in the Netherlands and some of its neighbouring countries. The aim of the study is to provide some insight into the forms of duty of care for Internet service providers in the Netherlands, France, Germany and the United Kingdom. The study also focuses on the role of the national governments and the reasons for the current form of setup. The central research question is the following:

Which forms of duty of care for Internet service providers apply or are being developed in the countries mentioned? What is the role of the national government in this context? What are the reasons for the chosen approach and what are the experiences with this approach?

Several sub-questions were addressed in addition to the central research question, in the context of both the stocktaking and the analysis part of the study (actual/legal content of duties of care, experiences, (direction by) market parties/governments, future policy/regulations). These have been processed in the country-specific studies and their descriptions in Chapter 3.

In the study, Internet service providers are understood to mean market parties engaged in providing access to the Internet to end-users.[2] In terms of telecommunications law, the activity in question consists of a "public telecom service".[3] In addition, these parties are often active as providers of so-called hosting and caching services (see below, under "Legal context").

Duties of care are primarily about the relationship between the government and Internet service providers and usually take the form of regulations or coregulation. Where this is

[1] See paragraph 1.3.

[2] See OECD (2010) about the conceptual framework to be adopted, which is one of our sources for the description of Internet service providers: "...Internet service providers are generally meant to signify Internet access providers, which provide subscribers with a data connection allowing access to the Internet through physical transport infrastructure".

[3] So-called resellers of services offered by others are outside the scope of this definition.

not the case, any forms of self-regulation will also be considered. It should be noted that it is often difficult to draw the line between coregulation and self-regulation. The relationship between government and Internet service providers may have consequences for the liability and responsibility of Internet service providers.[4] These (civil-law) aspects are beyond the scope of this study.

1.2 Themes

The research question is tested through five themes that were chosen in consultation with the commissioning authority, with the idea that in principle they represent the most relevant aspects of the underlying problems.[5]

The first theme relates to breaches of Internet security. What kind of duties of care are provided for in order to deal with privacy breaches or malware placement? Internet security is already subject to regulation on the basis of the European framework for the communication sector. This legislative framework, as stipulated in Article 4 of the Directive on privacy and electronic communications, plays a leading role in the study.

The second theme relates to child pornography. Child pornography on the Internet is among the subjects that required attention at an early stage in the development of the online environment; Internet service providers have been closely involved in this aspect.

Copyright is the third theme of the study. The focus is not on copyright as such but on the possible involvement of the Internet service provider when it comes to observing and protecting applicable copyright.

Identity fraud has been included as the fourth theme, especially because in 2007 the European Commission recommended that identity fraud be considered a crime in its own right.

The last theme relates to the question as to whether Internet service providers play a part in the sale of stolen goods, more particularly with regard to offering these goods via such platforms as auction sites.

The themes partly overlap with each other or raise similar issues, for instance with respect to security aspects and applied procedures (such as forms of notice and take down)[6], or in the field of enforcement.

---

[4] On the issue of liability, see: De Cock Buning and Van Eek (2009); Van Hoboken (2009).
[5] For a wider description of cybercrime activities, see: Van der Hulst/Neve (2008).
[6] For notice and take down, see paragraph 1.4.2.

The themes are not dealt with exhaustively in this study, but they are mainly considered from the central study question, i.e. if there is, and if so what kind, a regulated relationship between the government and Internet service providers.

1.3 Value chain

Internet service providers constitute only one of several parties that are active in the value chain between end-users and providers of services (services of the information society as well as other forms of transaction).[7] A provider of an information service uses a hosting provider to make its website accessible on the Internet. Next, the website is opened up via intermediaries, such as search engines, before end-users with Internet access via an Internet service provider obtain the information on the website. Another example is that of the end-user who wishes to access an auction/selling site through his Internet service provider to obtain goods that possibly come from a web shop that sells through the auction platform. The operation is handled via a digital bank transaction. Thus, the value chain does not only involve interconnected actions, but is also an economic value chain with a multitude of (financial) transactions. Where the role of the Internet service provider could not be determined in the study, it has been investigated whether other intermediaries in the value chain have any duties of care.

Two legal frameworks, both of European origin, are decisive for answering the study's question. The Directive on privacy and electronic communications, which is part of the directives regulating the communication sector, includes duties of care with respect to Internet security that are relevant for Internet service providers. Secondly, the provisions of the E-commerce Directive are also relevant. Although the Directive's rules on "mere conduit", "hosting" and "caching" are focused on the liability of intermediaries, such as Internet service providers, they have also led to duties of care/self-regulation in many countries. In the study assignment, attention was drawn explicitly to the Communication of the European Commission on identity fraud. Finally, the definition of the legal framework for child pornography, copyright and the sale of stolen goods is discussed in further detail.

[7] For this value-chain approach, see Dommering and Van Eijk (2010) and Rand Europe (2008).

1.3.1 Internet security

By virtue of Article 4 of the Directive on privacy and electronic communications adopted in 2002,[8] providers of publicly available electronic communication services (which include Internet service providers as well) are required to take appropriate technical and organizational measures to safeguard the security of the services provided. If necessary, this should happen in conjunction with the provider of the public communication network on which the service is provided. The measures to be taken should ensure a security level that is proportionate to the state of the technology and the costs of its execution. In the second paragraph of the article, it is stipulated that providers are to inform their subscribers of the special risks of network security breaches. If the risk lies outside the scope of the measures to be taken by the service provider, the latter must inform the users of any possible remedies, including an indication of the expected costs.

Article 4 was recently extended in the context of the revision of the European framework for the communication sector.[9] Member states have to implement the adjustments by 25 May 2011 at the latest. A new paragraph 1a has been added to the article, imposing obligations on the providers regarding access to personal data, protecting stored or transmitted personal data and introducing a security policy with respect to the processing of personal data. The national authorities need to be able to audit the measures taken and to issue recommendations. In a new third and fourth paragraph, a notification obligation is introduced as to breaches related to personal data.[10] Breaches are to be reported to the competent national authority. When the personal data breach is likely to have adverse effects on the personal data or the privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach. Further rules can be laid down at national level. In addition, the European Commission can adopt technical implementing measures.

In the Netherlands, the original Article 4 of the Directive has been implemented in Article 11.3 of the Telecommunications Act. This is essentially similar to Article 4. A preliminary draft law amending the Telecommunications Act so as to implement the new regulatory framework was recently published.[11] Amendments to Article 11.3 of the Telecommunications Act provide for additional protection with respect to managing personal data and further regulatory powers in that respect. The notification obligation for breaches of personal data is laid down in a new paragraph 11.3b of the Telecommunications Act, whereas a new chapter 11a is inserted, which further focuses on continuity of service issues in relation to with public electronic communication networks

[8] 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 201/37, 31.07.2002.
[9] Directive 2009/136/EC of 25 November 2009 (Citizens' Rights Directive), OJ L 337/1, 18.12.2009.
[10] For further information on the notification obligation, see Boer and Grimmius (2009).
[11] http://www.internetconsultatie.nl/nrfimplementatie

and public electronic communication services, including a notification obligation regarding security breaches and integrity loss.

1.3.2 E-commerce Directive

The E-commerce Directive ("Directive on electronic commerce")[12] of 2000 plays a major role for Internet service providers. It comprises a system in which three activities are distinguished: "mere conduit", "caching" and "hosting".[13] Mere conduit (Article 12) consists in the uncut transfer of, or providing access to, information. Mere conduit thus includes the core activity of Internet service providers, i.e. providing access to the Internet. If they do not make any further selections or changes to the information, the Directive excludes liability for such activity. Nevertheless, a court or an administrative authority may demand that a service provider terminates or prevents an infringement. Caching (Article 13) refers to the temporary but unmodified storage of information. Hosting (Article 14) refers to activities associated with the storage of information provided by a recipient of the service. This includes hosting a website or personal pages. With regard to caching and hosting, it is stipulated in the Directive that liability is avoided when providers remove information after they have obtained actual knowledge (with respect to information that is – evidently – unlawful/illegal, or where appropriate, by an order to that effect). This is also called "notice and take down". In the Netherlands, the provisions of the Directive have been implemented in Article 6:196c of the Civil Code. The Dutch Penal Code provides that intermediaries which collaborate in making data accessible are granted immunity from criminal prosecution (Article 54a Penal Code).[14] A bill is under way to include notice and take down in Article 54a Penal Code, thus making this procedure also part of criminal law. Additionally, the Code of Criminal Procedure is to be amended to include a provision on the basis of which a public prosecutor may demand cooperation in making content on the Internet, which is subject to prosecution, inaccessible.[15]

In the provisions of the Directive on mere conduit, caching and hosting, nothing is stated about duties of care. Parties acting in conformity with the Directive, however, can claim a limitation of their liability. Yet, if member states opt for prescribing the notice and take down principle as binding, the Directive would not oppose this. Market parties can make notice and take down part of self-regulation. In either situation, there is a duty of care which is within the scope of this study.

---

[12] 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 (Directive on electronic commerce), OJ L 178/1, 17.7.2000.

[13] To a large extent, this system has been derived from the US Digital Millennium Copyright Act (DMCA). For further information, see Elken-Koren (2006).

[14] For a critical review on Article 54a, see Schellekens, Koops, Teepe (2007).

[15] Speech by the Dutch Minister of Justice Hirsch Ballin on the occasion of the launch of the Internet Security Platform on 8 December 2009 (http://www.ecp-epn.nl/sites/default/files/Toespraak-_mvj_8december2009.pdf).

In 2007, the E-commerce Directive was extensively assessed in a study by G. Spindler and T. Verbiest.[16] In this study commissioned by the European Commission, various trends are observed, which are also discussed in the current study. The angle adopted in the 2007 report, however, is different and focuses on the liability of intermediaries in a general sense.[17] The study should be the prelude to a revision of the E-commerce Directive, but so far the European Commission has not made any proposals yet, although they have been announced in the context of the European "Digital Agenda".[18]

1.3.3 Identity fraud

Identity fraud on the Internet is understood to mean appropriating somebody else's identity with the intention of committing unlawful acts.[19] Definitions may vary, but they all boil down to this. In a communication of 2007, the European Commission notes that identity fraud in itself is not made punishable in all member states.[20] It is stated that it is often easier to prove the criminal offence resulting from the identity theft than to focus on identity theft as such. This does not alter the fact that identity fraud is a violation of, for instance, privacy regulations. A study commissioned by the European Commission into identity fraud in the EU Member States is currently being carried out. This may lead to further regulations in 2012.[21]

1.3.4 Child pornography

The fight against child pornography on the Internet is supported to a large extent by the private INHOPE initiative, which was started in 1995 and which is backed by the European Union.[22] INHOPE is an association of national hotlines where child pornography (and related activities, including grooming – i.e. contacting children online with the intention of abusing them sexually online and/or offline) can be reported. After verification, the notification is passed on to the relevant authorities. In the Netherlands, the Child Pornography Hotline (*Meldpunt Kinderporno*) is the INHOPE partner.[23] The INHOPE practice can be considered a form of notice and take down.

Child pornography has been on the European agenda for some time. In the Framework Decision of 22 December 2003, it is stipulated that member states are to take measures

---

[16] Spindler/Verbiest 2007.
[17] The doctrine of intermediaries' liability is under development.
[18] http://ec.europa.eu/information_society/digital-agenda/index_en.htm.
[19] For identity fraud, see: De Vries et al (2007); Van der Meulen (2009).
[20] European Commission, communication from the Commission to the European Parliament, the Council and the Committee of the Regions towards a general policy on the fight against cyber crime, COM(2007) 267 final, 22 May 2007.
[21] European Commission plan to deliver justice, freedom and security to citizens (2010-2014), Memo/10/139, 20 April 2010.
[22] International Association of Internet Hotlines, www.inhope.org.
[23] http://www.meldpunt-kinderporno.nl.

against the proliferation of child pornography.[24] A proposal was recently published to replace the Framework Decision by a directive.[25] Article 21 of the draft directive provides that member states should take measures to block access to child pornography. This blocking should come with the necessary guarantees. Furthermore, member states are to take measures to remove child pornography from the Internet. As stated in the preamble, blocking is important when the information originates from countries outside the European jurisdiction.

In the field of child abuse, the police authorities in Europe are already collaborating intensively in the CIRCAMP[26] programme, and further cooperation between Europe and the United Stated (where most child pornography apparently is hosted) has been announced.[27] The form in which blocking is conducted, is left to the member states. Self-regulation by Internet service providers on the basis of codes of conduct is mentioned as an option (besides blocking by order of the judiciary or police on the basis of possibilities to that effect within the civil and/or penal law). The choices for alternatives are partly based on what is permitted by national regulation.

1.3.5 Copyright

The regime of the E-commerce Directive was partly implemented to establish the position of parties such as Internet service providers with regard to copyright infringements (see section 1.3.2 above for a further description of the rules of the E-commerce Directive). Supplementary to this, we can refer to the discussion in the context of the New Regulatory Framework (NRF)[28] for the communication sector about the "three strikes" – or graduated response – issues.[29] Proposals to assign a specific role to Internet service providers in enforcing copyright (with respect to downloading music, video, e-books and games in particular)[30] have eventually not led to European regulations. It should also be noted that in Article 3a of the Framework Directive,[31] it is stipulated that fundamental rights and

[24] Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography, OJ L 13/44, 20.1.2004.

[25] European Commission, Proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA, Brussels, 29.3.2010, COM(2010)94 final; see also: European Commission, press release IP/10/379, 29.3.2010 and MEMO/10/107, 29.3.2010.

[26] Cospol Internet Related Child Abusive Material Project (www.circamp.eu).

[27] For the collaboration between Europe and the United States, see http://www.independent.co.uk/-news/media/ us-eu-to-launch- programme-against-internet-child-pornography-1941748.html

[28] The New Regulatory Framework concerns the existing directives for the communication sector and can be found in two directives: Directive 2009/136/EC of 25 November 2009, OJ L 337/11 (18.12.2009) and Directive 2009/140/EC of 25 November 2009, OJ L 337/37 (18.12.2009).

[29] See also: TNO/SEO/IVIR (2009) and Ringnalda, Elferink and De Cock Buning (2009).

[30] In some countries, e.g. the Netherlands, downloading is not punishable; in other countries it is. See literature in the previous note.

[31] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), OJ L 108/33 (24.04.2002), amended by Directive 2009/140/EC of 25 November 2009, OJ L 227/37 (18.12.2009).

freedoms are to be observed by member states when taking measures on access to, or the use of, services and applications by end-users. This interest is supported by the Netherlands.[32]

1.3.6 Sale of stolen goods

The sale of stolen goods on the Internet, particularly the role of the Internet service provider in this, has been given relatively little attention so far on a European level. Platform providers, such as auction sites, claim they perform hosting services as described in the E-commerce Directive. Meanwhile, some preliminary questions have been referred to the Court of Justice of the EU. This pertains to the *eBay v. L'Oreal* case,[33] where the issue is not stolen goods but the sale of articles that breach intellectual property rights.

1.4 Setup of the study

The legal and policy-based context of the five themes as well as the involvement of Internet service providers has been examined through an analysis of the literature in the field. The relevant regulations and/or self-regulation have been inventoried and summarized in country-specific studies.

Because of the highly dynamic nature of the subject matter of the study and of its ongoing development, a traditional study of literature was deemed not to be sufficient. Instead, the aim has been to validate the findings of the study of literature and enrich them with local information. To this end, visits were made to the selected countries and interviews were conducted with 6 to 8 stakeholders in each country. The researchers held meetings with representatives of (interest groups of) Internet service providers, governments, regulatory and supervisory bodies, social organizations and independent experts. In addition, in the Netherlands interviews were carried out with several organizations/companies that, besides Internet service providers, are part of the value chain, such as Marktplaats/eBay and Google. The list of interviewed parties is included in the appendices.

As agreed with the interviewees, the results of the interviews have been kept anonymous. The researchers are responsible for the interpretation of the interviews and the processing method.

[32] *Kamerstukken II* (Parliamentary documents), 2009-2010, 29838, nr 24.
[33] http://www.judiciary.gov.uk/docs/judgments_guidance/l'oreal-ebay.pdf. Preliminary questions: Publ C 267/40, 7.11.2009, case C-324/09.

The literature study was concluded in April 2010. Any subsequent developments have been included only to a limited extent. The majority of the interviews were conducted in January-February 2010.

An advisory committee chaired by Prof. mr. F.W. Grosheide has assisted the researchers (see Appendix 2). The setup of the study was discussed with the committee, after which the interim results were reported. Finally, the draft report was discussed with the committee, and the researchers incorporated the comments of the committee in the final report.

1.5 Outline of the report

Chapter 1 of this report defines the subject matter and the questions under analysis and describes the setup of the study. In Chapter 2 ("Stocktaking and findings"), (co/self)regulatory measures in the countries under study are described per theme on the basis of the country-specific studies and the interviews conducted. The analysis and conclusions are provided in Chapter 3. In the country-specific studies (included in Appendix 1), the current legal framework and any relevant legal developments are described in further detail. Each time, an outline of the implementation of the E-commerce Directive is given in a general introduction, as it is relevant for most of the themes. Next, the existing special regulations (legal provisions and other measures, such as self-regulation) are sketched per theme, and their application is discussed more closely. Where appropriate, other developments, such as new bills, are mentioned separately.

2 Stocktaking and findings

2.1 Introduction

In the study, the regulations of the selected countries – the Netherlands, France, Germany and the United Kingdom – have been inventoried. First of all, the relevant legislation and regulations have been identified. Where specific regulations were lacking, it has been investigated whether any forms of self-regulation and/or coregulation exist. The individual country-specific studies are provided in Appendix 1. These country-specific studies also include references to relevant parliamentary documents, literature and jurisprudence.

In addition to the stocktaking part of the study, several interviews with stakeholders were held in the four countries.

In this chapter, a summary of the current issues is provided per theme based on the national regulatory situation and the information given during the interviews.

2.2 Internet security

In all the countries under study, the content of Article 4 of the Directive on privacy and electronic communications can be found in the national telecommunication acts. In each instance, reference is made to the importance of the protection of privacy and personal data in electronic communications. Internet security has been studied in this context in particular.

In the countries under study, hardly anything substantial can be found on duties of care. It is clear, however, that Internet service providers are understood to have mainly two duties of care. The first pertains to taking suitable technical and organizational measures to safeguard Internet security. The second pertains to informing the end-users about specific risks and measures that can be taken to minimize these risks, in so far as the Internet service provider does not have the obligation itself to take measures. In most countries, the minimum requirements or best practices have not been further defined in regulations or jurisprudence.

In the Netherlands, a process has been started, upon the initiative of the Independent Post and Telecommunication Authority (*Onafhankelijke Post en Telecommunicatie Autoriteit*, OPTA), to put the duties of care as laid down in Article 11.3 of the Telecommunications Act into practice. This has resulted in the analysis of relevant issues for the establishment of policy

rules. Currently, only rules on the obligation of informing end-users about certain risks have been formulated.

These policy rules have been laid down in the "Policies for information providers on Internet security" (*Beleidsregels informatieplicht voor aanbieders over internetveiligheid*). Further consultations with the Dutch Government on rules obliging Internet service providers to take security measures have been planned.

OPTA is working with the Dutch National Police Services Agency (*Korps Landelijke Politiediensten*, KLPD) on the basis of a protocol containing agreements on information exchange. The KLPD can act against security breaches to the extent that the national penal law allows for sanctions related to this. In addition, OPTA has its own powers to impose administrative sanctions. Studies have shown that the Netherlands is a pioneer in Europe concerning various Internet security aspects.[34]

Many Dutch Internet service providers have entered into a covenant in which the intentions have been laid down for the joint combat against botnets. The exchange of information on the basis of the covenant plays a major role in this. End-users should be helped to clear their computers, before they obtain access to the Internet again.

In the United Kingdom, the Internet Services Providers' Association (ISPA UK) has formulated "best current practices", specifically for the secure handling of e-mail. This document is not compulsory for the members.

In Germany, a provision in the national telecommunications act deals with the organizational measures required of Internet service providers; the provision focuses on the prevention of interruptions, the effects of external attacks and catastrophes. Here, too, further implementation is left to the stakeholders. In addition, an anti-botnet website has been developed upon the initiative of ECO (*Verband der deutschen Internetwirtschaft* – Association of the German Internet Industry) and the federal government, through which Internet service providers play an active role in dealing with reported and detected botnets, by means of a call centre that actively helps to clear the computers of the clients who report. The costs are partly carried by the government.

In France, the spam issue in particular has led to further government involvement. The "Signal Spam" help line was set up with the assistance of public authorities in collaboration with professional parties. This initiative is in line with the recommendations of the French Association of Internet Service Providers (AFA) on technical measures against spam.

The French Government has recently made a proposal for a statutory regulation that will oblige Internet service providers to report certain security breaches with respect to personal data to the French supervisory authority in this field (CNIL – *Commission nationale*

de l'informatique et des libertés). This proposal can be regarded as an early response to the recently extended Article 4 of the Directive on privacy and electronic communications. In both the Netherlands and France, the government has expressed its intention to make this notification mandatory for other services of the information society, and not only for Internet service providers.

In the interviews, it was emphasized that further concrete steps towards putting in place the duties of care arising from the (new) European directive framework are necessary. The interviewed parties indicated in general that Internet traffic inspections might be in conflict with privacy legislation and principles regarding the confidentiality of (tele)communication. From a technical perspective, however, there are various possibilities. Additionally, on the basis of agreements with customers, Internet service providers filter information because of viruses and spam. Several parties have expressed their concern about the lack of clarity of the legal framework concerning the admissibility of such methods. There is little transparency as to who is affected by these methods and to what extent.

Botnets are clearly a concern for Internet service providers. In the interviews, this problem was discussed as a separate aspect within the Internet security theme and the legal framework arising from the implementation of Article 4 of the Directive on privacy and electronic communications. Internet service providers may face blacklisting due to botnets, causing certain services, such as e-mail, to be disrupted. Although many public sources with location data on botnets are currently available, it is difficult to catch all of them, and extensive work is required to deal with botnets in this way. Establishing the reliability of the public sources mentioned is also difficult.[35] Quarantine measures for such computers seem to be necessary, but limiting Internet access has also a negative impact. Furthermore, differences in available resources imply that not all Internet service providers would (like to) act against botnets for their customers.

Risks associated with the use of wireless routers have received special attention. The interviewees were asked if the current duties of care in the field of Internet security also cover this issue. It is clear that besides Internet service providers there are several other market parties supplying wireless routers. These parties are not within the scope of the current telecommunication-related legal framework.

Another question in the interviews was to what extent the effectiveness of the measures taken to implement the obligation to provide information as set out in Article 4 of the Directive on privacy and electronic communications, is being supervised. The question emerged whether the national government could play an active role in instructing end-

[34] Dumortier and Somers (2008).
[35] In this context, see: Van Eeten et al (2010).

users about the safety and security of the Internet or whether it could at least be more closely involved in ensuring that the information actually reaches the end-users.

With respect to Internet security, the question was asked which public authorities could be entrusted with dealing with security breaches. The answer to the question depends on whether a security breach is a national security issue or not. In France, this determines competences, since the French national telecommunication authority (ARCEP) has not been granted the authorization to handle national security policy issues. Other authorities in the field of privacy and national defence could play a role, but this has not been further defined or little is known about it.

2.3 Child pornography

Even before the adoption of the E-commerce Directive, the theme of child pornography received ample attention. In practice, notice and take down is implemented via a system of hotlines in the context of INHOPE, the European organization in this field. The websites of these hotlines act as the first entry point for notifications. In general, the focus is exclusively on publicly accessible Internet traffic, especially websites. These hotlines play an important role in handling notifications of child pornography, with the active cooperation of the police and the judicial authorities, also at international level. Most of the time, Internet service providers send their notifications directly to these hotlines.

In some countries, codes of conduct have been developed which include recommendations for notice and take down with regard to child pornography.

In the context of the European Framework for Safer Mobile Use, providers of mobile telephony in all the countries under study have signed framework agreements, in which access to child pornographic material is discussed as well. In these agreements, the providers acknowledge their duty of care to contribute to the removal of child pornographic content on the Internet.

In the Netherlands, a Notice and Take Down Code of Conduct (*Gedragscode Notice and take down*) has been developed by the NICC (National Infrastructure Cybercrime). The code is administered in the framework of the Internet Security Platform (*Platform Internetveiligheid*), where the government and market parties work together. The code of conduct is a declaration of intent that the major Internet service providers have underwritten. Service providers in general can use the code for developing notice and take down procedures. The code of conduct aims at offering a number of options with respect to the application of notice and take down procedures to illegal content on the Internet. Handling such procedures is mainly the task of the providers themselves. The role of the judicial authorities is not described. The legal basis in the Dutch Penal Code for a notice and take down order by a public prosecutor in a criminal context requires some clarification,

especially with respect to guarantees for a sufficient judicial assessment of such an order. A revision of this provision was announced at the time of the implementation of the E-commerce Directive, but so far it has not been completed yet. The lack of such guarantees has been detected in both the literature and in recent case law.

Several parties in the Netherlands, including the Child Pornography Hotline (*Meldpunt Kinderporno*) and the Internet Security Platform (*Platform Internetveiligheid*), support plans for filtering Internet traffic for child pornography. In the context of the latter platform, in which the Dutch Government is involved, the development of a blacklist has been announced, to be used for filtering by Internet service providers.

In the United Kingdom, the non-governmental Internet Watch Foundation (IWF) acts as a hotline for child pornography reports. On the basis of self-regulation the IWF plays a binding role, not only bringing Internet service providers and experts together but also involving educational institutions and the general public in combating child pornography. The IWF not only takes care of assessing child pornography notifications, referring them to (international) criminal investigation authorities, but also generates a blacklist used by a high percentage of Internet service providers in the United Kingdom for blocking child pornography on the Internet. In its code of conduct, the association of Internet service providers (ISPA UK) also refers to the role of the IWF.

The *Freiwillige Selbstkontrolle Multimedia-Diensteanbieter* (FSM) is a self-regulation body in Germany. In addition to a hotline, the FSM has a code of conduct for its members, which include all major Internet service providers. Under the code, the members are required to play an active role in the fight against child pornography, including an obligation to forward notifications to criminal investigation institutions. It also provides for warning members or expelling them from the organization if they do not comply with the provisions of the code.

A recently adopted act in Germany (*Zugangserschwerungsgesetz*), which obliges Internet service providers to block child pornographic material belonging to a list prepared by the national police authority (*Bundeskriminalamt*), seems to be on its way to being abolished. In this context, the German Government has also drawn up individual contracts with Internet service providers, the content of which is not known. This act and these contracts have met with much resistance due to the major breach of communication confidentiality and their impact on privacy and freedom of expression in general. No initiatives have been taken to actually prepare the intended list, and now the reversal of the act is being considered. This has also been confirmed in the interviews.

In France, a signaling procedure defined by the law is used for certain categories of "particularly harmful illegal content", including child pornography. Consequently, Internet service providers have the legal obligation to forward notifications of child pornography to the relevant public authorities.

In addition, the French Association of Internet Service Providers (AFA) has developed a code of conduct, which is close to the Dutch Code of Conduct on Notice and Take Down. However, the French code exclusively pertains to certain categories of illegal content, including child pornography.

In France, the co-regulatory platform *Forum des droits sur l'internet* has issued several recommendations on child pornography on the Internet. One of these has led to a legislative proposal that provides for the imposition on Internet access providers of the obligation to filter child pornographic content.

In the interviews, it became clear that Internet service providers are willing to cooperate in combating child pornography, but that they keep a weather eye open for measures reaching too far concerning their own liability, in view of the liability restrictions in the E-commerce Directive. They also worry that the imposition of obligations relating to combating child pornography may lead to the creation of further obligations in other fields.

In general, the interviewees were satisfied with how the INHOPE hotline system is functioning. One of its mentioned benefits is that the requirement to classify the notified material can be delegated to the hotlines. Too much involvement in classification could lead Internet service providers to intervene in a random fashion. This could result in an unnecessarily strictly censored Internet. The same could happen if more practices were to emerge in addition to the hotlines, especially if so-called blacklists were used.

On the basis of the interviews, active monitoring of Internet traffic, with the use of deep packet inspection for instance, does not seem to be applied. According to the majority of interviewees, deep packet inspection is considered a disproportionate measure.

Several stakeholders expressed (serious) doubts about the effectiveness of filtering measures. They also warned that active filtering by Internet service providers could lead to the development of new encryption techniques as well as underground networks for the spread of such techniques, which will be difficult to detect.

From the interviews it is apparent that various policy aims are put forward as a motivation for the introduction of filtering obligations to deal with child pornography. In addition to the fundamental aim of effectively combating child pornography, with the protection of children as the central objective, the prevention of undesirable confrontation with illegal content is also mentioned.

Furthermore, it was noted that the police sometimes do not have sufficient resources or expert staff to deal with child pornography. Traditional criminal investigation methods for

the fight against child pornography often impose heavy demands on the investigating authorities.

Several interviewed parties emphasized the importance of good support for the parents for teaching sensible Internet use when raising their children.

Several parties referred to the practice in the United States whereby market participants from the financial sector work together to check transactions in order to combat access to child pornography on the Internet.

2.4 Copyright

Similar to the theme of child pornography, the regulations laid down in the E-commerce Directive are the decisive legal framework for the copyright theme in all the countries under study. On the basis of this, the duty of care of Internet service providers only pertains to measures for removal of offending content, in the form of notice and take down procedures in the context of caching and hosting activities.

With respect to copyright, the practice of notice and take down is often not as strictly defined in a specific framework as for child pornography. In the United Kingdom and France, however, there are legal initiatives to establish so-called "graduated response systems". In France, the adoption of the legislation that has become known under the name HADOPI[36] has been completed. In the United Kingdom, the Digital Economy Act has recently been adopted.

In the Netherlands, a number of court decisions establishing the liability of certain Internet (service) providers for copyright infringement have given rise to a further discussion on the limits of the duty of care of Internet service providers. These cases (see the country-specific study) were primarily heard in courts of lower instance and were mostly about websites that were not entitled to the status of hosting services and the corresponding liability restrictions contained in the E-commerce Directive. In each case, the involvement in copyright breaches was such that the limited definition of hosting activities in this directive didn't apply. In one case, an Internet service provider was ordered by the court in a provisional relief procedure to intervene by denying access to a website holder who unlawfully facilitated a copyright breach. In the literature, there is much criticism on this decision.

In the Netherlands, the private use exception in the current Copyright Act, on the basis of which copying, including downloading, of copyright-protected material for private

36 The act is officially referred to as the Loi favorisant la diffusion et la protection de la création sur Internet but is mostly dubbed the Loi HADOPI, after the name of the authority created by the act, the Haute Autorité pour la Diffusion des Oeuvres et la Protection des Droits sur Internet.

purposes is a permitted act, has recently been under discussion at parliamentary level. Such an exception (i.e. where copying for private use also covers downloading) cannot be found in the copyright legislation in the other countries under study. A parliamentary commission in the Netherlands has proposed to delete the current exception with respect to downloading. This discussion also dealt with the question of whether and how Internet service providers can play a part in enforcing the proposed new prohibition. There have been proposals on using techniques for this, with which Internet traffic can be checked structurally on the level of the files transferred, such as deep packet inspection and fingerprinting. According to the commission, it should also be provided for by law that Dutch Internet service providers or hosting providers should keep the customer data of individuals and companies that set up websites via their infrastructure. In a first reaction, the Dutch Government has indicated they agree with the work group that there are various problems in the field of copyright that need to be tackled. The proposals of the commission have not led to any concrete bills yet, but the commission has indicated that they do not regard the use of deep packet inspection as an option anymore.[37]

In the United Kingdom, the duty of care of Internet service providers has hitherto been based on the liability restrictions of the E-commerce Directive, as implemented in national legislation. A new act (the Digital Economy Act), however, was recently passed. By virtue of this new act, Internet service providers are to actively forward notifications of rightful claimants to alleged infringers. On the basis of the new provisions, the providers also need to keep lists of end-users who have been the subject of such notifications. They also need to make these lists with identifiable data available to rightful claimants to help detect repeated breaches by end-users. The Internet user's identity is not to be disclosed by means of these lists. If forwarding the notifications does not result in putting an end to the infringements, Internet service providers can be obliged to put technical restrictions on the use of Internet connections.

In Germany, the implementation of the E-commerce Directive is decisive for the duty of care of Internet service providers with regard to the protection of copyright on the Internet. The German regulations implement the provisions of the Directive literally.

In France, the new legislation, known as the HADOPI laws, has introduced new obligations for Internet access providers. These obligations are new in comparison with the existing duties of care arising from the E-commerce Directive regarding mere conduit, caching and hosting activities by Internet service providers.

Due to the end-users' obligation to secure their Internet connection to prevent copyright infringements – an obligation laid down in the French Code of Intellectual Property – Internet service providers must propose efficient technical measures that are suitable to that purpose. Such measures are included in a list prepared by the HADOPI authority (*Haute Autorité pour la Diffusion des Oeuvres et la Protection des Droits sur Internet*), which was set up pursuant

[37] *Kamerstukken II* (Parliamentary documents), 2009-10, 29838, nr 28.

to the new legislation. Additionally, Internet service providers must inform end-users in their user agreements about the possible sanctions in case of non-compliance with the aforementioned obligation. If the HADOPI authority, together with the judicial authorities, decides to intervene, Internet service providers can be required to send warning e-mails to end-users (stating that the unauthorized use has been detected) or, in the event of ongoing negligence, to cut off Internet connections. If Internet service providers fail to cooperate, they may be subject to a penalty.

The HADOPI legislation is very recent. Implementing regulations have not been adopted yet. The intended list of measures to secure Internet connections, on which Internet service providers are to advise end-users, has not been prepared either. No warning e-mails have been sent yet.

The interpretation in French jurisprudence of the duties of care of Internet service providers has focused primarily on the limitation of liability for hosting activities, as defined in the implementing legislation of the E-commerce Directive. Like in the Netherlands, most of the time, the interpretation is made by courts of lower instance – and not confirmed by higher courts.
Many cases concern the actual knowledge of hosting providers about the presence of unlawful material, which is required to establish intervention as an obligation for hosting providers, pursuant to the formulation of the liability restriction. In a few cases, hosting providers received an injunction, on the basis of their duty of care, to prevent any attempt to put the same content on the Internet again after it had been removed from a website for the first time.

It was generally emphasized in the interviews that the measures right owners wish to see are not covered by the liability restrictions of the E-commerce Directive. Internet service providers who are asked to detect and block Internet traffic that is in breach of copyright, run the risk of being held liable themselves. Furthermore, doubts were expressed about the technical feasibility of the detection of infringing material, which is passed on or stored by Internet service providers. Sending warning e-mails upon establishing the infringing nature of certain material was mentioned as an option.

Concerning the HADOPI legislation, interviewed stakeholders expressed many doubts. They warned that such stringent legislation might lead to the development and use of encryption technology for the distribution of copyright-protected material. Then, the use of the same technology could be used to share illegal content. Some emphasized that Internet service providers should not be put in the position to monitor Internet traffic or to contribute to punitive measures against end-users. There is also much doubt about the capacity of Internet service providers and of the judicial authorities to support the active approach of copyright protection prescribed by the HADOPI legislation. Investigating authorities also questioned the proportionality of the measures and pointed to the relationship with other investigating authorities with respect to cybercrime.

Some parties pleaded for considering the Internet a universal service, incompatible with drastic measures by Internet service providers. Plans for legislation similar to the French HADOPI regulations seem to be looked upon with growing reluctance in other countries. Many parties also pleaded for restraint when it comes to adopting HADOPI-like legislation. No experience has been gained yet as regards the effectiveness and applicability of such regulations.

Similar questions were raised in the context of the Digital Economy Act in the UK. Another issue with respect to the regulations in France and the UK is how they relate to the new Article 1, paragraph 3a of the Framework Directive, which stipulates that measures taken by member states regarding end-users' access to, or use of, services and applications through electronic communications networks shall respect the fundamental rights and freedoms of natural persons, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and general principles of Community law. This includes the right to privacy and rules on due process.

2.5 Identity fraud

Appropriating somebody else's identity in itself has not been made punishable in any of the countries under study. This means that, on the basis of the limitation of liability for Internet traffic as defined in the E-commerce Directive and implemented in all countries, Internet service providers do not have any special duty of care with regard to identity fraud.

The problem of online identity fraud has been related in particular to other service providers on the Internet, such as social networking websites and banks facilitating online transactions. Due to their involvement in Internet activities by means of which identity fraud is committed, these parties cannot appeal to the liability exceptions of the E-commerce Directive.[38]
The importance of a notification obligation for Internet service providers for security breaches involving personal data has recently been under discussion in the Netherlands at a parliamentary level. This might contribute to combating identity fraud on the Internet. This notification obligation is related to the new Article 4 of the Directive on privacy and electronic communications, which includes such an obligation for Internet service providers as discussed in the section on the theme of Internet security.

In the United Kingdom, the Fraud Act 2006 was recently passed, which includes a general penalization of fraud. This act was drawn up so as to include emerging practices with respect to new technologies as well.

38 The fact remains that general liability rules and privacy regulation apply to them.

In the German debate, phishing in particular has been discussed as a fraudulent practice on the Internet. Phishing is the practice by which existing websites are copied and a certain reliability of these copies is feigned although the websites are fake. These phishing websites are used to lure users into providing their identifiable data, such as log-in data. The discussion concentrated on whether such practices can be punishable under the current criminal legislation. A number of provisions were referred to that could cover phishing.

In France, it has been proposed to make appropriating somebody else's identity a punishable offence. Additionally, a technical tool (IDéNum) has been developed with which the authenticity of an online claim on somebody's identity can be established.[39] The French Government is the initiator of this tool and has made it available for general use by service providers.

From the interviews it becomes clear that it is complicated to have Internet service providers directly cooperate in combating identity fraud online. As an example, the fight against phishing was discussed. Effective combating by Internet service providers is primarily hampered because fraudulent websites use certain IP addresses only briefly or are hosted abroad. Some Internet service providers have indicated they are willing to take action within these technical limits after notifications of phishing websites, to prevent being blacklisted due to hosting such websites. Other measures are technically difficult to apply, and they conflict with the right to communication confidentiality and rules on privacy protection. Some parties warned against bringing too many subjects under the Internet service providers' responsibility.

In general, Internet service providers were not identified as the parties to be made accountable in this context. Social networking sites, banks and credit card companies have been mentioned as relevant parties.[40] It should be noted that these parties already take initiatives to counter fraud, whether or not in collaboration with the government.

Further education of end-users has been mentioned several times as a major element in countering identity fraud and has led in various countries to public campaigns, among other things.

2.6 Sale of stolen goods

The sale of stolen goods is mainly discussed in relation to platforms such as those of – globally operating – eBay, which is dominant in the countries under study (the Dutch platform Marktplaats.nl is also in the hands of eBay). Auction and selling platforms are the

[39] http://www.idenoum.com/.
[40] See also: Van der Meulen (2006) and (2009); Vermissen (2009).

most important players in the sale of stolen goods via the Internet. It can be derived from the interviews that beyond these platforms there are few problems of significance – for the scope of this study, that is. The conclusion is that the E-commerce Directive is the legal framework within which the discussion on this theme takes place. The status of the platforms involved is a fundamental issue. As regards the sale on auction and selling platforms of goods that breach intellectual property rights, a varying picture has emerged so far from court cases on different levels. All countries have jurisprudence in this field. In the terms of the E-commerce Directive, there is no unequivocal categorization of these platforms.

In Dutch jurisprudence, the status of auction sites such as eBay and Marktplaats has not been defined any further in relation to the E-commerce Directive. In case law, several requests for measures in connection with the sale of goods breaching intellectual property rights have been assessed in the context of general liability legislation. In this context, notice and take down is considered a proportional measure in the light of the care that may be required of these websites. In jurisprudence, preventive filtering of advertisements prior to their placement or the compulsory listing of such details as the advertiser's name, address and place of business are not acknowledged as suitable measures.

In the *L'Oréal v. eBay* case,[41] the High Court of the United Kingdom ruled in favour of eBay and acquitted this organization from liability for material offered by its users that breaches the trademark right of others.

In Germany, the *Bundesgerichtshof* (Federal Court of Justice) ruled in three different cases that online auction websites, in contrast to Internet service providers and other intermediaries, are directly responsible for offering counterfeit and pirated goods (*Störerhaftung*). In addition, this court has developed a preventive remedy for right owners against auction websites. This means that auction websites have a duty of care to prevent future breaches of intellectual property rights by users who have already been considered potential infringers. The court has ruled that the use of filter software can help and that such measures are not disproportionate.

Several courts in France, including a court of higher appeal, have ruled that eBay is to be regarded as a hosting provider and that it is not obligated to perform any preventive investigations into the integrity of the advertisements placed. The Court of First Instance for Commercial Law (*Tribunal de commerce*), however, refused to qualify eBay as a hosting provider in three decisions in 2008. This court held eBay liable for its lack of supervision and its failure to take efficient and suitable measures against the sale of counterfeit and pirated goods.

[41] See paragraph 1.3.6.

In France, there are several recommendation documents, prepared by expert groups and initiated by the government. One of these pertains to the trade in cultural goods and recommends, among other things, the creation of a register of (stolen) cultural goods. It is specifically aimed at cooperation between online selling platforms and trademark owners to counter the online trade in counterfeit and pirated goods. There have been governmental discussions about which activities of platform providers could be subject to the liability restriction for hosting providers in the E-commerce Directive (and implemented in French law). To date, the recommendations and discussion in this respect have not led to any changes in the legal provisions.

It was widely expressed in the interviews that Internet service providers are not always the proper parties for regulating the online sale of stolen goods. Some of the Internet service providers indicated they had never received a request for intervention with respect to stolen goods. Others indicated they were prepared to cooperate with the judicial authorities and the police if asked to do so. Checking Internet traffic for this aspect is not effective, and it is technically unfeasible. A formal duty of care would lead to excessive intervention by Internet service providers and possibly could escalate in the creation of further duties of care in other fields. Intervention with regard to illegal content in general might be next and would result in disproportionate restrictions on (future) economic activities on the Internet.

In general, platform providers that facilitate the online sale of goods are seen as the key players. These platform providers have introduced self-regulation, on account of the fact that the reactions of the users of such platforms provide a major motivation to take responsibility for this problem. This self-regulation mainly consists of forms of notice and take down procedure by eBay and others, with these parties referring to the liability exception that applies from the implementation of the E-commerce Directive for service providers that perform hosting activities. In their opinion, the exception is also applicable to them.

Platforms for the online sale of goods have taken several initiatives setting up procedures for the handling of complaints about offers of stolen goods and counterfeit and pirated goods. Additionally, users are informed about existing procedures and about the regulations that apply.

There is collaboration with the judicial authorities and the police, who can count on an active response from the platform providers. There are also active consultations with the judicial authorities and the police about the reactions of the original owners of stolen goods. Debate on the sale of stolen goods and fraud often leads to the conclusion that these are civil matters (for instance with regard to claiming compensation for the financial damage incurred).

Intellectual property right holders, especially trademark owners, put much pressure on platform providers. The measures they have asked for are reflected in several legal proceedings. Their requests have been partly met by the procedure provided via the Verified Right Owner Programme (VeRO), in which especially eBay has invested.[42] This procedure also relates to the identification of rightful claimants and to identifying relationss with advertisements on the platforms afterwards [Nico, this yellow part is not very clear, especially the word "afterwards".].

[42] http://pages.ebay.nl/vero/.

3 Analysis and conclusions

3.1 Introduction

The environment of the subject under study is dynamic. In addition to the sketch in the previous chapter, some general observations are provided here and conclusions are formulated.

3.2 Value chain

The research question is focused on duties of care in the context of the relationship between the government and Internet service providers. On both a national and international level, Internet service providers receive a lot of attention, not only with respect to their relationship with the government, but also in connection with other civil-law parties, for instance regarding the issue of liability (under civil law). This study pertains to the former relationship. If there is no such relationship, it has been investigated if duties of care exist elsewhere in the value chain that Internet service providers are part of.

In section 1.3, it is stated that Internet service providers are among the players who are active in the (economic) value chain between end-users and the providers of services. This is confirmed when we hold the five themes up against the light. In several parts, specific duties of care for Internet service providers can be discerned, arising from the sector-specific regulation or in consequence of the rules on E-commerce. With other themes, duties of care are rather seen in relation to other parties in the value chain, more specifically the parties that offer specific services or that facilitate the operation of platforms for such services.

At first sight, putting the responsibility on the Internet service providers seems to be a simple option. After all, the Internet service providers are the ones who control the end-users' access to the Internet. Internet service providers are gatekeepers, and they fulfil a bottleneck job.

At the same time, it becomes clear that this approach is less and less compatible with the dynamics of the Internet (such as the involvement, as described, of many – interacting – parties), with the associated business models, with considerations of efficiency and with aspects of general interest. It is true that Internet service providers are pivotal, but they

constitute just one of the parties in a complex value chain. Putting the duties of care only on the Internet service providers causes an imbalance, which on the one hand does not do justice to the providers' position, and on the other hand brings with it some adverse effects for the provision of services and innovation, for instance. After all, Internet service providers will assess their risks on the basis of their own business model. If this allows only a limited risk margin, it is likely that the risks will be ruled out or mitigated, with the result that services that increase the risk will no longer be accessible for end-users or that new services will not be developed. Efficiency considerations are also important: after further testing, seemingly obvious solutions may appear to be inefficient or may appear to lead to high costs (this is the case with filtering or deep packet inspection, for instance). The general interest plays a role when it comes to securing access to the Internet for everybody at affordable rates.

The importance of a value-chain oriented approach is gaining attention in the literature,[43] but it is also endorsed by many of the interviewees. Internet service providers in particular are critical of the extent to which they are considered to have duties of care. They blame this partly on their high profile and the direct relationship they have with the end-users. At any rate, other parties in the value chain agree that in many cases Internet service providers are not the party with whom the duties of care should rest, and they take a stand themselves as well. This is apparent, for instance, in their involvement in the fight against child pornography, in enforcing copyright, in countering identity fraud or the sale of stolen goods and in promoting Internet security. The concept of a value-chain approach would therefore deserve further attention.

3.3 Position of Internet access providers

Internet service providers provide access to the Internet to end-users and additionally perform various other tasks, such as hosting personal pages on websites or supplying added value services, such as e-mail. In the study, it becomes clear that sufficient importance should be attached to this distinction. In their capacity as access providers, the Internet service providers are subject to the light e-commerce regimen of "mere conduit" anyway, but they also claim that the message/content is of no concern to them and that they, as transporters, cannot be held responsible for the content of what they transport.

As transporters the Internet service providers are required to respect the confidentiality of communications, it is stated, and therefore they cannot actually bear any responsibility for what Internet users (or service providers) do on the Internet. Some access providers believe that, in principle, they are obliged to allow spam to pass through, for instance – after all, the traffic between providers and users is not to be hampered – but they use spam filters on the basis of their contractual relationship with the end-users. In this context, it is important

[43] OECD (2010); Dommering and Van Eijk (2010); Rand Europe (2008); Ofcom (2008).

to ascertain where the protection that goes with the "mere conduit" regime of the E-commerce Directive begins and ends. Can the Internet service provider as an access provider be strictly separated from the Internet service provider as a provider of additional services, such as spam filtering? Are such services to be regarded as a separate category or is this a matter of activities that are subject to (or are to be included in) the rules for hosting/caching?

These arguments partly coincide with the viewpoints that are generally expressed in the discussion about Internet neutrality. Supplementary to this, it is argued that Internet access can be regarded more and more as a universal service. Even though providers are each other's competitors, they believe that end-users are entitled to Internet access and that in principle they cannot discriminate against users at admission.

3.4 Notice and take down dominant

In summary, it can be concluded that with three of the five themes (copyright, child pornography and the sale of stolen goods) notice and take down systems are dominant mechanisms. As the occasion arises, the regulations prescribe that Internet service providers are to set up notice and take down procedures to comply with their duties of care. Where no specific legal obligation is in place, the study indicates that Internet service providers have implemented notice and take down procedures at their own initiative so as to be able to appeal to the diminished liability regime for hosting and caching activities.

However, notice and take down also often occurs outside the circle of parties that are subject to the hosting and caching exceptions, such as among platform providers and other intermediaries (e.g. search engines). They mostly cannot refer to a special legal rule (there are countries that have extended the protection of the e-commerce rules to other players in the value chain, including platform providers),[44] but they use notice and take down to limit their general responsibility under civil law. Since the legal framework has not been defined any further, it is not clear to what extent a similar appeal to diminished liability is justified, as stipulated for the parties to which the provisions of the E-commerce Directive apply.

Notice and take down procedures have already been the subject of detailed study and evaluation, as described in section 1.3.2, but should be given closer attention. What is more, the revision of the E-commerce Directive is one of the points of action on the European Digital Agenda.

[44] See Van Hoboken (2009) and the European Commission (2003).

3.5 Local context

From the stocktaking and analysis of national regulations in combination with the interviews it becomes clear that national circumstances are partly decisive for the way in which the regulations are set up. In the United Kingdom, self-regulation has traditionally been highly developed. This is also reflected in the system adopted for combating child pornography, which goes beyond merely a notification system. In France, the emphasis is rather on regulation through legislation, and self-regulation is clearly less developed than in the United Kingdom. Germany's position is closer to that of the United Kingdom than to the French position. In great outline, the Dutch position seems to be close to the German position. There is self-regulation, and it works, certainly in the case of child pornography. The code of conduct for notice and take down provides some added value but also has its weak sides, such as the wide possibilities of interpretation and the absence of an enforcement mechanism.

3.6 Enforcement problems

The enforcement of the applicable code faces several critical factors. Firstly, as to enforcement under penal law, there is always a balancing act between the seriousness of the case and the available means. With child pornography, a substantial investigation structure is in place, but it is not always sufficient. Furthermore, where traditional investigation methods – whether or not supplementary – are called in, they appear to be equally effective and at times in themselves sufficient. The associated dilemmas for the Netherlands have already been well identified,[45] and the interviews show that elsewhere, too, comparable problems are struggled with, including the lack of sufficient knowledge about the technological aspects.

Making filters compulsory was mentioned in several interviews. There is much hesitation about the effectiveness of filtering, which is also confirmed in the literature.[46] Those who really set their minds on it, can easily circumvent the filters. Filters would make things invisible at best, but they do not stop the unlawful activity. Filtering may thus become an excuse for not optimizing the combat against the underlying illegal activities. Other issues are involved as well, however, such as who is liable for the good functioning of filters, what the risks for underblocking/overblocking/mission creep are, what the proportionality of the measures is, etc. These issues are not new, but they always come up in discussions about filtering. Strikingly enough, various respondents (also from the side of the authorities involved) recognize the limits of filtering. Others consider filtering the ultimate remedy: if enforcement comes up against the absence of jurisdiction, filtering could be deployed as an option.

45 Stol et al (2008).
46 See for instance Stol (2008); Callanan et al (2009).

In the interviews, it is further indicated that there is much hesitation about deploying criminal measures as part of recent legislation in the field of copyright. Especially in France, where this new legislation is in its implementation stage, there are some doubts as to its effectiveness, for instance with regard to the fact that large groups of the population will be discriminated against and that the regulation has strongly political overtones. Additionally, the social resistance phenomenon is referred to: the authorities involved allegedly have different priorities and would be facing a proportionality problem, and the judicial institutions are said not to have the capacity to deal with a large number of cases. Like elsewhere, the question is asked whose problem is solved here, with an implied reference to the sector's own responsibility as to guarding its own economic interests, such as the development of new business models. Finally, several parties have expressed their concern that peer-to-peer will go underground and will use encryption on a massive scale. This would create an untraceable communication network in which large sections of the population participate. There is the risk that this network will also be used for purposes other than merely distributing copyright-protected material.

Deep packet inspection as an enforcement method has been suggested but meets with strong opposition. Internet service providers refer to the principle of confidentiality of communications and state that permanently monitoring all Internet traffic is very expensive. Experts ask questions about the proportionality/legitimacy of deep packet inspection.

When new regulations are imposed, it is important that sufficient attention is paid to the proportionality of the measures proposed and the consequences for enforceability.

3.7 Answering the research question

In the first place, the research question is focused on the forms of duty of care that apply to, or are developed for, Internet service providers in the countries under study, the role of the government and the underlying motivations for the chosen approach, and the experience gained. The various sub-aspects of the study question are discussed in the country-specific studies, but are briefly summarized here as well, and they are described in the conclusions in the next section.

With respect to the five themes, the governments opt for keeping a wide range of regulatory possibilities open. Only to a very limited extent is it true that the government remains completely uninvolved and that the initiative is entirely left to the market parties. There is rather a trend from less involvement towards more involvement, with a strong emphasis on forms of coregulation and self-regulation, affected by European regulatory frameworks. These frameworks prescribe explicit national implementation, for instance in the case of Internet security (as part of the European regulatory framework for the communications sector) and the E-commerce Directive. In some cases, an additional responsibility has been laid down in regulations, for instance prescribing a notice and take

down procedure for caching and hosting. Such a procedure is not compulsory under the E-commerce Directive, although its introduction is a logical consequence. Nevertheless, countries opt for securing the procedure and giving it a legal context, partly because of the way in which regulatory issues are being dealt with nationally or depending on considerations on whether and how legal certainty should be provided to market parties. In the field of child pornography, self-regulation and coregulation are at the basis of defining duties of care, possibly because of the fact that there has been much European guidance and because the subject can count on a strong willingness among the market parties to cooperate. Governments clearly promote the current notification system and also provide (financial) support. In general, the current system of responsibilities of Internet service providers regarding child pornography is viewed positively. With respect to issues of a more radical nature, such as filtering, the national law system requires a specific legal basis (see the discussion in the Netherlands on filtering). The radical nature in itself may render defining the legal framework especially important, for example for reasons of legal certainty.

The Internet service providers' role as regards the copyright theme is a good example (in two countries) of drastic government intervention through regulations and is the subject of much discussion. In this controversial matter, coregulation or self-regulation was obviously not an option. For the time being, there is no experience with the respective regulation, as it is still in an implementation stage. The question is if the chosen approach has not been espoused too enthusiastically and if such aspects as the enforceability and the social basis have been given sufficient consideration.

Unlike Internet security, which has a clear legal framework, a legal framework is not defined for the sale of stolen goods. Nevertheless, the regulation of Internet security (Article 4 of the Directive on privacy and electronic communications) still raises several questions. A need for further (European) guidance is discernible. It can be deduced from the study that, as regards the sale of stolen goods, this is considered a problem which primarily occurs elsewhere in the value chain (on the level of platform providers), so that no special role has been assigned to Internet service providers.

In the study, it becomes apparent that as to the chosen approach the critical limits of several aspects are coming into view. Advancing insights and the relevance of the value chain are at play here. Where e-commerce is concerned, things are more clearly discernible. Questions have arisen about the scope of the current regulations, with respect to both the conceptual framework (e.g. the question about which parties may claim a hosting status) and how to deal with other players in the value chain, such as platform providers. With Internet security, the increased strictness of the provisions in the European directive framework and the introduction of a notification obligation provide new impulses for discussion on the position of the government and supervision on the one hand, and the Internet service providers' responsibilities on the other hand. Given the new regulations to be implemented in the member states, a more active involvement from the side of the

government and supervisors (in the communication sector as well as from a privacy perspective) is likely.

3.8 Conclusions

A varied picture emerges from the study, which indicates that the developments, including improving the balance within the value chain, are still underway. Internet security, more particularly with regard to the relationship between the Internet service provider and the end-user, is still in its infancy. This does not mean that nothing is happening in practice, but formally a framework has hardly been defined and there is little self-regulation at this stage. On the other hand, there is a virtually identical regimen for child pornography in the countries under study, where parties are prepared to provide far-reaching assistance in combating this phenomenon. The (INHOPE) notification system is found in all countries either on the basis of self-regulation or in consequence of a legally defined duty of care. The use of filtering is a recurring issue in the prevention of the proliferation of child pornography. Much attention is devoted to copyright, and in two countries the regulations on copyright have been tightened, so that it has become possible to restrict Internet access or to cut end-users off from the Internet. There is strong criticism against the new rules, and from the interviews it becomes clear that the actual enforcement possibilities are subject to much criticism as well. Identity fraud is mainly tackled in the context of the consequences of identity fraud. Making identity fraud punishable in itself (besides the possibilities already in place to act under public law) is generally not deemed necessary. The sale of stolen goods via platform providers (i.e. auction and selling sites, etc.) is considered the platform provider's prime responsibility.

The varied picture and the still dynamic nature of the subject make it hard to define proven best practices. Yet, the data gathered in the study provide some interesting information.

On the basis of their study, the researchers come to the following conclusions:

1. Towards a value-chain approach
Duties of care, as analysed in the study, cannot be linked to one specific party in the value chain between Internet service providers and end-users, but they should be the joint, well-balanced responsibility of the stakeholders in the value chain. Only then, undesired obstacles to Internet access can be prevented and innovation will not be stifled. With the possible introduction of new obligations, it should be tested in advance what their effects on the value chain will be (such as implications for business models and innovation).

2. Testing effectiveness and enforceability in advance

Testing in advance of (intended) legal intervention as regards effectiveness and enforceability contributes to preventing symbolic legislation and undesired (social) effects.[47]

3. Deployment of notice and take down procedures

Notice and take down procedures appear to be a widely accepted mechanism. The procedures are not only used by Internet service providers (in their capacity as providers of hosting and caching services). Other parties in the value chain, such as platform providers, have similar procedures. Most of the countries under study do not have a specific legal basis for these procedures, although there are some initiatives in the field of self-regulation and coregulation. It is advisable to set a more detailed framework for notice and take down, to define/vary the circle of parties that can use such procedures more closely and to indicate what the effects of such procedures are. Problems related to notice and take down, and more generally the position of the E-commerce Directive, have already been the subject of study but need to be looked into more closely. It is a telling sign that no proposals have yet been made for adjusting the E-commerce Directive, although such proposals have been announced in the context of the European Digital Agenda.

4. Clarifying Internet security and privacy

The new rules on Internet security and privacy (Article 4 of the European Directive on privacy and electronic communications) are unclear and require further specification as to their meaning and impact. In principle, it is a European task to prevent differences on a national level that are too significant. A clearer dividing line between security issues that touch on the relationship between Internet service providers/end-users and security issues on a national level is desirable.

5. Increase in the state of knowledge

The need for further regulation is partly fuelled by the lack of sufficient technical and practical knowledge. There appear to be many knowledge gaps in relation to the problems under study in particular. When end-users, supervisors, enforcers and regulators gain further knowledge, this may contribute to less regulation pressure. The importance of education is widely supported.

[47] See the German discussion on filtering of child pornography and what is said in the interviews about the implementation/application of the French HADOPI legislation.

4 Bibliography

Boer & Grimmius (2009)
L. Boer & T.K. Grimmius, *Melding maken? Internationale quick scan meldplicht gegevensverlies*, research commissioned by the ministry of Economic Affairs, Research voor beleid, 2009

Chavannes (2007)
R. Chavannes, 'Brein/KPN: het gevaar van een bagatel', *Mediaforum* 2007-6, p. 177.

Callanan e.a. (2009)
C. Callanan, M. Gercke, E. de Marco & H. Dries-Ziekenheiner, *Internet Blocking, balancing cybercrime responses in democratic societies*, research commissioned by the Open Society Institute, 2009.

De Cock Buning & Van Eek (2009)
M. de Cock Buning & D. van Eek, 'Aansprakelijkheid van derden bij auteursrechtinbreuk', *IER*, 2009/5, 10/2009, p. 224-232.

Coupez (2010)
F. Coupez, 'Obligation de notification des failles de sécurité: quand l'Union européenne voit double...', François Coupez, <www.juriscom.net>, 30 January 2010.

Dommering & Van Eijk (2010)
E.J. Dommering & N.A.N.M. van Eijk, *Convergentie in regulering: Reflecties op elektronische communicatie*, Ministry of Economic Affairs, 's-Gravenhage, March 2010.

Dumortier & Somers (2008)
J. Dumortier & G. Somers, *Study on activities undertaken to address threats that undermine confidence in the Information Society, such as spam, spyware and malicious software*, Time.lex CVBA, Brussels, 2008.

Van Eeten, Bauer & Tabatabaie (2009)
M. van Eeten, J.M. Bauer & S. Tabatabaie, *Damages from Internet Security, A framework and toolkit for assessing the economic costs of security breaches*, research commissioned by OPTA, TU Delft, February 2009.

Van Eeten, e.a. (2010)
M. van Eeten, J.M. Bauer, Hadi Asghari, Shirin Tabatabaiea, & Dave Rand, *The Role of Internet Service Providers in Botnet Mitigation An Empirical Analysis Based on Spam Data,* http://weis2010.econinfosec.org/papers/session4/weis2010_vaneeten.pdf

European Commission (2003)
European Commission, *First Report on the application of 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* (Directive on electronic commerce), COM(2003)702 def.

Gercke (2006)
M. Gercke, 'Zugangsprovider im Fadenkreuz der Urheberrechtsinhaber: Eine Untersuchung der urheberrechtlichen Verantwortlichkeit von Downloadportalen und Zugangsprovidem für Musikdownloads', *Computer und Recht* (2006) 22:3, p. 210-216.

Gercke (2009)
M. Gercke, 'Die Entwicklung des Internetstrafrechts im Jahr 2008', *ZUM* (2009), p. 526-538, 528.

Van Hoboken (2009)
J.V.J. van Hoboken, 'Legal Space for Innovative Ordering. On the Need to Update Selection Intermediary Liability in the EU', *International Journal of Communications Law & Policy*, 2009-13, p. 1-21.

Van der Hulst & Neve (2008)
R.C. van der Hulst & R.J.M. Neve, *High-tech crime, soorten criminaliteit en hun daders*, WODC, 2008.

Elkin-Koren (2006)
N. Elkin-Koren, 'Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic', 9 *N.U. J. Legis. & Pub. Pol'y* 15 (2006).

Kuner e.a. (2009)
C. Kuner, C. Burton, J. Hladjk & O. Proust, *Study on Online Copyright Enforcement and Data Protection in Selected Member States*, Study commissioned by the European Commission, Hunton & Williams, 2009.

Van der Meulen (2006)
N. van der Meulen, *The Challenge of Countering Identity Theft: Recent Developments in the United States, the United Kingdom, and the European Union*, Tilburg: International Victimology Institute Tilburg, 2006

Van der Meulen (2009)
N.S. van der Meulen, 'Identiteitsfraude: de eerste stap, nu nog de rest', *Computerrecht* 229,38, p. 61-64.

OECD (2010)
OECD, *The Economic and Social Role of Internet Intermediaries*, Paris, April 2010.

Ofcom (2008)
Ofcom, *Ofcom's Response to the Byron Review,* 2008
(http://www.ofcom.org.uk/research/telecoms/reports/byron/).

Rand Europe (2008)
Rand Europe, *Responding to Convergence: Different approaches for Telecommunication regulators*, 2008.

Ringnalda, Elferink & De Cock Buning (2009)
A. Ringnalda, M. Elferink & M. de Cock Buning, *Auteursrechtinbreuk door P2P filesharing, regelgeving in Duitsland, Frankrijk en Engeland nader onderzocht*, WODC, 2009

Schellekens, Koops & Teepe (2007)
M.H.M. Schellekens, B.J. Koops & W.G. Teepe, *Wat niet weg is, is gezien. Een analyse van art. 54a Sr in het licht van een Notice-and-Take-Down-regime*, Tilburg, November 2007.

Stol e.a. (2008)
W.Ph. Stol, H.W.K. Kaspersen, J. Kerstens, E.R. Leukfeldt & A.R. Lodder, *Filteren van kinderporno op internet, Een verkenning van technieken en reguleringen in binnen- en buitenland*, WODC, 2008.

Spindler & Verbiest (2007)
T. Verbiest & G. Spindler, *Study on the Liability of Internet Intermediaries*, study commissioned by the European Commission (contract ETD/20-06/IM/E2/69), November 2007.

Stratix (2007)
Stratix Consulting, *Onderzoek inzake Artikel 11.3 Tw, Concept Dreigingsbeeld,* Hilversum, 2007.

TNO/SEO/IVIR (2009)
Ups and downs. Economische en culturele gevolgen van file sharing voor muziek, film en games, a study by TNO Information and Communication Technology, SEO Economic Research and the Institute for Information Law, commissioned by the Dutch Ministries of Education, Culture and Science, Economic Affairs and Justice, February 2009.

Thoumyre (2008)
Lionel Thoumyre, 'Précisions contrastées sur trois notions clés relatives à la responsabilité des hébergeurs', 35, *Revue Lamy Droit de l'Immatériel*, Février 2008.

Vermissen (2009)
J.A.G. Vermissen, 'Sociale netwerken en privacy', *Privacy & Informatie* 2009-5, p. 233-237.

De Vries e.a. (2007)
U.R.M.Th. de Vries, H. Tigchelaar, M. van der Linden & A.M. Hol, *Identiteitsfraude: een afbakening, een internationale begripsvergelijking en analyse van nationale strafbepalingen*, WODC/ Universiteit Utrecht, 2007.

Appendixes

1. Country studies

The Netherlands

General introduction

I. Current regulations

Legislative framework:

There are several legislative provisions in the initial law implementing the E-commerce Directive (2000/31/EC) which set out the framework defining the liability of Internet service providers with respect to data transmitted and stored in the online environment.[48] These provisions demand measures of Internet service providers relating to all of the themes that are discussed in the following paragraphs and there, when relevant, references are made to this introductory part for a detailed description of these provisions.

Implementing Articles 12 to 15 of the E-commerce Directive (2000/31/EC), Article 6:196c of the *Burgerlijk Wetboek* (BW – Civil Code) contains safe harbour provisions which exempt "providers of information society services" from civil liability for providing certain information, put on their facilities by others, under certain circumstances. The article, in paragraphs 1, 3 and 4, refers to Article 3:15d §3 BW for a definition of the service providers that fall under the scope of the provisions. A key requirement in this definition is that the economic activity involved in the provision of such services must be understood to encompass more than only direct online transactions. Also, the services should be used "at a distance", i.e. in a geographical sense, by electronic means through a system of storage and processing of data, and on individual request.

The provisions outline a duty of care by creating a safe harbour for these types of service providers in relation to the transmission and storage of information occurring while executing requests for their services, as far as the providers transmit or store publicly available information on their facilities. The conditions for benefiting from the safe harbour, summed up in a limitative manner by these provisions, make clear which measures the providers should take to exempt themselves from liability as regards certain information originating from their subscribers and users. The provisions contain a distinction between mere conduit, caching, and hosting activities. The providers addressed by Article 6:196c BW can only rely on the safe-harbour provisions therein when it can be said that they in no way are involved other than by providing the technical means to facilitate the communication concerned.

48 Aanpassingswet richtlijn inzake elektronische handel [Implementation Law Directive on Electronic Commerce], Stb. 2004, 210; *Kamerstukken II* 2001/02, 28 197 [Explanatory memorandum to the Implementation Law Directive on Electronic Commerce]

The article explicitly states, in §5, that the provisions do not exclude the possibility of obtaining a court order to end or prevent the distribution of information by the Internet service providers concerned. The provisions contain no general obligation to monitor the information which the providers transmit or store or to actively seek facts or circumstances indicating illegal activity, in line with Article 15 §2 of the E-commerce Directive. No duty to report to the competent public authorities alleged illegal activities undertaken or information provided, which Article 15 §2 of the E-commerce Directive leaves as an option for the member states, has been implemented.

Article 6:196c §1 deals with mere conduit activities by the providers in question. Mere conduit covers transmitting information of others and giving access to the provider's communication facilities. §2 of the article states that storing information temporarily, in a interim manner and automatically for the sole purpose of transmitting this information, with a duration that is only reasonably necessary for this purpose, falls under "transmitting" and "providing access" as mentioned in §1. As long as Internet service providers do not cache or host information on their servers, in the sense respectively of §3 and §4 of the article, they do not have to take any measures, provided they do not initiate the transmission, do not decide who will receive the information and do not select and/or amend the transmitted information.

Article 6:196c §3 BW covers caching activities, in the sense of storing information of others for the sole purpose of making this information available on request of third parties more efficiently, all in an automated, interim and temporary manner. Internet service providers have to meet five cumulative requirements to avoid liability for caching information on their facilities. First, they should not alter the information. Second, they have to comply with the conditions on access to the information. Third, they need to comply with rules, widely recognized and used by the relevant industry sector, on updating the information. Fourth, they should not alter the technology widely recognized and used in the relevant industry sector to obtain information on the use of the information. And fifth, Internet service providers do have to make sure they can react, by way of promptly taking measures to remove or disable access to the cached information, upon obtaining knowledge of the fact that at the original location in the communication network the infringing information has been removed or access to it has been blocked, or of the fact that a competent authority has ordered to remove or block the information.

Hosting providers are addressed by Article 6:196c §4 BW. It concerns service providers who, pursuant to the definition of Article 3:15d §3 BW, offer hosting services in the sense of storing information upon the request of others. These providers have to take measures in order to avoid liability only if they have actual knowledge of the unlawful character of an activity or information hosted by them for others, or, as regards civil claims for damages, if they should reasonably be aware of facts and/or circumstances clearly pointing to this unlawful character. For this knowledge to be established, a notification in itself is

not enough. It should concern manifestly unlawful activities or information. It could be the nature, quality or status of the information which makes it unlawful or punishable. Under these circumstances, the hosting providers have to promptly remove or disable access to the unlawful material.

Next to the safe-harbour provisions of Article 6:196c BW, Article 54a of the *Wetboek van Strafrecht* (Sr – Criminal Code) contains an exemption from prosecution which could function as a safe-harbour for providers of telecommunication services in a similar way to Article 6:196c BW. In addition, Article 125o of the *Wetboek van Strafvordering* (Sv – Code of Criminal Procedure) provides legal grounds to block access to or remove content in an "automated work". Both articles are explicitly mentioned in the explanatory memorandum to the implementation law of the E-commerce Directive, as being intended to serve as the legal ground for the implementation of the safe harbour provisions for intermediaries in Articles 12 to 15 of the Directive, in the context of criminal procedures.

Article 54a Sr states that intermediaries, who provide telecommunications services consisting of the transfer or storage of data originating from others, will not be prosecuted in connection with these activities as long as they comply with an order by a public prosecutor to take all reasonable measures to prevent access to data under investigation. The order needs to be authorized by an examining judge on request of the public prosecutor.

Article 125o Sv provides the legal ground for investigation and prosecution authorities to make data, which have been encountered during a search in an "automated work" with which a punishable act has been performed, inaccessible to the extent that it is necessary to end the punishable act or to prevent further punishable acts from being committed. The act of making the data inaccessible needs to be authorized by a public prosecutor or an examining judge (§1), and must ensure that the original content manager and third parties are prevented from further accessing and making use of the data and that further distribution is prevented (§2). As soon as the data seizes to be relevant to the criminal proceedings, it should be made available again to the original content manager upon authorization by a public prosecutor or an examining judge.

Other regulatory measures

The measures required by the safe-harbour provisions of Article 6:196c BW and Article 54a Sr to avoid liability or prosecution, as described above, essentially demand of the Internet service providers covered by such articles to have some form of notice and take down (NTD) procedure in place. There are no statutory NTD procedures in the Netherlands to give further substance to these requirements for these Internet service providers.

The *Gedragscode Notice-and-Take-Down* (Notice and Take down Code of Conduct) provides general standards for NTD procedures for intermediaries who provide a "public telecommunications service on the Internet" (Article 1b) and have to deal with complaints about unlawful and/or punishable content in the online environment. The code was set up by the Dutch Government, Internet corporations and interest groups.[49] The first version of the code was coordinated by the *Nationale Infrastructuur ter bestrijding van Cybercrime* (NICC – National Infrastructure to fight Cybercrime), which is directly supervised by the Ministry of Economic Affairs. The founders of the code administer it on a continuous basis, currently through the *Platform voor de InformatieSamenleving* (ECP-EPN – Platform for the Information Society), a negotiation platform for government bodies and private companies. The ECP-EPN also hosts the *Platform Internetveiligheid* (Internet Safety Platform), which is intended as a strategic discussion forum for government and private parties to develop initiatives to enhance Internet safety, like the code.

The standards in the *Gedragscode Notice-and-Take-Down* are arranged in articles, to which an explanatory memorandum has been added. The articles set out how the intermediaries concerned should deal with (valid) complaints about unlawful and punishable content, like the distribution of illegal goods or child pornography. A special mention is made in the memorandum to "undesirable" content; as regards this category of content, it is suggested that the addressed intermediaries can decide on their own what types of information they consider to fall under it and if they want to deal with it in the same way as unlawful and punishable content. Article 3b suggests that intermediaries use their customer agreements to describe their criteria to deal with undesirable content. The code gives guidelines on how to assess whether a complaint is valid or not, and on which steps need to be taken following a decision by the intermediary that taking down the material is the proper response to a valid complaint. Article 1c states that the code is not applicable where, based on law and case law, other obligations on the intermediaries are in force. In the memorandum, it is specified that the code does not create new statutory obligations. The memorandum refers to the liability regime for Internet service providers of Article 6:196c BW.

Several, including the largest, Dutch Internet providers have issued policy rules on the NTD-procedure they use.[50]

---

49 See http://www.ecp-epn.nl/werkgroep-notice-and-takedown for a list of the initiators and subsequent supporting parties.

50 As examples, the following can be mentioned [Dutch only]: KPN has issued the "Klachtenprocedure Internet", see: http://www.kpn.com/prive/service/veiligheid/abuse/welke-incidenten.htm; UPC has issued the "Regeling Notice & Takedown", see: http://www.upc.nl/pdf/upc_internet_veiliginternet notice_&_takedown.pdf; SIDN has issued the "Notice-and-Take-Down-procedure voor .nl-domeinnamen", see: http://www.sidn.nl/ace.php/p,727,6106,2118423720,021009_-_Notice-and-Take-Down-procedure_voor_nl-domeinnamen_pdf; XS4all has issued policy rules on the NTD-procedure it uses in 2007, which have been influential in the development of the Dutch Notice and Takedown Code of Conduct. See: http://www.xs4all.nl/overxs4all/contact/media/beleidsregels_klachten.pdf

II. Application of the current regulations

Legislative framework

The explanatory memorandum to Article 6:196c BW states that the measures that can be demanded pursuant to the safe-harbour provisions of the article, like the removal of a website, should be reasonable and proportionate considering the costs and the technical and personnel requirements for the Internet service providers concerned, and should be subsidiary.[51] Although it is clear that the provisions of Article 6:196c BW require some form of NTD procedure by the service providers concerned, so far it has been deliberately left to co-regulatory and voluntary self-regulatory measures to provide details on such procedures. There are no statutory regulations on who should judge the proportionality of the measures in question.

In the case of *Lycos v. Pessers*, concerning an anonymous publication on a website, which according to Pessers was unlawful because of a false accusation, the court formulated a new duty of care for Internet service providers, with its own conditions, with regard to requests for subscriber details like names, addresses and domiciles.[52] The *Hoge Raad* (Dutch Supreme Court) confirmed the standards which the *Hof Amsterdam* (Amsterdam Court of Appeal) had formulated as guidelines to evaluate the necessity for Internet service providers to provide identifying data of information providers of allegedly unlawful content. An Internet service provider should provide such identifying data when there is a substantial likelihood that the content is unlawful and could cause harm, the person requesting the data has an actual interest in obtaining the data, there is no less far-reaching measure available to obtain the data and the interest of the requesting party outweighs the interests of the Internet service provider and, in this case, the website owner.

The E-commerce Directive has left open the question if, and under which conditions, Internet service providers have to react to such requests from civil parties. According to the Dutch Government, in light of the judgment of the Court of Justice of the European Union in the case *Promusicae v. Telefónica de Espaáa SAU*, the standards of the *Lycos v. Pessers* case appear satisfactory.[53]

Recent case law on allegedly defamatory information on websites also concerns the provisions of Article 54a Sr. For example, an examining judge refused to authorize a public prosecutor to order the Dutch Internet service provider Budget Webhosting to take down content. In spite of this, the public prosecutor went ahead and issued an NTD-order against

51 *Kamerstukken II* 2001-02, 28197, nr. 3, p. 51. [Explanatory memorandum to the Implementation Law Directive on Electronic Commerce]

52 Hoge Raad [Supreme Court of the Netherlands] 25 November 2005, Mediaforum 2006-1, nr. 1 with note by. A.H. Ekker, Lycos Netherlands B.V. versus A.B.M. Pessers [in Dutch].

53 *Kamerstukken II* 2007-2008, 29838, nr. 7, p. 2-3. See also: Kamerstukken II 2007/08, 28684, nr. 133, p. 2-3. [parliamentary documentation]

Budget Webhosting, which the Internet service provider refused to follow because the order lacked the approval of the examining judge. Before the court, the public prosecutor argued that the situation would have been unsatisfactory if no order were to be possible, because there had been no real evaluation of the allegedly illegal contents by the examining judge and there was no way under current law to ask for judicial review of the examining judge's decision. The court indicated that the Dutch legislator should deal with such a question and not the judicial branch. The prosecution thus had been unlawful.[54]

Other regulatory measures

The E-commerce Directive, for example in recital 40, also encourages member states to promote coregulatory and self-regulatory measures. The Dutch Government has supported this and has left the development of procedures for dealing with notices on unlawful activities and information deliberately to coregulation and voluntary self-regulatory measures.[55]

There is no formal list of members adhering to the *Gedragscode Notice-and-Take-Down*. Companies and intermediaries that implement this code of conduct should make this known themselves. Implementation of and compliance with the code is voluntary. There is no possibility, as the explanatory memorandum in the code explicitly states, to formally enforce compliance with the code.

The code mentions in Article 6c the option for intermediaries to decide to provide contact details, like names, addresses and domiciles, of the information provider to the person filing a notice. In the explanatory memorandum, the standards for the evaluation needed in such a case, as developed in case law like the *Lycos v. Pessers* case discussed above, are reiterated. It is mentioned in the memorandum that there is no statutory obligation for intermediaries to retain such contact details of its users and subscribers. It should be noted that the code contains no standards on how to react when an intermediary's evaluation of the unlawful or punishable character of certain content is contested and corrected, for example by a court upon request of the original information provider. This could lead to the need to put back certain content. Article 4a juncto 5a of the *Gedragscode Notice-and-Take-Down*, according to the explanatory memorandum, imply that when a notice is formally made by a public prosecutor, the intermediary has the obligation to take down the content

54 Rechtbank [District Court] Assen 24 November 2009, LJN BK4226 (unlawful prosecution Budget webhosting), [in Dutch]. See also: Hof [Court of Appeal] Leeuwarden 20 April 2009, LJN BI1643 and BI1645 [both in Dutch].

55 *Kamerstukken II* 2001-02, 28 197, nr. 3, p. 26. [Explanatory memorandum to the Implementation Law Directive on Electronic Commerce] See also: Kamerstukken II 2007/08, 28684, nr. 133, p. 14. [parliamentary documentation]

without a separate evaluation of the punishable character of the content. It is stated that in that case, such an evaluation will have been sufficiently taken care of by a competent authority.

III. Current developments

The Ministry of Justice has announced that one of the main elements of current policy to deal with illegal content on the Internet is the development of legal instruments to provide grounds for government authorities to order the take down of such content. The current status of Article 54a Sr and Article 125o Sv as the statutory grounds for the possibility of a formal NTD-order will be evaluated.[56]

56 K*amerstukken II* 2007-08, 28684, nr. 133, p. 2 and 14. [parliamentary documentation]

Internet security and safety

I. Current regulations

Legislative framework

Implementing Article 4 of the Directive on privacy and electronic communications (2002/58/EC) (e-Privacy Directive), Article 11.3 of the *Telecommunicatiewet* (Tw – Dutch Telecommunications Act) contains a twofold duty of care for providers of publicly available electronic communications networks and publicly available electronic communications services.

The article refers to Article 11.2 Tw, which defines the type of providers to which the provisions apply. The Dutch Government found it necessary to include both types of providers, because they are interdependent in this matter. The definition of these networks and services in the Dutch Telecommunications Act covers for example Internet access providers and providers of mobile communication through telecommunication networks.[57] Internet service providers offering services through electronic communication networks which concern content-related services, like resellers or providers of "over-the-top" (OTT) services, for example webmail, are not covered.[58]

Article 11.2 Tw contains a general duty of care to ensure the protection of personal data and the privacy of subscribers or users of networks or services. The article refers to the *Wet Bescherming Persoonsgegevens* (Wbp – Dutch Data Protection Act) as the general legislative framework on the protection of individuals with regard to the processing of personal data and on the free movement of such data.[59]

Article 11.3 § 1 Tw states that "adequate" measures, technical and/or organizational, need to be taken to ensure the safety and security of the networks and services offered. It clarifies that, for a measure to be "adequate", the level of security should be proportionate to the risk presented, taking into account the current state of technical developments and the costs incurred to apply these techniques. The measures should be taken in the general interest of the protection of personal data and the privacy of subscribers and users.

Article 11.3 § 2 Tw adds a duty to inform subscribers when "particular risks" exist as regards the safety or security of the networks and services offered. As long as providers are

57 *Kamerstukken II* 1996–97, 25533, nr. 3, p. 71 and 119. [explanatory memorandum to the Dutch Telecommunications Act].

58 *Kamerstukken II* 2002–03, 28 851, nr. 3, p. 89. [explanatory memorandum to the Implementation Law Directive 2002/58/EC on privacy and electronic communications]

59 Article 13 Wbp contains a similar obligation as in Article 11.2 Tw. Data controllers need to take technical and organizational measures to protect identifying data against loss or any form of unlawful processing.

not dealing with these risks when applying Article 11.3 § 1 Tw, they should also inform subscribers about the possible measures to counter these risks, and the expected costs that come with such measures. The explanatory memorandum to the law reforming Article 11.3 § 2 Tw in the light of Article 4 of the e-Privacy Directive, mentions possibilities to encrypt communication and firewalls as measures about which Internet service providers could inform their users and subscribers.[60]

The Independent Post and Telecommunications Authority of the Netherlands (OPTA), as an independent administrative body, is the authority entrusted with monitoring (see Article 15.1 § 3 Tw) and enforcing (see for sanction possibilities Article 15.2 § 2 and 15.4 § 4 Tw) the provisions of Article 11.3 Tw.

Other regulatory measures

According to Article 18.8 Tw, the Minister of Economic Affairs has the possibility to issue decrees containing further rules relating to Internet safety and the security of publicly available electronic communications networks and publicly available electronic communications services, including technical and organizational measures to be demanded from the same providers as in Article 11.3 Tw. Contrary to Article 11.3 Tw, these rules do not have to only relate to the protection of personal data and the privacy of subscribers and users. At this moment, no such decrees have been issued.

OPTA has published policy rules relating to the duty to inform as outlined in Art 11.3 § 2 Tw. These rules set out which specific risks are encompassed by this duty of care, the possibilities that Internet service providers have to inform their users and subscribers about, the legislative framework giving the authority to OPTA to monitor this duty of care and the sanctions that OPTA considers appropriate for breaches of this duty.[61]

A covenant on measures against botnets has been concluded and announced by several large Internet service providers in August 2009.[62] It states that information about botnets should be exchanged between providers. The follow-up should be to help users to clean their computers and to reconnect them.

60 *Kamerstukken II* 2002-03, 28851, nr. 3, p. 153-154. [explanatory memorandum to the Implementation Law Directive 2002/58/EC on privacy and electronic communications]

61 "Beleidsregels informatieplicht voor aanbieders over internetveiligheid" [policy rules with respect to Article 11.3 § 2 Tw], 2009, OPTA/ACNB/2008/202938, http://www.opta.nl/nl/actueel/alle-publicaties/ publicatie/?id=2838.

62 See: http://www.xs4all.nl/nieuws/bericht.php?msect=nieuws&id=1055&taal=nl.

II. Application of the current regulations

Legislative framework

It has been debated whether Article 11.3 Tw is an obligation to perform to the best of one's ability or to produce a certain result. § 1 seems to have some wriggle room. § 2 does contain an obligation to inform, albeit with its limitation to "particular risks".[63]

In 2006, OPTA initiated the "project 11.3 Telecommunicatiewet", which aimed to give substance to the duties of care described in Article 11.3 Tw. It started by assigning a research project to Stratix, a Dutch consultancy firm.[64] The assignment was to map current and upcoming dangers and threats on the Internet, mainly by interviewing some involved parties. The goal was to add clarity to the question of how far the duties of care mentioned in Article 11.3 Tw must reach. Insight in the dangers and threats to be found on the Internet would help to ascertain which security measures would be "adequate", in the terminology of Article 11.3 Tw. The Stratix report contains an overview of the results from the interviews, together with some (conceptual) proposals for policy instruments.

With the results of the report by Stratix in mind, OPTA identified three tracks to develop, which would make up the total duty of care regulated by Article 11.3 Tw. First, a security part as described by Article 11.3 § 1 Tw, relating to the general safety and security of the Internet to be protected by "adequate" measures. Second, the duty to inform users of Internet networks and services of special threats to safety and security, and of possible means to fight these threats, as described by Article 11.3 § 2 Tw. The third track consists in dealing with the threat of botnets.

After a consultation and several talks with the main Dutch Internet service providers in 2007, OPTA concluded that there was too much resistance amongst the Internet service providers consulted against the policy rules in respect of the security part which it had developed following the findings of the research by Stratix. On the other hand, OPTA felt that there did seem to be a general interest in developing a quality mark to inform consumers about the level of security and safety to be expected when using the services of a certain Internet service provider.[65] In the end, the involved Internet service providers did not come to agreement on such a quality mark. OPTA concluded in 2008 that a quality mark would only be effective with broad support, which at that moment was lacking.[66]

63 *Kamerstukken II* 1997–98, 25 533, nr. 5, p. 126. [Note on parliamentary discussion on the explanatory memorandum to the Dutch Telecommunications Act]

64 Stratix (2007).

65 "Zorgplicht internetaanbieders" [letter from OPTA to Dutch Internet service providers], 2008, OPTA/ACNB/2008/201166, http://www.opta.nl/nl/actueel/alle-publicaties/publicatie/?id=2591.

66 "Vervolg zorgplicht internetaanbieders" [letter from OPTA to Dutch Internet service providers], 2008, OPTA/ACBN/2008/202005, http://www.opta.nl/nl/actueel/alle-publicaties/publicatie/?id=2718.

Botnets receive special attention because, according to OPTA, dealing with this problem is of particular importance for the safety of Internet networks and services.[67] Some doubts have been expressed, though, as to whether botnets fall under the scope of Article 11.3 Tw, which refers to the general interest of the protection of personal data and the privacy of subscribers and users. In general, botnets seem to be approached as a duty of care issue, both by OPTA and Internet service providers. Appropriate measures, as demanded by Article 11.3 Tw, are developed through regulatory measures, like the covenant which is discussed in this section under "other regulatory measures".

In general, an issue of jurisdiction arises with regard to botnets. There is cooperation with the KLPD (Dutch National Police Force), which is regulated by a covenant between OPTA and the KLPD. The protocol mainly regulates possibilities to exchange information and findings in the search of botnets and their initiators.[68] The KLPD can take action against botnets to the extent that the spread of malware, as prohibited by Article 4.1 of the *Besluit universele dienstverlening en eindgebruikersbelangen* (BUDE – Dutch Decree on Universal Service and Users' Rights), is an offence under the Dutch Penal Code.[69] Otherwise, and mutually exclusive, administrative measures by OPTA are possible. For example, an Internet service provider could be sanctioned as a co-offender of the prohibition on spreading malware.[70]

After deciding not to adopt the policy rules developed in 2007, OPTA started to focus on giving substance to the duty of Internet service providers to inform users as described by Article 11.3 § 2 Tw and the enforcement of this duty. OPTA first established a benchmark and then left it to the companies themselves to give shape to their duties. No evaluation process has been envisioned yet. In individual cases, OPTA will probably only sanction if an Internet service provider is heavily lacking in this area. In January 2009, OPTA issued policy rules relating to this duty of care (as discussed below).

In general, OPTA aims to actively contribute to an ongoing debate in the Netherlands between all involved stakeholders on subjects related to the development and safety of the Internet.[71]

---

67 Ibid.[check reference in final version]

68 "Samenwerkingsprotocol OPTA-KLPD" [Collaboration Protocol OPTA-KLPD], 2007, OPTA/TN/2007/201789, http://www.opta.nl/nl/actueel/alle-publicaties/publicatie/?id=2401.

69 Article 138a, 138b, 161sexies and 161septies, 350a and 350b DPC are mentioned in the protocol.

70 The Dutch Internet provider Mega Provider has been ordered by OPTA to stop facilitating spam through its e-mail services: "Last onder dwangsom Megaprovider B.V.", 2006, OPTA/IPB/2006/202031, http://www.opta.nl/nl/actueel/alle-publicaties/publicatie/?id=2033.

71 "Vervolg invulling 'Zorgplicht internetveiligheid' (artikel 11.3 Telecommunicatiewet)" [letter from OPTA to Dutch Internet service providers], 2007, OPTA/IPB/2007/202505, http://www.opta.nl/nl/actueel/alle-publicaties/publicatie/?id=2439.

Other regulatory measures

The main argument of the Internet service providers against the policy rules proposed by OPTA was that such rules would most likely quickly become outdated, seeing the rapidity at which Internet technology evolves.

OPTA encourages self-regulation, like the proposal of the Internet service providers to develop a quality mark, or the idea to develop agreement about best practices; however, at the moment, it feels the need to discuss the substance of the duties of care regulated by Article 11.3 § 1 Tw with the State Secretary of Economic Affairs.

The covenant that has been concluded between Internet service providers, as mentioned above, states that information about botnets should be exchanged between providers. The follow-up should be to help users to clean their computers and to reconnect them. The level of support will vary though, considering differences in the business models of Internet service providers.

III. Current developments

"Project 11.3 Telecommunicatiewet" ended partly with the conclusion that OPTA would have to consult further with the relevant Dutch ministry, in this case the Ministry of Economic Affairs. So far, such consultations have not occurred. It has not been discussed yet if the concept policy rules, which were developed after the research by Stratix in 2006, will be further developed.

In the Netherlands, the question has been raised if a duty to report the loss of personal data due to a security breach, both for government agencies in charge of vital infrastructures and private companies, could help to stimulate better protection of stored privacy-related information.[72] Such a duty to report exists in several countries throughout the world.[73] This question was raised as well during the negotiations between the European Commission, the EU Telecommunications Council and the European Parliament on the revision of the Directive on privacy and electronic communications (2002/58/EC), which was completed on 24 November 2009. The Dutch Government has acknowledged that, due to this revision, there is now an obligation to implement a duty to report the loss of personal data in data systems for telecom providers and Internet service providers. The government has explicitly expressed its support for the possibility to extend this duty to "providers of information society services" in general, like banks and online shops.[74]

72 *Kamerstukken II* 2007-08, 29 668 and 26 643, nr. 22, p. 1. [parliamentary documentation]
73 Boer & Grimmius (2009).
74 *Kamerstukken II* 2008-09, 26 643, nr. 138, p. 1. [parliamentary documentation]

Child pornography

I. Current regulations

Legislative framework

The possession, distribution and making available of an image, or a data carrier holding an image, of a sexual act (apparently) involving a person who is evidently under 18 is punishable under Article 240b of the *Wetboek van Strafrecht* (Sr – Dutch Penal Code). Also, accessing such an image through an automated work or by using a communications service, is punishable under the same article.

Article 6:196c of the *Burgerlijk Wetboek* (BW – Civil Code) exempts "providers of information society services" from civil liability for certain content put on their facilities by their subscribers and users under certain circumstances, as discussed in the introductory part of this report.

Other regulatory measures

The *Gedragscode Notice-and-Take-Down* (Notice and Take down Code of Conduct), as discussed in the introductory part of the report, provides general standards for the development of NTD procedures by intermediaries who provide public Internet services and have to deal with complaints about unlawful and/or punishable content in the online environment, like child pornography.

Specifically relating to child pornography, the *Meldpunt Kinderporno op Internet* (Dutch Internet Hotline against Child Pornography) has been set up to serve as a hotline in the network of INHOPE.[75] It has been set up by Internet service providers and interested users, and operates as the only actor in this field next to the Dutch police, under the auspices of the Dutch Ministry of Justice and the European Commission. In the last eleven years, the hotline has received more than 40,000 notices. These can come directly from individual Internet users or from Internet service providers. The hotline checks whether the notified material is punishable under current law, specifically Article 240b Sr. If the material seems punishable, this will be reported to the criminal investigation department of the Dutch police. If the material does not originate in the Netherlands, partners in the network of INHOPE will be notified, or the Dutch police will contact foreign investigation departments. The hotline will only consider notices on material that has been distributed

75 http://www.meldpunt-kinderporno.nl/default.htm

through Internet services that are publicly accessible. Distribution through one-on-one e-mail for example falls outside this scope.

II. Application of the current regulations

There seems to be a general agreement amongst Internet service providers that the distribution of child pornography is a matter they can and should deal with, and they are willing to cooperate with notices from the competent authorities and private parties, like the Dutch Internet Hotline against Child Pornography. This hotline plays an active role in the evaluation of notices and informing the competent public authorities.

III. Current developments

The Dutch Internet Hotline against Child Pornography has advocated plans for filtering, which are currently being developed. One of the measures supported is a pilot to use hash-filtering technology as developed by the Internet provider Leaseweb.[76]

The *Platform Internetveiligheid* (Internet Safety Platform), an initiative of Dutch government bodies and private companies, coordinated by the *Platform voor de InformatieSamenleving* (ECP-EPN – Platform for the Information Society), has announced the development of a blacklist to prevent the distribution of child pornography through the Internet, which should be maintained by market actors together with the government. No details on the make-up of this list have been provided so far.[77] In general, it should be mentioned here that previous practices in the Netherlands relating to filtering of child pornography have been abandoned. A blacklist provided by the KLPD (Dutch National Police Force) proved to lack sufficient legal ground.[78] Serious doubts have also been raised on the effectiveness and proportionality of blocking child pornographic content by preventing access to it or through filtering. The Dutch Government has also acknowledged before that blocking and filtering as a means to deal with illegal content on the Internet can prove to be ineffective to some extent and runs the risk of extending to other content that is not illegal.[79]

The Dutch Internet Hotline against Child Pornography also advocates a multi-stakeholder approach, similar to the best practices of the Financial Coalition Against Child Pornography (FCACP) called "Internet Merchant Acquisition Best Practices for the

76 Meldpunt Kinderporno, "Brief voor Algemeen overleg Tweede Kamer. Meldpunt Kinderporno op Internet, September 2009" [letter provided as input for parliamentary discussion in the Dutch Lower House], http://www.meldpunt-kinderporno.nl/files/Biblio/Brief AO Kinderporno September 2009.pdf.
77 http://www.ecp.nl/platform-internetveiligheid.
78 Stol e.a. (2008), p. 133-140.
79 *Kamerstukken II* 2007-08, 28684, nr. 133, p. 14 and 22. [parliamentary documentation]

Prevention and Detection of Commercial Child Pornography".[80] This coalition has also been mentioned in the explanatory memorandum to the law implementing the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. According to the government, cooperation with banks and credit card companies could be of importance to track down suspects, as these companies function as bottlenecks providing financial transaction facilities. It is noted that these companies, as expressed through the FCACP, acknowledge they have a certain responsibility in this context.[81]

80 http://www.fdic.gov/news/news/ financial/2007/fil07072.html.
81 *Kamerstukken II* 2009-10, 31810, nr. 3, p. 4-5. [parliamentary documentation]

Copyright

I. Current regulations

Legislative framework

The main law on copyright is the *Auteurswet* (Aw – Dutch Copyright Act). This law protects rights holders against unlawful use of their works, like unauthorized publication and/or reproduction of copyrighted materials. The law permits downloading of music or films without the prior consent of the rights holder, to the extent that this falls within the explicit exemptions set out in the law. The most relevant exemption within the scope of this report can be found in Article 16b and Article 16c Aw, concerning copying for own use – also referred to as the "thuiskopie" (lit: homecopy). This implies that consumers can download without the consent of the rights holder, for their own use.

The position of Internet service providers in relation to copyright is framed by Article 6:196c of the *Burgerlijk Wetboek* (BW – Civil Code). This has been confirmed by the government when developing this framework.[82]

Other regulatory measures

The *Gedragscode Notice-and-Take-Down* (Notice and Take down Code of Conduct) also applies to issues concerning copyright infringement.

II. Application of the current regulations

Case law has shown that Dutch courts can feel they have to read extra requirements in, and thus newly formulated exceptions to, the safe-harbour provisions of Article 6:196c BW when it comes to copyright infringement through the services of providers falling under the scope of this article. In the case of *BREIN v. KPN telecom B.V.*, a website containing bittorrents for the distribution of works protected by intellectual property rights was considered manifestly unlawful. The defendant, in its role as Internet access provider performing mere conduit activities, was ordered by a preliminary relief judge to close the Internet connection account of a subscriber if in the future the same unlawful website were

82 In the explanatory memorandum to the law implementing the InfoSoc Directive (2001/29/EG), it is explicitly stated that liability for intermediaries through involvement in the online traffic of copyright infringing materials is covered by the safe-harbour provisions of the E-commerce Directive: *Kamerstukken II* 2001-02, 28482, nr 3, p. 38-39. [explanatory memorandum to the Implementation Law Directive on Copyright and Neighboring Rights in the Information Society] See also: *Kamerstukken II* 2005-06, 30 392, nr. 6, p. 7. [Note on parliamentary discussion on the explanatory memorandum to the Implementation Law Directive on Enforcement of Intellectual Property Rights]

to be put on its facilities.[83] It has been argued that such an obligation goes against the limitative manner in which the conditions of Article 6:196c BW, specifically §1 relating to mere conduit activities by Internet service providers, have been formulated. The necessity of the order in light of the freedom of speech of the subscriber has been criticized as well.[84]

Other recent case law has dealt with intermediaries that, according to the courts, fall outside the scope of the safe-harbour provisions as defined in Article 6:196c BW. In cases like *BREIN v. Mininova* and *BREIN v. The Pirate Bay*, the defendant parties have been ordered to stop facilitating continuous infringements of copyright and/or other intellectual property rights, which is considered unlawful under general tort law. Seeing their involvement with the content they provide, the owners of these websites are considered to do more than provide "information society services" and cannot be seen as Internet service providers in the sense of Article 6:196c BW.[85]

III. Current developments

Recently, in the Dutch parliament, the exemption for private copying in the current Dutch Copyright Law, which covers downloading, has been discussed. In this discussion, arguments can be found that promote a role for Internet service providers to assist in the enforcement of a newly proposed prohibition which would make downloading (of music and films) from an illegal source unlawful. Measures which can be used to structurally monitor Internet traffic, like "deep packet inspection" and "fingerprinting", have been advocated for this purpose. The parliamentary commission proposing the new prohibition also advocates a new obligation for Dutch Internet service providers and hosting providers according to which they should retain identifying data of their subscribers who use their infrastructure for putting up websites.[86] In its first reaction, the Dutch Government agrees with the commission that current issues relating to copyright require new measures.[87] So far, the proposals of the commission have not been followed up by proposals of law.

83 Rechtbank [District Court] Den Haag (preliminary relief judge) 5 January 2007, Auteurs-, Media- en Informatierecht 2007-2 nr. 9 m.nt. O.L. van Daalen; Computerrecht 2007-2, 46 m.nt. L.A.R. Siemerink BREIN versus KPN Telecom. [in Dutch]

84 Chavannes (2007).

85 Rechtbank [District Court] Utrecht 26 August 2009, LJN BJ6008, BREIN versus Mininova; Rechtbank [District Court] Amsterdam (preliminary relief judge) 22 October 2009, LJN BK1067 The Pirate Bay versus BREIN. [both in Dutch].

86 *Kamerstukken II* 2009-10, 29838 and 31766, nr. 19 (herdruk), p. 34-35. [parliamentary documentation]

87 *Kamerstukken II* 2009-10, 29838, nr. 22. [parliamentary documentation]

Identity fraud

I. Current regulations

Legislative framework

Identity fraud as such is not punishable in the Netherlands.[88] Only effects of identity fraud are punishable. For example, credit card fraud is only punishable if it has been used to gain some form of benefit, according to Article 232 of the *Wetboek van Strafrecht* (Sr – Dutch Penal Code). The fraud in itself does not lead to a criminal conviction. In addition, Article 11.7 § 4 of the *Telecommunicatiewet* (Tw – Dutch Telecommunications Act) requires the use of a true identity in spam messages. The use of a false identity in such messages could influence the height of the administrative fine, which can be issued under the Dutch Telecommunications Act.

Seeing that identity fraud is not an offence in itself under Dutch criminal law, it is difficult to imagine a situation where the types of Internet service providers that fall under the scope of Article 6:196c BW would have to deal with identity fraud through their facilities. Internet service providers do not have a general obligation to monitor the information that they transmit or store or to actively seek facts or circumstances indicating illegal activity. If hosting providers store websites containing fraudulent information, the fact that this type of information is not punishable and thus not manifestly unlawful, means that Internet service providers do not have to take down the fraudulent materials upon notice, to benefit from the safe harbours that Article 6:196c BW creates.

Other regulatory measures

It can be noted here that in the Notice and Take down Code of Conduct (NTCC), "undesirable content" is mentioned as a separate category, in respect of which it is suggested that the addressed intermediaries can decide on their own what types of information fall under it and if they want to deal with it the same way as unlawful and punishable content. Online identity fraud, not being punishable as such under Dutch criminal law, could be handled as "undesirable content".

The Dutch Government, as an initiative of the Ministry of Internal Affairs (BZK) and the Ministry of Justice, has set up a *Centraal Meld- en Informatiepunt Identiteitsfraude en –fouten* (CMI – Central Notice- and Information Hotline Identity Fraud and Wrongful Registration of

88 Fraud with travel documents is punishable as such. See Article 231 Dutch Penal Code. It can be noted here as well that identity fraud entails activities that are prohibited by the Wet Bescherming Persoonsgegevens (WBP – Dutch Data Protection Act).

Personal Data), which is a continuation of a trial that started in 2008.[89] The trial was a formalization of a former private initiative that functioned as a self-regulatory hotline, which was part of the *Stichting Aanpak Financieel-Economische Criminaliteit in Nederland* (SAFECIN – Association Prevention of Financial-Economic Crime).[90]

II. Application of the current regulations

Dutch ministries have officially acknowledged the CMI as a definitive service as of 1 March 2010. For the moment, there is little information on its functioning.

III. Current developments

See the developments as mentioned in the part on "Internet security and safety", amongst which plans for a legislative duty to report the loss of personal data caused by a security breach.

89 See: http://www.overheid.nl/identiteitsfraude
90 See: http://www.identiteitsfraude.nl/index.php?s=p_1&p=9

Trade in stolen goods

I. Current regulations

Legislative framework

Under Article 417bis of the *Wetboek van Strafrecht* (Sr – Dutch Penal Code), it is an offence to acquire, hold or pass on a good while knowing at the moment of acquiring or holding it, as can be reasonably expected, that the good before that moment had been obtained through a criminal offence.

Art. 6:196c *Burgerlijk Wetboek* (BW – Dutch Civil Code) is applicable, as far as relevant for this theme.

Other regulatory measures

The *Gedragscode Notice-and-Take-Down* (Notice and Take down Code of Conduct) also applies to issues concerning trade in stolen goods.

II. Application of the current regulations

Legislative framework

Internet service providers do have a role in the application of the legislation mentioned above, in relation to the trade in stolen goods. Most notable is the role of providers of platforms.

In the case of *Stokke v. Marktplaats*, the question arose if the website Marktplaats, a Dutch subsidiary of eBay, has a duty to collect contact details of its users, specifically names, addresses and domiciles. Before answering this question, the District Court Zwolle/Lelystad, an ordinary court of first instance, in an interlocutory judgment, concluded that it should not leave out a judgment on possible duties for this kind of auction sites under general tort law, even if such a website falls, as a hosting provider, under the regime of Article 6:196c §4 BW, which is a lex specialis to general tort law. The court therefore did not decide on the question whether or not Marktplaats is a hosting provider in the sense of Article 6:196c §4 BW. According to the court, considering the E-commerce Directive, and the purpose and parliamentary history of Article 6:196c §4 BW, there are possibilities under general tort law to demand measures of Marktplaats to prevent or limit damages due to copyright infringing materials, but concludes that in this case precautionary monitoring of the advertisements put on the website would be disproportionate to the interests involved. Also, the NTD procedure Marktplaats has

implemented on its website meets the requirements of the care that can be expected from Marktplaats.[91]

As regards the request that Marktplaats be obliged to register the contact details of its advertisers, so as to be able to pass them on when Stokke (the plaintiff) establishes its rights are infringed, the court, in its final judgment, considered that this would also be disproportionate. In this context, the same court considered that to refer parties like Stokke to providers of e-mail addresses, which Marktplaats has of all its subscribers, to find out the requested contact details, would not be an alternative because these services are too loosely connected to the damaging infringement. It is to be expected that these service providers, like Internet service providers in the sense of the E-commerce Directive, do not have the obligation to provide the account details when weighing the involved interests, because their services have an even more remote connection to the (secondary) infringing act by private individuals who put up advertisements for goods protected by intellectual property rights than the services offered by Marktplaats.[92]

Other regulatory measures

Platform providers have set up measures to deal with the trade of stolen goods in the online environment. eBay and Marktplaats (a Dutch subsidiary of eBay) have their own NTD procedure, based on their so-called Verified Right Owner Program (VeRO),[93] which contains guidelines on how to react to notices on infringements of intellectual property rights.

91 Rechtbank [District Court] Zwolle/Lelystad, 3 May 2006, LJN AW6288, Stokke A.S. versus Marktplaats B.V. [a Dutch subsidiary of Ebay]. [interlocutary judgement, in Dutch].

92 Rechtbank [District Court] Zwolle/Lelystad, 14 March 2007, Stokke A.S. versus Marktplaats B.V. [a Dutch subsidiary of Ebay]. [see specifically consideration 2.5] See for comparison also: Rechtbank [District Court] Utrecht (preliminary relief judgment) 9 July 2002, LJN AE5537 Teleatlas versus Planet Media Group. [in Dutch]

93 http://pages.ebay.nl/vero/

United Kingdom

General introduction

Current regulations

Legislative framework

The Electronic Commerce (EC Directive) Regulations 2002, which implement the E-commerce Directive (2000/31/EC) into UK law, define the liability framework of Internet access providers and, more generally, Internet service providers. In line with the E-commerce Directive, these Regulations stipulate that Internet access providers and Internet service providers are exempted from liability for content online under certain conditions.

According to Regulation 17, an Internet service provider is exempted from liability if it acts as mere conduit. This is the case if the service it provides consists of either the transmission of information provided by a recipient of the service in a communication network, or the provision of access to a particular communication network. Thus, this is the provision applicable to Internet service providers when they provide access to the Internet.

Regulation 18 sets out that a service provider is exempted from liability if it is caching material. This is the case where the caching is "automatic, intermediate and temporary for the sole purpose of providing a more efficient service". However, this exemption is only valid if the service provider does not modify the information, complies with all access conditions imposed with regard to the site, complies with any rules regarding the updating of the information, does not interfere with the lawful use of technology used to obtain data on the use of the information, and 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 has been removed or access to it has been disabled.

Regulation 19 states that a service provider is exempted from liability if it is hosting material. This means that where an information society service is provided that consists of the storage of information provided by a recipient of the service, the service provider shall not be liable for damages or for any other pecuniary remedy or for any criminal sanction as a result of that storage, where it does not have actual knowledge of unlawful material and, where a claim for damages is made, is not aware of facts or circumstances from which it would have been apparent to the service provider that the activity or information was unlawful. Furthermore, the service provider must act immediately upon gaining knowledge that the material is unlawful by either removing or disabling access to the

material. Finally, the person who has posted the material must not be under the authority or control of the service provider.

Regulation 22 provides a definition of "notice" for the purpose of gaining "actual knowledge" in the context of Regulations 18(b)(v) and 19(a)(i). It states that a court shall take into account all matters which appear to it in the particular circumstances to be relevant and, among other things, shall have regard to whether a service provider has received a notice and the extent to which any notice includes the full name and address of the sender, details of the location of the information in question, and details of the unlawful nature of the activity or information in question. Regulation 6(1)(c) states also that the details of the service provider, including its electronic mail address, which make it possible to contact it rapidly and communicate with it in a direct and effective manner shall be made available. Here, the Regulations go beyond the scope of the E-commerce Directive, which failed to provide any such definition and information.

Article 15 of the E-Commerce Directive states that member states shall not impose a general obligation on Internet service providers to monitor the information they transmit or store. The UK Government decided not to include this within the 2002 Regulations. The reason is that the government was concerned that such an inclusion would not only confer no additional legal certainty on intermediaries but could even introduce uncertainty if the prohibition were interpreted differently from its meaning in the Directive.

Internet security and safety

I. Current regulations

Legislative framework:

The primary piece of legislation with regard to Internet security and safety are the Privacy and Electronic Communications (EC Directive) Regulations 2003. These Regulations implement the Directive on privacy and electronic communications (2002/58/EC) (e-privacy Directive). Article 5 of the Regulations, which is a literal implementation of Article 4 of the Directive, regulates responsibilities in relation to safety and security.

Other regulatory measures

Other regulatory measures mainly take the form of self-regulation by the involved stakeholders, amongst which regulations to deal with the distribution of spam and malware. Most notably, next to a general Code of Conduct (which is discussed below under the next theme), the ISPA UK has adopted three Best Current Practices (BCPs): a) BCP on Blocking and filtering of Internet traffic; b) BCP on Unsolicited Bulk Email (spam); and c) BCP on Law Enforcement Contact.[94] The first BCP specifies that users need to be informed appropriately when filtering measures are applied. The second BCP on spam specifies that Internet service providers should ensure that all e-mail generated within their own networks can be attributed to a particular customer or system, and that appropriate arrangements for the handling of reports of abuse by their customers are operated. Furthermore, where abuse is proven, the Internet service provider should take effective action to prevent the customer from continuing that abuse. The third BCP sets out which measures Internet service providers should take so that requests by, for example, judicial authorities can reach them properly. There is no self-regulation specifically related to Internet safety and security.

II. Application of the current regulations

Legislative framework:

The implementation of the Privacy and Electronic Communications (EC Directive) Regulations 2003 has not resulted in further regulations. On the website of the independent regulator and competition authority for the UK communications sector, OFCOM, users are directed to their Internet service providers.

94 http://www.ispa.org.uk/home/page_364.html.

Other regulatory measures

As illustrated above, no other formal measures are currently in place, which impose duties of care for intermediaries with regard to material violating the integrity and security of information technology systems. However, as described above, the non-mandatory self-regulatory Best Current Practice (BCP) document on Unsolicited Bulk Email has been implemented. While this is effective in some cases, it is not necessarily an effective measure in general as it lacks enforcement power and a centralised approach.

Child pornography

I. Current regulations

Legislative framework:

The primary pieces of legislation regulating the distribution, making and possession of child pornographic material in the UK are the Protection of Children Act 1978 (POCA) (which does not apply in Scotland or Northern Ireland) and section 160 of the Criminal Justice Act 1988 (CJA 1988) (which has effect throughout the UK). The POCA defines as offences the taking, distribution, showing, and publishing of child pornographic photographs. The Sexual Offences Act 2003, s 45, amending the POCA 1978, s 7(6), defines a child as a person under the age of 18. The POCA was further extended by the Criminal Justice and Public Order Act 1994 (CJPOA 1994), s 84, to include photographs in electronic data format, thereby introducing the concept of "pseudo-photographs". Pseudo-photographs are technically photographs, but they are created by computer software manipulating one or more pre-existing pictures. The CJA makes the mere possession of an indecent photograph of a child an offence.

As analysed in detail in the introductory part of this chapter, the Electronic Commerce (EC Directive) Regulations 2002 define the liability framework for certain service providers on the Internet for online illegal content and thus also child pornographic material. It is in this context that, during the interviews, the different stakeholders raised the point that they are generally open to undertaking any efforts possible to avoid the dissemination of child pornographic content, but that, however, they are afraid that if they agree to any additional measures this would impose liability on them, which might then also be extended to other areas, such as copyright infringement.

Other regulatory measures

In addition to the legislative regulatory measures, and in light of the Electronic Commerce (EC Directive) Regulations 2002 liability exemptions, other measures have been developed to regulate online child pornographic content. Most notably in relation to Internet service providers, a non-governmental organisation, the Internet Watch Foundation (IWF), was founded in 1996 to deal with the regulation of online child pornography material worldwide (and obscene and race hate material in the UK). The IWF works in collaboration with the online industry, law enforcement, government, the education sector, charities, international partners and the public to minimise the availability of this content.

The IWF is an independent, self-regulatory organisation that provides a channel for the public and IT professionals to report online content within the IWF's remit, acting as the "notice and take-down" body for this content. The IWF has an e-mail, telephone and fax hotline so that users can report material related to child pornography and other obscene material.

The IWF is governed by a Board of Trustees. Initially, the board of the IWF consisted exclusively of representatives of Internet service providers. The current board, however, comprises a wider range of experts from different organisations and backgrounds. The role of the board is to monitor and review the IWF's remit, strategy, policy and budget.

II. Application of the current regulations

Legislative framework

The main problem of the existing legislative framework regulating the distribution, creation, and possession of child pornography is the application and enforcement of such rules in the online scenario. Frequently, existing legislation is challenged in court on matters relating to the novel environment of the Internet and its storage, publishing and distribution means. For instance, a court has had to rule on whether having indecent photographs stored on the cache of a computer system belonging to a certain person constitutes "possession" by that person.

Furthermore, in the interviews it has been emphasized – which is relevant in all the countries under consideration in this report – that the E-commerce Directive and correlated notice and take down procedures are primarily limited to content that is in the public domain and thus can be detected by third parties who can inform the Internet service provider about this. However, this is mainly limited to websites, while most of the child pornographic content is distributed via protected channels, such as peer-to-peer, Bit Torrent and closed newsgroups.

Other regulatory measures

The IWF accepts complaints for illegal content that falls within its remit. Around 85% of reports to the IWF are about child pornography, 10% about general obscenity, and 5% about racial hatred.[95] In 2008, the IWF processed 33,947 reports. However, most material being reported is hosted outside of the UK.

95 http://www.iwf.org.uk/documents/20091214_iwf_annual_report_2008_pdf_version.pdf.

Upon receipt, the IWF examines the reports from the public to verify the illegality of the content according to UK legislation and takes appropriate actions upon confirmation of this. All IWF employees responsible for verifying the content are trained by UK police to adequately undertake this task.

Arguably, the most important outcome of these activities is a daily updated "blacklist" of child pornography URLs, which is passed on to UK Internet service providers for removing or blocking. Currently, 98% of all UK Internet service providers are blocking content based on this blacklist. The blacklist is sent to Internet service providers in encrypted form, to avoid illicit use thereof, but the Internet service providers can edit the list and add their own URLs to it.

Furthermore, the content is reported to the UK police if it originates within the UK, and removal is recommended from the servers of UK Internet service providers. If the content originates in a foreign country, this is reported to partner organisations (if existent) in the country concerned and access to the content is blocked within the UK. If no partner organisation exists, the responsible foreign Internet service providers are informed. Furthermore, the content is reported to SOCA (Serious Organized Crime Agency), who organises liaison with foreign police forces about removal. If IWF blocking is applied, a 404 "technical error" page is returned, when a browser tries to access the page in question.

In addition, the UK Internet Service Providers' Association (ISPA UK) has adopted a code of practice in 1999, which was amended in 2002.[96] This code sets out specific minimum standards with regard to tackling illegal Internet content. All members need to adhere to this code of practice, which is intended to govern the conduct of the ISPA members. This code of practice contains in section 5 references to the work of the IWF. While ISPA membership does not automatically confer IWF membership, it requires ISPA members to adhere to the IWF notice and take down procedure.

The IWF runs a very effective hotline and blacklist system. It provides a quick and practicable method of removing child pornographic content from UK public view. Furthermore, by operating the hotline, the IWF protects Internet service providers for example from having to deal with complaints from the public about such material.

III. Current developments

In the interviews, a separate aspect was emphasized, that is the general education of Internet users, and particularly parents, about the potential risks involved in using the Internet. The Byron Review on Safer Children in a Digital World suggested that while the

96 http://www.ispa.org.uk/about_us/page_16.html

Internet is very popular with children, there is a lack of knowledge and awareness on the part of parents about their roles to ensure the safety of their children online with regards to harmful material.[97]

97 http://www.dcsf.gov.uk/byronreview/pdfs/Final%20Report%20Bookmarked.pdf

Copyright

I. Current regulations

Legislative framework:

The primary piece of legislation regulating the use, copying and distribution of copyrighted material in the UK is the Copyright, Designs and Patents Act 1988 (CDPA).[98] The CDPA gives the creators of literary, dramatic, musical and artistic works the right to control the ways in which their material may be used. Furthermore, the Act provides various remedies to protect rights holders against the unauthorised copying of their works. According to the CDPA, s17, copyright is infringed by *reproducing a work in any material form, including storing it by electronic means.* S18 of the CDPA further specifies that *issuing copies of a work to the public* infringes the copyright of the rights holder. Furthermore, s107(1) CDPA stipulates that it is also a criminal offence to *possess an infringing copy of a copyright work in the course of business without the licence of the copyright owner*, or, as specified under sub-para (e), *to distribute an infringing copy other than in the course of business to such an extent as to affect prejudicially the owner of the copyright*.

Other regulatory measures

There is no self-regulation in the UK specifically related to copyright. Neither an overarching code of conduct nor a prescribed notice and take down procedure exist.

II. Application of the current regulations

Legislative framework

Generally, the CDPA is also the relevant Act to determine liability of Internet service providers for copyright infringement. Here, the question arises whether the transport of copyright infringing material by Internet access providers, and the hosting and storing on their servers of copyright infringing material by Internet service providers can be considered a primary or secondary infringement of copyright according to the CDPA. No UK case law dealing with this question exists, however, in *Sony Music Entertainment v. Easyinternetcafe*,[99] the judge established that while liability for primary copyright infringements under s17 and s18 of the CDPA is strict (that is, absence of knowledge of the infringement is not a defense), this does not mean that it extends to involuntary actors,

98 http://www.opsi.gov.uk/acts/acts1988/UKpga_19880048_en_1.htm.
99 Sony Music Entertainment (UK) LtD & Others v. Easyinternetcafe Ltd [2003] EWHC 62(Ch).

such as Internet service providers, which have no ability to control the infringing action in question.

Other regulatory measures

It was stated in the interviews that the current regulations are considered to be sufficient. Internet service providers manage their own policies for when requests to remove infringing materials are received. The possibility for right holders to apply for a court order was emphasized as well. Next to these practices, references to the Digital Economy Act, which is currently under development and discussed below, were made.

III. Current developments

The Digital Economy Act was adopted on 8 April 2010. It includes eleven topics, one of which introduces a graduated response system.[100] After a certain number of copyright infringements, an Internet access provider may be required to disconnect a subscriber from the Internet. The Act inserts articles 124A to 124N in the Communications Act and sections 17 and 18 of the Act contain provisions on the powers of the Secretary of State.

The Act lays down the so-called "Initial Obligations" in Articles 124A and 124B. According to Article 124A a copyright owner may send a copyright infringement report to a provider containing the alleged copyright infringement, the description thereof and the evidence that shows the subscriber's IP address and the time at which the evidence was gathered. The report must be sent to the Internet access provider within the period of one month beginning with the day on which the evidence was gathered. Article 124B provides that the Internet access provider must keep information on the received notifications in a so-called "Copyright Infringement List". The information about the infringements of the accused subscriber may also include notifications of other copyright owners so that a copyright owner can determine whether or not the infringer infringes habitually. It is hoped that copyright owners will only target the most serious repeat infringers so as to spare one time infringers and make sure that legal action is effective and efficient. A copyright owner who has notified a provider of an infringement may require the disclosure of the information kept by the provider. The Copyright Infringement List may not reveal the identity of the subscriber.[101] In order to obtain the subscriber's identity, the copyright owner has to get a court order. After the identity is revealed, the copyright owner may sue the infringer for damages.

100http://www.opsi.gov.uk/acts/acts2010/pdf/ukpga_20100024_en.pdf. Explanatory memorandum: http://www.publications.parliament.uk/pa/ld200910/ldbills/001/2010001.pdf. See also for an earlier consultation: http://www.berr.gov.uk/consultations/page51696.html.

101 Digital Economy Bill, Explanatory notes, p. 9. http://www.publications.parliament.uk/pa/ld200910/ldbills/001/2010001.pdf. See also for an earlier consultation: http://www.berr.gov.uk/consultations/page51696.html.

These Initial Obligations only come into effect after an Initial Obligations Code is implemented. The Code, according to Articles 124C to 124E, must provide for procedural criteria on the format, required information and time limits for the Copyright Infringement Report, the Copyright Infringement List and the notification of the report sent by the provider to the alleged infringing subscriber. The Initial Obligations Code may also contain voluntary provisions agreed upon by all parties. It is hoped that all stakeholders, including copyright owners, providers and consumers, will contribute to the Code.[102] Article 124C states that the regulatory authority OFCOM has to approve the Initial Obligations Code and if it does not approve it or if a Code has not been drawn up, Article 124D specifies that OFCOM must make one itself.

The Secretary of State may impose technical obligations on a service provider, obliging it to undertake measures against its subscribers in terms of a limit of speed or capacity, a block or limit on subscriber's access to certain material or a limit on or suspension of the service to the subscriber.[103] In order for the Secretary of State to better assess whether or not measures should be taken, OFCOM makes assessment or progress reports. The Secretary of State may order a provider to undertake action against a subscriber if that person meets certain criteria.[104] OFCOM must draft a Technical Obligations Code specifying regulations on the measures enforced by the Secretary of State. The Technical Obligations Code must also contain specific provisions on the procedure for the determination of subscriber appeals, the required grounds for appeals and the determination of guilt of the subscriber.

Both the Initial Obligations Code and the Technical Obligations Code should appoint a neutral person, in relation to the providers, copyright owners and OFCOM, with the duty of receiving subscriber appeals. Those appeals might either relate to the alleged infringement or the identification of the person as the copyright infringer. Appeals may also relate to the storage of information by the provider or the inclusion of certain information in the Copyright Infringement List. Article 124K specifies that an appeal is possible to a First-tier Tribunal regarding the technical obligations imposed by the Secretary of State. A First-tier Tribunal is a generic tribunal established by Parliament for appeals on government decisions. The First-tier Tribunal has the power to withdraw, remit or confirm the decisions on technical measures and it may also admit costs. The technical measures would presumably be postponed until the dispute has been resolved.[105]

Article 124L of the Communications Act specifies that Internet access providers who fail to disclose information on customers who evidentially have repeatedly infringed copyright can be fined for up to £250,000 for non-compliance.

---

102 Digital Economy Bill. Explanatory notes, p. 10.
103 See also: http://www.berr.gov.uk/consultations/page51696.html
104 Digital Economy Bill. Explanatory notes, p. 12.
105 Digital Economy Bill. Explanatory notes, p. 12.

Identity fraud

I. Current regulations

Legislative framework:

No legislation explicitly regulating identity fraud exists in the UK. However, the Fraud Act 2006 has been drafted in light of emerging technologies and is apt to deal with this type of fraudulent activity. As opposed to previous legislation, the 2006 Act requires neither proof of deception nor the obtaining of any property. Section 1 of the 2006 Act creates a new general offence of "fraud", which can be committed in three ways: by false representation (s2); by failing to disclose information (s3); and by abuse of position (s4). More specifically, section 2 provides that a person is in breach of this section if he: (a) dishonestly makes a false representation, and (b) intends, by making the representation (i) to make a gain for himself or another, or (ii) to cause loss to another or to expose another to a risk of loss.

However, no formalised duty of care exists for Internet service providers with regard to online identity fraud.

II. Application of the current regulations

Legislative framework

Due to its broad reach, the 2006 Act will cover all forms of phishing activity, including sending of spoof emails to unsuspecting businesses and individuals ("vishing") and sending of targeted phishing emails ("spear phishing").[106]

Education about identity fraud is part of a public awareness campaign, supported by the government and involved companies.[107] There is specific attention for the role of Internet service providers in these initiatives. The emphasis lies on stakeholders that are confronted with the effects of identity fraud.

106 A Savirimuthu, J Savirimuthu, "Identity Theft and Systems Theory: The Fraud Act 2006 in Perspective", (2007) 4:4 SCRIPTed 436.
107 http://www.identitytheft.org.uk/

Trade in stolen goods

I. Current regulations

Legislative framework

The trade of stolen goods is regulated in the UK by the Theft Act 1968. According to section 22, an offence is created if a person handles stolen goods, that is if (otherwise than in the course of stealing) knowing or believing them to be stolen goods he dishonestly receives the goods, or dishonestly undertakes or assists in their retention, removal, disposal or realization by or for the benefit of another person, or if he arranges to do so. So-called e-fencing, which refers to the sale of stolen goods online, also falls within the scope of this section.

Due to the regulations implementing the E-commerce Directive, Internet service providers could be notified about stolen goods traded through their network/services, and asked to take appropriate measures.

Other regulatory measures

No other measures are currently in place with regard to creating duties of care for intermediaries to regulate the trade of stolen goods online. It is known that eBay, holding the largest market share for the sale of goods online, enforces its own procedures to prevent trade in stolen goods.

II. Application of the current regulations

Legislative framework

As mentioned above, e-fencing falls within the scope of section 22 Theft Act. A distinction needs to be made here between the trade of goods that were previously stolen and the trade of goods violating intellectual property rights. For the latter option, case law pertaining to intermediaries hosting the material (i.e. online auction houses) exists.

Recent case law has shown that courts in the UK are reluctant to impose duties of care on intermediaries (here online auction houses) for content offered by users. In *L'Oréal v. eBay*, the UK High Court ruled in favour of eBay and cleared it from liability for trademark

infringing content offered by a user. In this case, a number of questions have been referred to the European Court of Justice for a preliminary ruling.[108]

Other regulatory measures

Online platform providers, most notably eBay, have implemented measures to deal with the trade of stolen goods in the online environment. eBay has strict internal regulations and effectuates its own policies in relation to the trade in stolen goods, and cooperates closely with the prosecution authorities (see also the chapter on the trade of stolen goods in the country report on the Netherlands).

108 http://www.judiciary.gov.uk/docs/judgments_guidance/l'oreal-ebay.pdf. Reference for a preliminary ruling: OJ C 267/40 of 7/11/2009, Case No. C-324/09.

Germany

General introduction

I. Current regulations

Legislative framework

Articles 7-10 *Telemediengesetz* (TMG – Telemedia Act) implement the E-commerce Directive (2000/31/EC) into German law. According to Article 8 TMG, an Internet service provider is exempted from liability if it transmits in a communications network, or provides access to, data of others. This is the case if the service provider has not initiated the transmission, has not chosen the recipient of the information and has not selected or amended the transmitted information. The liability exemption also applies if the data is temporarily stored to enable its transmission in the communications network and not longer than usually necessary for the transmission.

Articles 9 and 10 TMG are pertinent to Internet service providers who are caching or hosting information of others. Article 9 TMG sets out that a service provider is exempted from liability if it is automatically and temporarily caching data of others for the purpose of its transmission to other users if: it does not modify the data (Nr. 1); complies with all access conditions to the data imposed with regard to the site (Nr. 2); complies with any rules regarding the updating of the data as defined in international industry standards (Nr. 3); and does not interfere with the lawful use of technology used to obtain information on the use of the data (Nr. 4). Furthermore, it must act 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 has been removed or access to it has been disabled, or a court or administrative body has ordered the removal or blocking.

Article 10 TMG provides that a service provider is exempted from liability if it is hosting material for a user, where it does not have actual knowledge of unlawful material and, where a claim for damages is made, is not aware of facts or circumstances from which it would have been apparent to the service provider that the activity or information was unlawful (Nr. 1). Furthermore, the service provider must act immediately upon gaining knowledge that the material is unlawful by either removing or disabling access to the material (Nr. 2). This exemption only applies if the person who has posted the material is not under the authority or control of the service provider.

In line with the E-commerce Directive, the TMG does not include any statutory notice and take down procedures for illegal Internet content. Article 7 TMG specifies that Internet intermediaries are not under a general obligation to monitor or inspect the transmitted or stored data for unlawful activities. Hence, intermediaries only have to act upon notification by a third party. Furthermore, Article 7 TMG states that the secrecy of telecommunications according to Article 88 *Telekommunikationsgesetz* (TKG – Telecommunications Act) needs to be preserved for any of the above-described activities. Article 88 TKG states that every service provider is obliged to preserve the secrecy of telecommunications, even after the activities that gave rise to such obligation have ceased. It further specifies that the secrecy of telecommunications applies to the content of all telecommunications and all of the ancillary circumstances, such as the participants of a telecommunication. It also applies to unsuccessful telecommunications attempts.

Internet security and safety

I. Current regulations

Legislative framework

The duties of care and liability of Internet intermediaries for the technical integrity and safety of networks and computer systems of customers depend on where the security breach occurred. Generally, security breaches can occur at two different levels: (a) at the level of the systems of Internet access providers and Internet service providers, and (b) at the level of the systems of end-users.

Article 7(1) TMG sets out that the liability exemptions for Internet access providers and Internet service providers as defined by Articles 8-10 TMG, which are analysed in detail in the introductory part of this chapter, are not applicable to own information, thus also not to the security of own systems. Therefore, the liability exemptions do not apply to the operational functionality or security of services offered by Internet access providers or Internet service providers. They are, however, applicable to content transmitted, as discussed above in the introductory part. Therefore, two scenarios need to be distinguished. In case the integrity and security of data of a user is violated by an intrusion and manipulation of the system of the Internet access provider or Internet service provider, the liability exemptions are not applicable. In case the integrity and safety is violated on the system of the user (either because the Internet access provider has transmitted malicious data, or a third person, who is also a user, has stored malicious data on the server of the Internet service provider), the liability exemptions of Articles 8-10 TMG are applicable.

Hence, Internet intermediaries have duties of care to sufficiently protect their own system against security breaches violating the integrity and safety of customer data (such as the destruction or loss of data, and the destruction of hardware due to malware attacks). If an intermediary does not comply with the duties of care and damages on the customer side occur, the customer might have a contractual or tortious claim against the provider. Such duties of care can for example be fulfilled through the use of virus scanners and firewalls.

However, for all claims for damages, Article 44a TKG specifies that service providers have a limitation of liability if they provide telecommunications services. Their liability is limited to 12,500 Euros for pecuniary losses.

In case the violation of the integrity and safety occurs on the system of the customer or is caused by a third party, the liability exemptions of Articles 7-10 TMG are valid. This means that intermediaries have no own duties of care as regards content that they transmit, host or cache, which violates the integrity and safety of systems of their customers, unless they are notified or gain knowledge about this. This, however, can already be the case if

unusual network traffic and activities are detected. However, as explained further in section 1 of this chapter, intermediaries do not have a duty to actively inspect network traffic for such activities.

In addition to these regulations, the Directive on privacy and electronic communications (2002/58/EC) (e-privacy Directive) stipulates in its Article 4 that the provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard the security of its services. This was implemented into German law in Article 109 TKG, which states that service providers have to take appropriate technical or other measures to protect the secrecy of telecommunications and other personal data and to protect telecommunications and other data processing systems against unauthorised access. The purpose of this article is to safeguard the confidentiality of telecommunications and guarantee an undisturbed operation of the service. In addition, telecommunications service providers, who have immediate control over the systems, are according to Article 109(2) TKG obliged to install sufficient precautionary measures against disruptions, which could disturb the operation of the system, attacks from the outside and effects of catastrophes. Primarily, these are measures to ensure the safety of data to avoid any loss or damage of data, and to prevent misuse of the data. Misuse can be the attack of outsiders (such as hackers) or the unauthorised access to data by employees. Which exact safety measures are appropriate needs to be established for each individual case. To establish this, a security officer needs to be nominated to compile a security concept (Article 109(3) TKG). For instance, such measures can be the installation of anti-virus software and access restrictions to server rooms.

Article 4 of the e-privacy Directive includes furthermore the provision that customers need to be informed about serious security breaches. This has not been implemented in Article 109 TKG. However, Article 93(2) TKG includes the provision that service providers need to inform customers about particular risks to the security of the network.

II. Application of the current regulations

Legislative framework

No case law exists in Germany that could serve to measure the effectiveness of the existing legislative framework. The problem with Article 109 TKG is that, while it sets out that service providers and operators of telecommunications networks have certain duties of care to ensure the security of the network, it does not specify the minimum security measures that must be in place. Thus, in the absence of any case law that could clarify this matter, a degree of legal uncertainty exists here.

III. Current developments

The Association of the German Internet Industry, ECO, together with the Federal Office for Information Security (*Bundesamt für Informationssicherheit* – BSI), has initiated an anti-botnet project. The aim of this project is to set up a helpline, where the general public can receive information and help to clear their computers of bots and viruses.[109] Internet intermediaries, like Internet service providers, can identify infected systems from suspicious network traffic patterns. The affected customer will receive a notification about the infection and a recommendation to visit the anti-botnet website for further help. It is envisaged that this notification will be delivered via different channels to ensure that it reaches the customer. It will appear as a pop-up window when a browser is opened, as well as be sent by conventional post.
The anti-botnet website offers assistance in a two-step process. Firstly, the customer can visit a website where information and tools for self-help are provided. Should this not suffice, the customer can in a second step contact an advisory centre where individual help is provided to clear the system of the malware and protect it in the future from further attacks. These actions, however, will not be mandatory for the customer. While this is a joint initiative between the private industry sector and the government (BSI), ECO is solely responsible for the implementation and management of this project so that no official enforcement mechanism exists.[110] It was highlighted that also no further actions such as the temporary termination of the Internet access are envisaged, should customers not comply with the recommendations.[111]

The government has also highlighted that any technical measures to detect infected systems need to be in accordance with the existing German data protection laws, and particularly the secrecy of telecommunications.[112] This was also confirmed by some of the stakeholders, who indicated that this would restrict the technical ability of detecting infected systems.

109 http://www.eco.de/verband/202_7268.htm.
110 http://www.eco.de/verband/202_7268.htm.
111http://www.heise.de/security/meldung/Bundesweite-Zentrale-zur-Botnetz-Bekaempfung-wirft-Fragen-auf-882987.html.
112 Ibid.

Child pornography

I. Current regulations

Legislative framework

The primary piece of legislation regulating the possession, distribution, showing and creation of child pornographic material in Germany is Article 184b *Strafgesetzbuch* (StGB – German Penal Code). A child according to these regulations is anybody under the age of 14, as specified in Article 176 StGB. According to Article 184c StGB, these regulations are also applicable to broadcasting, media- and teleservices, and hence the online environment. There, possession of online child pornographic material refers to the mere looking at such material on the Internet, as the Hamburg Court of Appeal has found. No permanent storage on the hard disk is required to fulfill this crime.[113] The distribution of child pornographic material on the Internet occurs when the data arrives on the computer of the user. It is irrelevant here whether the provider has transmitted it or the recipient has accessed it.[114] Furthermore, the showing or exhibiting of child pornographic content on the Internet occurs when a user has reading access to the data.[115]

Also, the articles which implement the E-commerce Directive, as described in detail in the introductory part, are applicable.

Other regulatory measures

In addition to the legislative regulatory measures, and in light of the liability exemptions under Articles 7-10 TMG, other measures have been developed to regulate online child pornographic content. Most notably in relation to Internet intermediaries, a system of non-governmental organisations, which are part of the INHOPE network and operate hotlines according to the INHOPE standards, exists in Germany. The German member organisations are the Association of the German Internet Industry (ECO), the *Freiwillige Selbstkontrolle Multimedia-Diensteanbieter* (FSM) and *jugendschutz.net*. FSM and ECO are relevant for the regulation of child pornographic content.

113 http://www.heise.de/newsticker/meldung/Urteil-Kinderpornos-anklicken-ist-strafbar-931446.html.
114 BGH, NStZ 2001, 569.
115 Ibid.

FSM is the association for voluntary self-regulation of multimedia service providers in Germany and was founded in 1997. Since 2005, FSM is a recognised authority for "regulated self-regulation" in Germany.[116] FSM was a founding member of INHOPE and offers a website for complaints about illegal material online, such as child pornographic content.[117] Members of the public can report such material via a web form or to a designated email address. Upon receipt, the FSM examines the report and should the illegality be confirmed, informs the relevant service provider of the material. The service provider will then receive a deadline to respond to the notification or remove the content. Should it not act within the given time frame, the appeals board will be notified about this and take appropriate action. In case the material originates in a foreign country, the FSM forwards the complaint to INHOPE, which then contacts the relevant partner organisation in the country in question. Approximately 23% of all complaints received pertain to child pornographic material. FSM does not accept complaints for content in newsgroups.

ECO is the association of the German Internet industry and was founded in 1993. It also operates a hotline for reporting of illegal material online, which is comparable to the one of FSM.In addition to this hotline, ECO also operates in collaboration with FSM the so-called *Internetbeschwerdestelle* (Internet complaints) hotline, which is the official German INHOPE complaints hotline.[118] Here, members of the public can report child pornographic content via web forms on the website. Different forms for the different technologies (such as websites, newsgroups or peer-to-peer) exist. FSM and ECO have split up responsibility for the different technologies between them, and complaints are forwarded to FSM or ECO according to their responsibility for the respective technology.[119] These complaints are then evaluated internally and the concerned service provider is informed, should the content be illegal according to German law. In case the content originates in a foreign country, the INHOPE member in the country concerned is contacted to ensure that appropriate actions are taken. In case no partner organisation exists in the country, the responsible foreign Internet service provider is informed. In addition, identified URLs are added to the INHOPE database, which is regularly updated and used to avoid redundancies when reporting material to a partner organisation.

116 "The system of '"regulated self-regulation'" is valid in the area of youth protection in online media since April 2003 and arranges a cooperation in youth protection in media of state and industry. This means that the state creates the legal framework and the according structures. Providers can fill this framework on their own authority while the state is able to avoid erroneous trends through a proper political frame and adequate monitoring facilities.

117 http://www.fsm.de/de/Beschwerdeformular.

118 http://www.internet-beschwerdestelle.de/index.htm.

119 FSM is responsible for information on the World Wide Web, mobile phone content accessible via the Internet, age verification systems, and chat. Eco is responsible for newsgroups, spam/e-mail, discussion for a, ICRA-labels, and peer-to-peer. http://www.internet-beschwerdestelle.de/beschwerde /verfahrensordnung/index.htm.

Furthermore, the FSM has adopted a code of conduct, which is mandatory for all members. All large German Internet access providers and Internet service providers are members of the FSM. In section 1, the code sets out that its purpose is to regulate unlawful material online. In section 2, it specifies that members have to ensure that child pornographic content is not offered or transmitted. Furthermore, members have to inform relevant authorities should they detect child pornographic material online.

II. Application of the current regulations

Legislative framework

The TMG regulations are effective with regard to content that is in the public domain and thus can be detected by third parties who can inform the Internet access provider or Internet service provider about this. However, this is mainly limited to websites, while most child pornographic content is distributed via protected channels, such as peer-to-peer, BitTorrent and closed newsgroups. Furthermore, the German regulations on the secrecy of telecommunications restrict the possibilities of intermediaries to carry out certain technical measures, such as the blocking of IP addresses. Thus the impact and effectiveness of this liability regime for Internet service providers is limited.

Other regulatory measures

FSM and ECO run a very effective hotline system for the reporting of child pornographic material by members of the public. It provides a quick and practicable method of removing child pornographic content from German public view. Furthermore, by operating the hotlines FSM and ECO protect Internet service providers for example from having to deal with complaints from the public about such material. However, no statistics as to what type of content is blocked and how the content is evaluated are published. This leads to a lack of transparency and therefore difficulty in assessing the system's actual effectiveness.

III. Current developments

In Germany, a new law has been enacted to regulate child pornographic content online.[120] The *Gesetz zur Erschwerung des Zugangs zu kinderpornographischen Inhalten in Kommunikationsnetzen* (Zugangserschwerungsgesetz – ZugErschwG; Law to complicate the access to child pornographic content in communication networks) was drafted in 2009, upon the initiative of Ursula von der Leyen, the then minister for family affairs. The aim of this law is to com-

120 http://www2.bgbl.de/Xaver/start.xav?startbk=Bundesanzeiger_BGBl.

plicate the access to child pornographic material on the Internet. To achieve this, according to Article 1 of the ZugErschwG, the German Federal Criminal Police Office (*Bundeskriminalamt* – BKA) shall compile a list with domain names, IP addresses and URLs of websites containing child pornographic material or linking to websites containing such material, which will be updated daily. Internet service providers with more than 10,000 customers will be obliged to block access to the websites on this list at least on the DNS level, as set out by paragraph 2. Furthermore, customers attempting to access such websites would be diverted to a website of the BKA, featuring a stop sign and a short explanation that the Internet browser was attempting to connect to content classified as child pornographic material by the BKA.[121] Internet service providers will have to compile and transfer an anonymous access statistic relating to such websites to the BKA. In addition to this law, the German Government has signed contracts with the five major Internet service providers about the blocking of child pornographic content. These contracts were negotiated with each single Internet service provider and the content is kept secret. Even the different Internet service providers do not know the content of the contracts with the others.

On 17 February 2010 the law was unexpectedly signed by the German Federal President and came into force on 22 February 2010 with its official publication.[122] The government has now agreed that the BKA will not compile a blacklist nor ask Internet service providers to block content.[123] Furthermore, it is currently being debated how this law could be annulled.

121http://de.wikipedia.org/w/index.php?title=Datei:Kinder_stopp.png&filetimestamp=20090418174246.

122 See note 9.

123http://www.heise.de/newsticker/meldung/Justizministerium-hofft-bei-Websperren-auf-abgerundete-Loesung-937249.html.

Copyright

I. Current regulations

Legislative framework

The primary piece of legislation regulating the use, copying and distribution of copyrighted material in Germany is the *Gesetz über Urheberrecht und verwandte Schutzrechte* (Urheberrechtsgesetz – UrhG, Copyright Act). The Act was first enacted in 1965 but has since been amended in light of the technological changes. Furthermore, the *Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft* and the *Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums* should be mentioned.

Articles 15-24 of the UrhG give the creators of literary, dramatic, musical and artistic works the right to control the ways in which their material may be copied, distributed and exhibited. The implementation of the InfoSoc Directive into German law adjusted the UrhG to the new telecommunications technologies. Article 19a UrhG sets out that the rights owner also has the right to publicly make available his work. Material is publicly available, if it is available to members of the public via wired or wireless transmission at a time and place of their choice. Importantly, the purchase of recording media does not confer the right to make it publicly available. Furthermore, the downloading of copyright protected material is, according to Article 53 UrhG, which regulates the lawful copying of copyright protected material for private use and other exemptions, unlawful, if an obviously illegally made public original was used to create the copy. Furthermore, the Act provides various remedies to protect rights holders against the infringement of their rights defined in Articles 15-24 UrhG. According to Article 97 UrhG, rights holders are entitled to the removal of the infringing content, and if the infringement occurs, can obtain an injunctive relief.

Generally, Articles 7-10 TMG define the liability framework and set out the duties of care of Internet intermediaries for illegal content online, and therefore also for copyright infringing material.

Other regulatory measures

The above-described legislative framework is the main tool for the regulation of copyright infringing material in Germany. As opposed to child pornographic material, no other measures similar to the hotlines operated by ECO or FSM exist that would create duties of care for intermediaries with regard to the regulation of copyright infringing material.

II. Application of the current regulations

Legislative framework

According to the prevailing opinion, both the public offering of a work online, as well as the subsequent transmission of the work, constitute making available in the sense of the Copyright Act. However, it is irrelevant whether the material was indeed retrieved or not by another person/user.[124] Thus, for example, the offering and sharing of copyrighted material on peer-to-peer systems on the Internet violates Article 19a UrhG.[125]

It has been debated whether, despite the liability exemptions of Articles 7-10 TMG, rights holders could obtain an injunctive relief against Internet access providers and Internet service providers. This would be the case, if Internet access providers and Internet service providers could be considered secondary infringers of copyright according to Articles 823 and 1004 *Bürgerliches Gesetzbuch* (BGB – Civil Code). A secondary infringer (*Störer*) is someone who wilfully, and adequately and causally participates in the causing or maintaining of an unlawful act. Internet service provides, by providing access to the Internet, create the risk of customers using these facilities for copyright infringing activities. A secondary infringement requires the violation of inspection duties (*Prüfpflichten*). Inspection duties are different from monitoring duties, which Internet service providers are exempted from under Article 7 TMG. Thus, this is the reason why despite the liability exemptions, Internet service providers could be considered secondary infringers of copyright. Inspection duties are violated if such an inspection can reasonably be expected of the secondary infringer. Whether this is the case for Internet service providers in relation to copyright infringements is controversial. However, in any case, the inspection duties of Internet service providers are limited by the secrecy of telecommunications according to Article 88 TKG (Article 7 TMG). The secrecy of telecommunications applies to the contents of telecommunications and traffic data. This includes the IP addresses of customers, as well as the pages accessed. Hence, it applies to the information relevant to establish whether a person has infringed copyright online. It is therefore not possible for an Internet service provider to undertake the relevant inspection duties without violating the secrecy of telecommunications. Internet service providers cannot be considered secondary infringers and rights holders cannot obtain an injunctive relief against them.[126]

124 Gercke (2006).
125 Gercke (2006).
126 Gercke (2006).

Identity fraud

I. Current regulations

Legislative framework

Identity theft as such is not punishable under German law. However, certain online crimes that include an element of identity fraud, most prominently phishing, can be illegal under German penal law (*Strafgesetzbuch* – StGB).

II. Application of the current regulations

Legislative framework

Courts have recently confirmed also for the online scenario that identity theft is not punishable under German law, e.g. in a case where the court established that registration and trading under a fake identity on eBay is legal.[127]

While it has been controversially debated in the past whether the provisions of the StGB apply to newly evolved online crimes such as phishing, the majority of authors now agree that Article 269 StGB, which regulates the forgery of evidentiary data, covers fraudulent activities such as phishing.[128]

127http://www.telemedicus.info/urteile/Internetrecht/899-KG-Berlin-Az-4-1-Ss-18109-13009-Strafbarkeit-der-Anmeldung-bei-eBay-unter-falschem-Namen.html.

128 See e.g., A. Seidl, K. Fuchs, "Die Strafbarkeit des Phishing nach Inkrafttreten des 41. Strafrechtsänderungsgesetzes" (2010) 2 HRRS, 85; M. Gercke, "Die Strafbarkeit von "Phishing" und Identitätsdiebstahl - Eine Analyse der Reichweite des geltenden Strafrechts", (2005) CR, 606 ff.

Trade in stolen goods

I. Current regulations

Legislative framework

The trade of stolen goods (*Hehlerei*) is regulated in Germany by the German Penal Code (StGB). Article 259 StGB states that an offence is created if a person acquires, purchases or otherwise obtains, or supplies a third party with, or profitably sells, goods, which another person has stolen or otherwise acquired through an unlawful act violating third party property rights. Importantly, it needs to be distinguished here between the trade of goods that were previously stolen and the trade of goods violating intellectual property rights.

Other regulatory measures

There is no specific self-regulation in Germany relating to the trade of stolen goods online. Providers of platforms do apply their own procedures to prevent the trade in stolen goods.

II. Application of the current regulations

Legislative framework

The Federal Court of Justice (*Bundesgerichtshof* – BGH) has ruled on three different occasions that online auction houses, as opposed to Internet service providers and other Internet intermediaries, are liable for counterfeit products as secondary infringers (*Störerhaftung*) and developed a preventive injunctive relief for rights holders against auction houses.[129] This means that operators of auction houses have a duty of care to prevent all future infringements of intellectual property rights by members, who are classified as potential infringers. The court suggested that the use of filter software could facilitate this and reasoned that such duties would not be disproportionate.

Other regulatory measures

As far as the position of platform providers is concerned, here reference can be made to the discussion on the internal procedures applied by parties like eBay in the other sections on trade in stolen goods in this report.

129 BGH Urteil: 11.03.2004 Az. I ZR 304/01; 19.04.2007 Az. I ZR 35/04; 12.07.2007 - Az. I ZR 18/04.

France

General introduction

Legislative framework

Articles 12 to 15 of the E-commerce Directive have been implemented into French law by the *loi pour la confiance dans l'économie numérique*[130] (LCEN – Law on Confidence in the Digital Economy). The scope of the law is much broader than the E-commerce Directive, as described below. Articles 6 and 9 set out the liability framework applicable to Internet service providers for transmitted and stored content. It should be noted that while Article 6 of the law has not been incorporated in any existing code and is enforceable as part of the LCEN, Article 9 has become Article L. 32-3-3 and Article L. 32-3-4 of the *code des postes et des communications électroniques* (CPCE – Code of the Postal Services and Electronic Communications). Article 6 is part of the legislative framework as an article of the LCEN.

Like the E-commerce Directive, the law distinguishes the three activities of Internet service providers: mere conduit (Article 6-I-1 LCEN and Article L. 32-3-3 CPCE), caching (Article L. 32-3-4 CPCE) and hosting (Article 6-I-2 LCEN). Article 15 of the E-commerce Directive, which exempts Internet service providers from any general obligation of monitoring information they transmit or store and of seeking facts or circumstances indicating illegal activities, has been implemented in Article 6-I-7 LCEN.

Under Article L. 32-3-3 CPCE, implementing Article 12 of the E-commerce Directive, a mere conduit provider, which either transmits communications or provides access to a communication network, will only be liable if it (a) initiates the litigious transmission; (b) selects the receiver of the transmission; or (c) selects or modifies the transmission's content. Under Article L. 32-3-4 CPCE, implementing Article 13 of the E-commerce Directive, a caching provider, which performs an automatic, intermediate and temporary storage of content for the sole purpose of making the transmission more efficient, is exempted from civil and criminal liability for stored content. However, the exemption falls when the caching provider modifies content, does not comply with its conditions of access or customary rules regarding its update, or interferes with the lawful and ordinary use of technology to obtain data.

A caching provider will also be liable if it does not expeditiously remove stored content or disable access to it either: (a) upon obtaining actual knowledge of the fact that content, at the initial source of the transmission, has been removed or access to it has been disabled; or (b) after the judicial authorities have ordered such removal or disablement.

130 Loi n° 2004-575 du 21 juin 2004, JORF n° 143 du 22 juin 2004, p.11168

Under Article 6-I-2 LCEN, implementing Article 14 of the E-commerce Directive, a hosting provider is defined as a legal or natural person, which makes storage of signals, texts, images, sounds and messages of any kind available to the public. A hosting provider is exempted from civil liability if: (a) it does not have actual knowledge of the illegal nature of stored content or of facts and circumstances showing its illegal character; or if (b) upon obtaining such knowledge, it acts expeditiously to remove or disable access to the data. Article 6-I-3 LCEN also exempts hosting providers from criminal liability under similar conditions, to the exception that a hosting provider is liable if it is aware of the illegal activity and information and not of the illegal nature of the activity or information.

Article 6-I-5 LCEN sets up an optional notification procedure, which permits to presume the actual knowledge of the hosting provider about litigious content stored on its website. This procedure falls outside the scope of the E-commerce Directive and provides for the communication of the following elements: date, details of the legal or natural person making the notification and of its recipient, description of the disputed facts with their exact location, reasons for which the content must be removed and copy of the letter sent to the content's author or editor requesting him to stop the illegal activity. Article 6-I-5 together with Articles 6-I-2 and 6-I-3 LCEN constitute the French "Notice and Takedown" procedure.

Moreover, under Article 15 of the E-commerce Directive, member states have the possibility to oblige Internet service providers to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements. Article 6-II, 1st indent, LCEN imposes on Internet access providers and hosting providers a duty to keep data allowing the identification of anyone, who has contributed to stored or transmitted content. Article 6-II, 3rd indent, allows competent authorities to request communication of these data. The type of data as well as the retention period should have been defined by a decree, which has never been adopted. Courts regularly use this article to request from hosting providers identification data of the disputed content's author.

Internet security and safety

I. Current regulations

Legislative framework:

The legal provisions regulating the technical integrity and safety of electronic communications are found in Article D.98-5 CPCE and in Article 34 of *Loi n°78-17 du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés* (Loi Informatique et Libertés).[131]

Under Article D.98-5 CPCE, implementing into French law Article 4 of the Directive on privacy and electronic communications (2002/58/EC) (e-privacy Directive), a telecom operator must take all the necessary measures to safeguard the security of communications using its network. It must comply with the technical requirements that can be established by ARCEP, the French regulator for the electronic communications and postal sectors. On a confidential basis, the regulator can receive communication of the measures taken to ensure the network security. The telecom operator has a duty to inform its subscribers of services permitting to increase the level of communication security and of any particular risk of security breach, together with the possible remedies and the likely costs involved. Article D.98-5 CPCE imposes duties on telecom operators, which are defined under Article L.32 (15°) CPCE as natural or legal persons exploiting an electronic communication network open to the public or providing an electronic communication service to the public. Article L.32 (6°) CPCE excludes from the scope of the definition, services consisting in the edition or distribution of public communication services via electronic means. In consequence, and following the interpretation given by the regulator itself, Internet access providers benefit from the status of telecom operators as they provide a service enabling the exchange of electronic communications.[132] Actors of the industry that are not involved in the emission, transmission and reception of signs, sounds, signals or images constituting electronic communications – such as hosting providers – are therefore excluded from the scope of Article D.98-5 CPCE.

Other regulatory measures:

In order to fight spam, "Signal Spam", a national hotline bringing together public authorities, private entities and professional organisations, was set up in November 2005. The purpose of the hotline is to inform Internet users about the different forms of spam

131 Loi n° 78-17 du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés, amended several times and available at : http://www.cnil.fr/en-savoir-plus/textes-fondateurs/

132 La lettre de l'Autorité de Régulation des Télécommunications, n° 41, Novembre/Décembre 2004, p.11 « Qu'est-ce qu'un opérateur de communications électroniques ? », available at : http://www.arcep.fr/fileadmin/reprise/communiques/lettre/pdf/lettre41-p11.pdf

(including phishing and scam) and fight against their dissemination, through the identification of emitting servers and "zombie PCs". Internet users register on the website, www.signal-spam.fr, and download a plug-in for their mailbox to directly forward unsolicited messages to the hotline. They also have the possibility to complete a form, available on the website, to report spam. After receiving the messages, Signal Spam analyzes the messages and reports them to the competent authorities, which can start investigation and impose sanctions on the spam's authors.

The problem of unsolicited communications is not a recent issue in France. In 2002, AFA, the association representing the interests of Internet service providers in France, amended its professional practices, to recommend that Internet service providers set up technical measures to detect spam and avoid its transmission.[133] In addition, AFA has published specific recommendations on its website intended for Internet service providers, e-mail software providers and e-mail service providers in order to fight spam. The recommendations relate, among others, to the protection of user's station against computer attacks and the detection of "zombie PCs".[134]

II. Application of the current regulations

Legislative framework

Article D.98-5 CPCE does not provide for specific sanctions in case of breach of duties of care by telecom operators. However Article L.36-11 CPCE gives a power of sanction to ARCEP when telecom operators do not perform their duties. Depending on the gravity of the breach, ARCEP can pronounce the partial or full suspension, for a maximum of one month, of the right to establish an electronic communication network or to provide an electronic communication service, or the withdrawal of such right for a maximum of three years. ARCEP also has the possibility to impose fines. On the basis of Article L.36-11 CPCE, ARCEP should be entitled to impose sanctions and fines on Internet access providers, which did not set up the appropriate security measures. During the interviews however, we were informed that security breaches are covered in France by "national defence secrecy" (*secret défense*) and are therefore confidential. They can only be communicated to other parties, which are duly authorized to deal with matters under "national defence secrecy". Currently ARCEP does not have this status and cannot receive communication of the security breaches pursuant to Article D.98-5 CPCE. The issue of security breaches should be tackled instead by the Ministry of Defence, through the French Network and Information Security Agency (FINSA or better known under the French acronym ANSSI). Very little information on the role of the ANSSI, in relation to security breaches, is available. However, the Agency manages an official portal on computer

133 Pratiques et Usages, les principes communs aux membres de l'AFA, www.afa-france.com/deontologie.html
134 Lutte contre le spam, http://www.afa-france.com/t_spam.html

security (www.securite-informatique.gouv.fr), issuing good practices and technical advice for the protection of individuals' and companies' computers.

Other regulatory measures:

From the annual report of "Signal Spam" 2007-2008, it appears that 14 million notifications had been made by the end of 2008 and 48,500 users were registered.[135] No information is available to assess the efficiency of the system and in particular the technical and human means available to process the high volume of notifications. However, from the information gathered during the interviews, it appears that Signal Spam does not itself process the messages notified but forwards them to the relevant competent authorities, thanks to the partnerships signed with them. As an example, after the signature of its partnership agreement with Signal Spam, the CNIL (*Commission nationale de l'informatique et des libertés* – National Commission for Information Technologies and Civil Liberties) launched in September 2008 a series of on-site controls to check whether online marketing companies complied with their legal obligations.

III. Current developments

In May 2009, on behalf of the Senate's Committee of Laws, two senators published a *Rapport d'information sur la vie privée à l'heure des mémoires numériques* (an Information Report on privacy at the time of digital memories).[136] They called, among others, for the creation of a new reporting obligation to the CNIL concerning security breaches.

On the basis of this report, on 6 November 2009, the two senators proposed a new *Loi visant à mieux garantir le droit à la vie privée à l'heure numérique* (Law to better guarantee the right to privacy in the digital environment).[137] Draft Article 7 proposes to amend Article 34 of *Loi Informatique et Libertés* and could constitute an early implementation of the new Article 4 of the revised e-privacy Directive (Directive 2009/136/EC). The proposal for Article 34 provides that "*the data controller [*would*] adopt all appropriate measures (…) to ensure the security of data and protect personal data against accidental or unlawful destruction, loss, alteration, disclosure, dissemination, storage, processing or unauthorized or unlawful access, especially when the processing implied data transmission on a network, as well as against any other form of unlawful processing. In case of a breach of personal data, the data*

135 Rapport d'activité 2007-2008, Signal Spam, available at : https://www.signal-spam.fr/Rapport2008-VF.pdf

136 « La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information », Rapport d'Information n° 441 (2008-2009), M. Yves Détraigne et Mme Anne-Marie Escoffier, fait au nom de la Commission des lois, 27 May 2009, available at : http://www.senat.fr/noticerap/2008/r08-441-notice.html

137 « Proposition de loi, visant à mieux garantir le droit à la vie privée à l'heure du numérique », n°93, by M. Yves Détraigne et Mme Anne-Marie Escoffier, 6 November 2009, available at : http://www.senat.fr/leg/ppl09-093.html

*controller [*would*] notify without any delay its data privacy correspondent [*belonging to its company*] or in his absence, the CNIL. If the breach affected personal data of one or more individuals, the data controller would inform them.*" The content, form and modalities of these notifications are to be defined by decree.

It should be noted that the current Article 34 of *Loi Informatique et Libertés* already provides for a similar obligation regarding the security and integrity of data. The new element introduced in the proposal is the notification of personal data breaches. This point complies with the new Article 4 of the revised e-privacy Directive, whereas other elements of the proposal diverge from the Directive.

First of all, the Directive imposes obligations to secure personal data on providers of publicly available electronic communications services, i.e. Internet access providers. The French text would apply to data controllers, i.e. the entity or person responsible for data processing. The category is much broader.

Second, the new Article 4 mentions notification to the competent national authority. In the proposal, the CNIL has been designated as such competent authority. It would have also been relevant to assess whether the French Network and Information Security Agency, ANSSI, might not have a role to play in the security of data processing,[138] as it has the mission of a national authority for Information Systems Security. The law proposal has been discussed by the Senate during the session of 23 March 2010 and forwarded to the National Assembly for discussion.[139]

138 Coupez (2010).

139 « Proposition de loi , adoptée par le Sénat, visant à mieux garantir le droit à la vie privée à l'heure du numérique », n° 2387, 24 March 2010, available at : http://www.assemblee-nationale.fr/13/dossiers/vie_privee_numerique.asp

Child Pornography

I. Current regulations

Legislative framework

The legal provisions regulating child pornographic content in France can be found in Article 227-23 of the *code pénal* (French Penal Code). Four offences are defined under this article.
The dissemination, fixation, recording and transmission of an image or representation of a minor constitute an offence when this image or representation has a pornographic character. The offering, making available and distribution of such an image or representation, by any means, as well as the import and export also constitute an offence. The penalties, sanctions and fines are increased when a communication network is used for the distribution of the image or representation of a minor to an undetermined public. The habitual consultation of such communication service available to the public, showing child pornographic images or representations, or the concealment of them is also punishable.[140]

Regarding the transmission and storage of online child pornographic content, the liability regime applicable to Internet service providers is the one defined in the *loi pour la confiance dans l'économie numérique* (LCEN – Law on Confidence in the Digital Economy) implementing the E-commerce Directive, as described in the introductory part. In addition, the LCEN has introduced provisions for specific illegal content listed in its Article 6-I-7, 3rd indent. This constitutes a category of content, which is considered particularly harmful and commonly described as *contenus odieux* (outrageous content).[141] Under this category, falls content relating to crimes against humanity, racial hatred, child pornography, incitement to violence or detrimental to human dignity. For this type of content, Internet access providers and hosting providers have the duty to set up a signalling procedure (*procédure de signalement*), easily accessible and visible, enabling anyone to report to them the presence of such content. After being informed, Internet service providers promptly notify the competent authorities (among others, the Central office against cybercrime, OCLCTIC,[142] the Information Technology Fraud Investigation Unit,[143] the police units, the gendarmerie – a type of military police – and the public prosecutor). Pursuant to Article 6-I-2 LCEN, only hosting providers must remove this manifestly unlawful content after being informed

140 Article 227-22-1 also punishes an adult who makes sexual proposals to a minor of 15 years old (or to someone pretending to be) with the use of a communication network.

141 « Rapport d'information de la Commission des Affaires Economiques, de l'Environnement et du Territoire à l'Assemblée Nationale, sur la mise en application de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique » n°627, by M. Jean Dionis du Séjour et Mme Corinne Erhel, 23 January 2008, available at http://www.assemblee-nationale.fr/13/rap-info/i0627.asp

142 Office Central de Lutte contre la Criminalité Liées aux Technologies de l'Information et de la Communication

143 Brigade d'enquêtes sur les fraudes aux technologies de l'information, BEFTI

of its presence. Internet access providers, on their side, are obliged to remove unlawful content at the request of a court.

Other regulatory measures

In the field of child pornography, several co-regulatory/self-regulatory tools and initiatives have been put in place.

In 1998, AFA (French Internet Service Providers Association), the professional association representing access, caching and hosting providers in France, set up the Point de Contact (www.pointdecontact.net), a hotline against *illegal content related to child pornography, racial hatred, apology for or incitement to commit crimes against people, terrorism or provocation to suicide.*[144] Point de Contact is the French member of the European hotline association, INHOPE. In 2004, AFA issued guidelines for professional good practices in the form of a code of conduct, signed by representatives of Internet service providers. The *Charte contre les contenus odieux* ("Code of conduct against harmful content") relates to content detrimental to human dignity and includes child pornography.

Article 2 of the code of conduct recalls the legal obligation for Internet service providers (Article 6-I-7 of the LCEN) to provide a signalling mechanism for harmful content and proposes the use of the centralized Point de Contact for this purpose. Internet service providers agree to put links to the Point de Contact's notification form on their community spaces – such as forums, chat rooms – and on the home page of their services, enabling Internet users to report content in one click. Internet service providers also commit to make information easily available to parents for protecting their children and to propose free filtering software together with a parental control solution. According to Article 3, Internet service providers will promptly notify litigious content to law enforcement, either directly or through the Point de Contact. They also agree to promptly remove illegal content or disable access to it. Following Article 4, Internet service providers agree to cooperate with the judicial authorities to keep elements of information allowing the identification of the content's author or the users of their services. They also communicate to the competent authority any changes of contact details and cooperate to set up any temporary and targeted monitoring of the information they transmit or store. Since September 2009, the Point de Contact is also accessible from a mobile phone.

Concerning mobile phones, another co-regulatory initiative should be mentioned. The AFOM –French Association of Mobile Operators – is, following the adoption of a *Charte d'engagements des Opérateurs sur le contenu multimedia* (Operators' code of conduct regarding mobile multimedia content), to protect minors against unlawful content (as defined by Article 6-I-7, 3rd indent, of the LCEN, e.g. child pornography) and sensitive content (such as pornography). The code of conduct has been adopted following Article 16 (e) of the E-

144 AFA's Annual Report, March 2008- June 2009

commerce Directive, which encourages the drawing up of codes of conduct, the Recommendation of the Council on the protection of minors and human dignity[145] in audiovisual and information services, as well as the Recommendation by the *Forum des droits sur l'Internet* relating to the protection of minors on the Internet and mobile networks.[146] It has been signed by the members of AFOM[147] and the Ministry of State for Social Security, Elderly, Disabled and Family. In addition to the obligations set up by the LCEN, mobile operators agree to improve their notification devices for illegal content and promptly remove or disable access to this type of content after being informed of its presence. The code was signed in 2006 and constitutes a part of the European Framework for Safer Mobile Use, a European initiative to ensure that children and teenagers can safely access content on their mobile phone.

Two other initiatives should be mentioned under this section. The first one involves the Ministry of Interior and the second one relates to the Recommendations published by the *Forum des droits sur l'Internet*.

In 2009, the Ministry of Interior set up a website, www.internet-signalement.gouv.fr, to which Internet users as well as AFA – thanks to a specific access through its Point de Contact – can directly report illegal content. The reported content is processed by the police units of the office in charge of cyber criminality, the OCLCTIC, through the platform called PHAROS (*Plateforme d'Harmonisation, d'Analyse, de Recoupement et d'Orientation des Signalements*). This platform has existed for several years but was initially only dedicated to child pornography.

Finally, the *Forum des droits sur l'Internet,* an independent organisation of coregulation created with the support of the French Government to facilitate dialogue among the different Internet players and the government, has published three Recommendations on child protection and child pornography.
The first one, "Children of the Internet (I), exposure of minors to harmful content on the Internet",[148] was adopted before the enactment of the LCEN. In this document, the Forum addresses recommendations to public authorities, parents and Internet actors. In particular, it calls on Internet access providers to add information about "child protection" on their home pages and on content providers to work on technical solutions (software) to describe the content of online files.

---

145 Council Recommendation of 24 September 1998 (98/560/EC) on the development of competitiveness of the European audiovisual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity, OJCE L270/40, 07.10.1998

146 Recommandation, Les Enfants du Net (I), l'exposition des mineurs aux contenus préjudiciables sur l'Internet, 11 février 2004, Forum des droits sur l'Internet but also Recommandation, Classification des contenus multimédia mobiles, 18 octobre 2006, established by a working group of the Forum at the request of the AFOM after the adoption of its Code of Conduct

147 Bouygues Telecom, Orange France, SFR, Debitel, M6 Mobile, Universal Mobile and Omer Telecom

148 Recommandation, Les Enfants du Net (I), l'exposition des mineurs aux contenus préjudiciables sur l'internet, 11 février 2004, le Forum des droits sur l'Internet

The second, "Children of the Internet II – Child pornography and paedophilia on the Internet",[149] recommends Internet service providers to adopt a high standard level regarding information dedicated to their users. The Forum also encourages all Internet professionals to put in place a mechanism similar to the mechanism described in the AFA's *Charte contre les contenus odieux*.

The third one, "Children of the Internet III – necessary conditions for the setup of filtering of child pornography websites by Internet access providers",[150] constitutes the latest document of the Forum. At that time, the Ministry of Interior as well as the Secretary of State in charge of Family, showed a particular interest in measures to block access to child pornographic websites located abroad and asked the Working Group in charge of the protection of children, under the auspices of the Forum, to study a possible legal and technical framework for filtering measures. The work of the Group has resulted in the Forum's third Recommendation. In this document, the Forum does not take position on the desirability of imposing or not filtering measures on Internet access providers but provides a legal and technical recommendation on the way to implement such measures, following the request of the public authorities. As a prerequisite, the Forum considers that the measures should only be applicable to child pornographic content. The proposed mechanism is as follows. Units of police, with the cooperation of Internet users (via notification platforms) would identify child pornographic content. The OCLCTIC, the office in charge of cyber criminality, would then establish a list of websites containing images or representations of sexual abuses on minors. This list would later be assessed by the competent national authority – not defined at this stage – and transmitted to Internet access providers, which would block these websites, subject to the websites' rights to defence. Internet access providers would either automatically include the list in their filtering device, without viewing the addresses at stake, or designate a person with the power to receive, decrypt and process the list before including it in the filtering process. Every Internet access provider would be free to choose its own filtering method.

The recommendations adopted by the Forum are policy tools and usually help the government before proposing a new law.

II. Application of the current regulations

Legislative framework

In application of Article 6-I-7, 4th indent LCEN, Internet access providers and hosting providers must set up a signalling mechanism allowing Internet users to notify them of illegal content such as child pornography. All the AFA members are complying with their legal obligation, through the use of the Point de Contact. However, one of the largest

149 Recommandation, Les Enfants du Net-II, pédo-pornographie et pédophilie sur l'internet, 25 janvier 2005, le Forum des droits sur l'Internet

150 Recommandation, Les Enfants du Net III, conditions nécessaires à la mise en place du filtrage des sites pédopornographiques par les FAI, 29 octobre 2008, le Forum des droits sur l'Internet

Internet access providers in France is not an AFA member and has set up its own mechanism.

This Internet access provider has implemented on its website a notification mechanism for content listed in Article 6-I-7, 3rd indent LCEN. The provider enables Internet users to report content detrimental to human dignity (including child pornography) by filling in a notification form to be returned by post to the Internet access provider. Although the mechanism complies with the legal provisions of the LCEN, one can wonder whether a notification by traditional mail is efficient enough to help fight against child pornographic content, which might not last more than a few hours. No figures on the number of notifications received, as well as on the type of content concerned, are publicly available.

All the other Internet access providers benefit from the Point de Contact, set up and managed by AFA. The *Charte contre les contenus odieux,* which prescribes the use of the Point de Contact, is not a legally binding document. However, its signatories comply with their legal obligation by linking their website to the hotline. Every year, AFA assesses the notifications made through the Point de Contact. In 2009, among 4573 websites notified as having child pornographic content, 987 were recognized as potentially illegal by the hotline's content analysts. The figures of 2009 are 15% lower than in 2008. According to AFA's press release,[151] these figures show the difference of appreciation between Internet users and the experts analyzing the reported content. It seems that Internet service providers have completely delegated their obligation of reporting illegal content to the Point de Contact, which checks in practice whether the reported content is illegal or not. If this is the case, the content is identified, notified to law enforcement (OCLCTIC) and forwarded to the hosting provider when it is hosted by a member of AFA or to one of the Point de Contact's international partners when the content is hosted by a foreign Internet service provider located in a country, which is a member of the INHOPE network. If AFA members can rely on the Point de Contact to be relieved from their obligation under Article 6-I-7 of the LCEN, this does not exonerate them from reporting to law enforcement content which has been directly notified to them by Internet users. From the statistics available, it appears that very few Internet service providers directly notify the presumably unlawful content to the OCLCTIC. For the year 2007, only three Internet service providers respectively reported 2, 5 and 122 instances of potentially unlawful content.[152]

151 http://www.afa-france.com/p_bilan_2009_pointdecontact.html

152 « Rapport d'information de la Commission des Affaires Economiques, de l'Environnement et du Territoire à l'Assemblée Nationale, sur la mise en application de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique » n°627, by M. Jean Dionis du Séjour et Mme Corinne Erhel, 23 January 2008, available at http://www.assemblee-nationale.fr/13/rap-info/i0627.asp

Other regulatory measures

Among the Recommendations proposed by the *Forum des droits sur l'Internet* on child pornographic content, the third one has served as a policy tool and has been used by the Ministry of Interior to propose a new law that would make the filtering of child pornographic content mandatory for Internet access providers.

III. Current Developments

On 27 May 2009, the Ministry of Interior proposed a new Law on the *Orientation et Programmation pour la Performance de la Sécurité Intérieure* (LOPPSI II – Orientation and Programming for the Performance of Internal Security).[153] The purpose of the law is to improve the security of citizens in France, through objectives set up for 2009-2013. Cyber criminality is one of the topics covered. Chapter II of the draft law relates to the fight against cyber criminality and creates new provisions to protect Internet users against child pornography. Under the terms of draft Article 4, with the consent of the judiciary authority, the administrative authority (Ministry of Interior) will transmit to Internet access providers the electronic addresses of communication services offering child pornographic content. Internet access providers will have the obligation to block these URLs. A decree will detail the modalities of implementation of this article. At this stage, the content of the decree is unknown and there is no certainty that it will provide for a right of appeal against decisions wrongly blacklisting URLs.

The proposal has already been discussed and adopted, at first reading, by the National Assembly. The text has been forwarded to the Senate[154] but has not been scheduled yet for discussion. Several questions and concerns have already been raised.
According to the Committee in charge of national defence and armed forces, no appropriate impact assessment study has been done to show the efficiency of the filtering measure as well as the evaluation of the global costs (in terms of compensation for Internet access providers as well as means for the government's services). During the parliamentary debates before the National Assembly, the risk of over-filtering or wrong filtering was invoked but was not considered a sufficient reason to withdraw the measure. Arguments on the efficiency and proportionality of the measure as well as its intrusive nature have also been expressed, without convincing, at this stage, the majority at the National Assembly. More discussions should be expected before the Senate.

153 « Projet de loi d'orientation et de programmation pour la performance de la sécurité intérieure », n° 1697, 27 May, 2009, available at : http://www.assemblee-nationale.fr/13/projets/pl1697.asp

154 « Projet de loi, adopté par l'Assemblée nationale, d'orientation et de programmation pour la performance de la sécurité intérieure », n° 292, 16 February 2010, available at : http://www.senat.fr/leg/pjl09-292.html

Copyright

I. Current regulations

Legislative framework

The legal provisions concerning the use, copying and distribution of copyrighted materials in France can be found in the *Code de la Propriété Intellectuelle* (CPI – French Intellectual Property Code), in Chapter I, Authors' Rights, of the First Part concerning literary and artistic property. The Code has been amended several times and especially by the *loi sur le droit d'auteur et les droits voisins dans la société de l'information* (Loi DADVSI – Law on Authors' Rights and Related Rights in the Information Society),[155] implementing the InfoSoc Directive (2001/29/EC), and by the *loi favorisant la diffusion et la protection de la création sur Internet* (Loi HADOPI 1 – Law furthering the Distribution and Protection of Creation on the Internet),[156] completed by the criminal provisions of the *loi relative à la protection pénale de la propriété littéraire et artistique sur Internet* (Loi HADOPI 2 – Law pertaining to the Protection under Criminal law of Literary and Artistic Property on the Internet).[157]

The CPI gives to the authors of literary and artistic works the right to control the way their materials are being used by others. Several remedies are also available to right holders for non-authorized uses of their works. Under Article L. 122-4 CPI, any reproduction of a work without the author's or right holder's consent is unlawful. Reproduction shall be understood as the physical fixation of a work by any process permitting its communication to the public under Article L. 122-3 CPI.

In order to describe the duties of care applicable to the different Internet service providers, it is relevant to distinguish the duties of care of Internet access providers from the duties of care of hosting providers.

Responsibilities of Internet access providers

Internet service providers are exempted from liability if they act as mere conduits under Article 6-I-7 *Loi pour la confiance dans l'économie numérique* (LCEN – Law on Confidence in the Digital Economy), as described in the introductory chapter.

However, pursuant to Article 7 of the same law, when Internet access providers promote the possibility to download, through their Internet access, files they are not supplying, they must clearly indicate on their advertisements that piracy undermines artistic creation.

155 Loi no 2006-961 du 1er août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information, JORF n°178 du 3 août 2006, p.11529

156 Loi 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet, JORF n°135 du 13 juin 2009, p.9666

157 Loi n° 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet, JORF n°251 du 29 octobre 2009, p.18290

Besides the obligations contained in the LCEN, the HADOPI laws have created additional duties of care for Internet access providers. Under Article L. 336-3 CPI – previously Article 335-12 CPI – subscribers must secure their Internet access to prevent its use for online copyright infringements. Article 6-I-1, 2nd indent LCEN, amended by the HADOPI laws, states that Internet access providers must inform their subscribers about existing security mechanisms to help them to fulfill their obligation to monitor the use of their Internet access. Internet access providers must propose to their subscribers at least one efficient technical means, included in a list established by the HADOPI Agency. According to Article L. 331-27 CPI, Internet access providers have to mention in their subscription contract the provisions of Article L. 336-3 CPI together with the measures that can be taken against the subscribers in case of breach of their duty of surveillance, as well as the civil and criminal penalties applicable in case of copyright infringement.
Besides their duty to inform subscribers, Internet access providers have to assist the HADOPI Agency and the courts when they handle breaches of the duty of surveillance and copyright infringements. Under Article L. 331-25 CPI, when a subscriber does not comply with his duty of surveillance, the *Commission de Protection des Droits* (Committee for the Protection of Rights) – one of the two components of the HADOPI Agency – can ask Internet access providers to send a first warning e-mail to their subscribers and six months later a second one to ask them to comply with their obligations.
In case of copyright infringement (Article 335-7 CPI) or gross negligence linked to the breach of the duty of surveillance (Article 335-7-1 CPI), the court can pronounce against the subscriber a supplementary penalty consisting in the suspension of his Internet subscription for a limited period of time. Once the court decision becomes enforceable, the supplementary penalty will be notified to the HADOPI Agency, and then transmitted to the Internet access provider. Within two weeks after the notification, the Internet access provider will cut off the Internet access, or be subject to a fine of € 5,000.

Responsibilities of hosting providers

Concerning hosting providers, their duties of care regarding copyright infringing materials are defined in Articles 6-I-2 and 6-I-7 LCEN. Hosting providers do not have a general obligation to monitor information and activities they transmit or store. They only have the obligation to remove or disable access to the information when *they have actual knowledge of the illegal nature [*of the information or activity*], or when they are aware of facts or circumstances from which the illegal nature of the activity or information is apparent.* The actual knowledge of hosting providers about the presence of illegal content is presumed, following Article 6-I-5 LCEN, when they receive a notification, which contains elements allowing the identification of the author, description and localization of the facts, reasons for the removal and evidence that the author was contacted to be asked to remove the content. The legal provisions defining the liability of hosting providers must be read in light of a decision of the *Conseil Constitutionnel* (French Constitutional Council) interpreting the Law on Confidence in the Digital Economy (decision 2004-496 DC).[158] In this decision, the Council gives a strict interpretation of Article 6-I-2 LCEN and considers that hosting providers can only be held

158 Décision n°2004-496 DC, JORF du 22 juin 2004, p.11182.

liable for not having removed content reported as unlawful when (a) the content is manifestly unlawful or (b) its removal has been ordered by a court. According to the *Conseil Constitutionnel*, hosting providers are only judging the "manifestly unlawful" nature of content and not the legality or illegality of content.

II. Application of the current regulations

Legislative framework

Responsibilities of Internet access providers

The rules defining the duties of care of Internet access providers have been recently set up by the HADOPI laws. The HADOPI Agency, in charge of "protecting rights on the Internet", is in place since January 2010 but might not send the first warning emails before July 2010, according to the Ministry of Culture and Communication and the Secretary General of the HADOPI Agency.

Some purely technical issues also prevent the enforcement of the legal provisions. Internet access providers must propose to their subscribers security measures from a list established by the HADOPI Agency, in order to secure their access and avoid its use for copyright infringements. However, such a list does not exist yet. The decree, which should define the way the security measures will be assessed and granted a quality label, has not been adopted yet (as provided by Article L. 331-26 CPI). In addition, the government still needs to define the offence of "gross negligence" linked to the breach of duty of surveillance by the Internet subscriber.[159]

Responsibilities of hosting providers

The responsibilities of hosting providers are framed by Article 6-I-2 et seq. LCEN. However, the exact scope of their obligations is subject to interpretation. According to the decision of the *Conseil Constitutionnel*, 2004-496 DC, interpreting Article 6-I-2 LCEN, only "manifestly" unlawful content should be removed by hosting providers, without the need for a court order. The notion of "manifestly unlawful" content has never been defined but some commentators consider that it covers the list of very harmful and illegal content described in Article 6-I-7, 3rd indent, of the LCEN (i.e. content relating to crimes against humanity, racial hatred, child pornography, incitement to violence or detrimental to human dignity).

No link has ever been made by the courts between the interpretation of the *Conseil Constitutionnel* and the list of illegal content mentioned in Article 6-I-7, 3rd indent LCEN.[160] Some courts have extended the notion of "manifestly" illegal content to other content.[161]

159 A decree is expected end of June 2010 but no official information on its content is available.

160 Thoumyre (2008).

161 CA Paris, 14ème ch.A, 12 déc. 2007, Google Inc et Google France v. Benetton Group et Bencom (trademark infringement and unlawful contents).

Concerning copyright infringement material, they have decided that such content does not have a manifestly unlawful nature.[162]

However, when right holders notify illegal content following the notification procedure of Article 6-I-5 LCEN, hosting providers have the obligation to remove it. Although this procedure is optional, courts seem to consider it mandatory to establish the effective knowledge of a hosting provider about the presence of copyright infringing materials on its website. Once properly informed (i.e. notified), the hosting provider has the obligation to remove the piece of content. It should be noted that the *Tribunal de Grande Instance* (French First Instance Court) and *Cour d'appel de Paris* (French Court of Appeals) have ruled that in the absence of accurate notification (missing URL, titles or localisation of the disputed materials), hosting providers could not be held liable for not having removed the disputed materials.[163]

Lower courts have also created an "extra duty of care" obliging hosting providers to monitor "a priori" subsequent infringements relating to already identified infringing materials. According to the *Tribunal de Grande Instance de Paris*, once a hosting provider has removed notified content, it has the duty to prevent its new publication by different users, without receiving any new notification.[164] The same Tribunal has, nonetheless, slightly adjusted its position in a case where a hosting provider had proposed adding watermarks to the materials and using software to notify new illegal content but the plaintiffs had not responded. In that case, the hosting provider was not liable for any new posting of the already notified illegal material.[165] However, in the absence of any decision from the *Cour de Cassation* (French Supreme Court), either confirming or reversing these judgments, it should be emphasized that the decisions of the *Tribunal de Grande Instance de Paris* do not have a binding effect.

162 TGI Paris, 15 April 2008, Jean-Yves Lafesse v. Dailymotion ; TGI Paris 15 April 2008, Omar & Fred v. Dailymotion ; TGI Paris, 22 September 2009, ADAMI, Omar & Fred v. YouTube.

163 TGI Paris, 24 June 2009, Jean-Yves Lafesse v. Google ; CA Paris, 6 May 2009, Dailymotion v. Nord Puest Productions & UGC Images.

164 TGI de Paris, Zadig Productions v. Google Video, 19 October 2007 ; TGI de Paris, Ordonnance de référé, Roland Madgane et autres v. YouTube, 5 March 2009 ; TGI Paris, 10 April 2009, Zadig Productions v. Dailymotion.

165 TGI Paris, 24 June 2009, Jean-Yves Lafesse v. Google Video.

Identity Fraud

I. Current regulations

Legislative framework

In France, the legal provisions relating to identity fraud can be found in Articles 433-19, 434-23 and 313-1 of the *code pénal* (French Penal Code) and Article 781 of the *code de procédure pénale* (French Code of Criminal Procedure).

Under Article 433-19 *code pénal*, the use of somebody else's name or a part of it as well as the change, alteration and modification of somebody else's name in an authentic document or an administrative document drafted for the public authority constitutes an offence, punished by 6 months' imprisonment and a fine of € 7,500. Article 781 *code de procédure pénale* makes punishable the use of a false name to obtain somebody else's criminal record.

Under Article 434-23 *code pénal*, the use of somebody else's name constitutes an offence only if the name is used in circumstances that lead or would have led to the initiation of criminal prosecution against the person whose identity has been stolen. The offence is punished by 5 years' imprisonment and a fine of € 75000. Under French law, the mere use of somebody else's name does not constitute an offence. Only the consequences of the identity theft (such as fraud with the use of a false name under Article 313-1 *code pénal*) and not the identity theft itself are punishable.

Regarding identity fraud, whether it concerns the prevention, the fight or search for offences, Internet service providers do not have any formal duties of care. They only have the duty to prevent security breaches relating to personal data – which could lead to identity fraud – as provided by Article 34 of *Loi n°78-17 du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés* (Loi Informatique et Libertés – Act 78-17 of 6 January 1978, Law on data processing, data files and individual liberties). Under this article, data controllers (including Internet service providers) take all the useful precautions, with regard to the nature of the data and risks of processing, to preserve the security of data and, in particular, to prevent their alteration and damage or access by non-authorized third parties (see Section on breaches of Internet security and safety for more details).

Other regulatory measures

In 2006, the Directorate for media development, a department answerable to the Prime Minister, was asked to launch operations to draw public attention to the issue of transaction security on the Internet. The purpose was to increase the use of authentication tools to prevent identity theft. According to the Secretary of State in charge of strategic

studies and the development of the digital economy,[166] Nathalie Kosciusko-Morizet, identification permits to disclose the identity of an entity, whereas authentication consists in verifying the identity of an entity. Authentication ensures that the Internet user's interlocutor is who he or she claims to be before the Internet user identifies him or herself. Authentication is viewed as a way to prevent the dissemination of personal data that, if fraudulently reused, would allow the signature of transactions under a stolen identity. The discussions and consultations with professionals and public authorities led to the signature of a *Charte pour la promotion de l'authentification sur Internet* (Charter to promote authentication on the Internet). The Charter was first signed in February 2008 by public authorities, and in June 2009 by players of the industry, including Free, eBay and Yahoo!France. The Charter does not contain articles but principles to which the signatories commit: provision of information to users regarding the different forms of malevolence (such as spam, phishing), but also promotion of appropriate authentication practices and authentication methods to secure computers.

On 1 February 2010, the Secretary of State in charge of strategic studies and the development of the digital economy presented a new quality-label called "IDéNum", a single electronic identity certificate to replace passwords and login on public and private websites using a small secure device. The French Banking Federation (FBF) and the French Insurance Federation (FFSA) are among the partners.[167]

II. Application of the current regulations

Legislative framework

Regarding the definition and prosecution of identity fraud (under Article 434-23 *code pénal*), the Court of Cassation has ruled that identity fraud is only punishable if the offence for the committing of which the identity was stolen is also punishable. When the identity theft is linked to defamatory acts, which are not proven or void, the identity theft is not punishable.[168] The intent of fraud in using the stolen identity is crucial. If the use of somebody else's electronic address does not amount to an identity fraud, the electronic address constitutes however an online identity.[169]

166 "Nathalie-Kosciusko-Morizet mobilizes actors of the digital environment to increase the Internet users' security", Press Release relating to the signature of the "Charter to promote authentification on the Internet", 17 June 2009

167 "Présentation du Label IDéNum, l'identité numérique multi-services », Press Release, 1 February 2010, available at http://www.telecom.gouv.fr/fonds_documentaire/internet/presentation_IDeNum.pdf

168 Cour de Cassation, Chambre Criminelle, N. 05-85857, 29 Mars 2006; Cour de Cassation, Chambre Criminelle, N. 06-84365, 30 Mai 2007 linked to Cour de Cassation, Chambre Criminelle, N.08-83255, 20 Janvier 2009

169 Cour de Cassation, Chambre Criminelle, N.08-83255, 20 Janvier 2009

Other regulatory measures:

The *Charte pour la promotion de l'authentification sur Internet* has been signed by several web 2.0 platforms, but only by one Internet service provider, Free. It should be noted that AFA, the French association representing the interests of Internet service providers in France, did not sign the document, although it falls under the scope of its members' activities.

III. Current Developments

Since several years, the issue of online identity theft has been identified as a priority in France.[170] In 2005,[171] and 2008,[172] two senators proposed a law to criminalize online identity theft, without the need of a fraudulent intent. None of these proposals has ever been discussed before the Parliament.

However, the Ministry of Interior also proposed on 27 May 2009, a law on the *Orientation et Programmation pour la Performance de la Sécurité Intérieure* (LOPPSI II – Orientation and Programming for the Performance of Internal Security).[173] The purpose of the law is to improve the security of citizens in France, through objectives set up for 2009-2013. Cyber criminality is of one of the topics covered. Chapter II of the draft law relates to the fight against cyber criminality and introduces a new Article 222-16-1 *code pénal,* which creates two offences in relation to identity theft. Making use, on an electronic communication network, of a third party's identity or data allowing his/her identification is an offence when there is intent to disturb his/her peace (or anyone's peace) or when there is intent to affect either his/her honour or his/her consideration. Both offences would be punishable by a penalty of 1 year's imprisonment and a fine of € 15,000. The proposal has already been adopted by the National Assembly[174] and forwarded to the Senate for discussion and adoption. During the discussions of the proposal of the law, several comments were made regarding the proportionality of the sentence and the vague notion of "disturbing somebody's peace".

---

170 A project of online ID (CNIE-Carte d'Identité Numérique) was also launched in 2005

171 « Proposition de loi tendant à la pénalisation de l'usurpation d'identité numérique sur les réseaux informatiques », n°452, by M. Michel Dreyfus-Schmidt, 4 July 2004, available at : http://www.senat.fr/leg/ppl04-452.html

172 « Proposition de loi relative à la pénalisation de l'usurpation d'identité numérique », n°86, by Mme Jacqueline Panis, 6 November 2008, available at : http://www.senat.fr/leg/ppl08-086.html

173 « Projet de loi d'orientation et de programmation pour la performance de la sécurité intérieure », n° 1697, 27 May , 2009, available at : http://www.assemblee-nationale.fr/13/projets/pl1697.asp

174 Projet de loi, adopté par l'Assemblée nationale, d'orientation et de programmation pour la performance de la sécurité intérieure », n° 292, 16 February 2010, available at : http://www.senat.fr/leg/pjl09-292.html

Trade in stolen goods

I. Current regulations

Legislative framework

The legal provisions relating to the sale of stolen goods can be found in Article L. 321-3 of the *code de commerce* (French Commercial Code) and in Article 311-1 et seq. of the *code pénal* (French Penal Code).

Online auctions are defined in Article L. 321-3 *code de commerce*, which distinguishes real online auctions, involving a third party selling a product to the highest bidder, from brokerage operations in online auctions, characterized by the absence of a sale by auction and the intervention of a third party. The latter do not constitute a sale by public auction according to Article L. 321-3 and are only subject to this code when they involve cultural property.

Regarding the sale of stolen goods, Article 311-1 *code pénal* punishes the fraudulent appropriation of something belonging to another person by 3 years' imprisonment and a fine of € 45,000. The receiving of stolen goods defined as concealment, retention or transfer of a thing that was obtained by a felony or misdemeanour as well as the fact of acting as an intermediary in its transfer is punished, under Article 321-2 *code pénal*, by a penalty of 5 years' imprisonment and a fine of € 375,000.

No articles provide for the responsibility of Internet service providers in case of sale of stolen goods on auction websites. Under Article 6 of the *Loi pour la confiance dans l'économie numérique* (LCEN – Law on Confidence in the Digital Environment), implementing Article 15 of the E-commerce Directive, Internet service providers do not have a general obligation *to monitor information and activities they transmit or store nor a general obligation to actively seek facts or circumstances indicating illegal activities.* Hosting providers only have the obligation to remove illegal content when they are informed – or should be aware – of its presence (as described in the introductory part).

Other regulatory measures:

As regards stolen goods on auction websites, only one initiative can be mentioned. The *Forum des droits sur l'Internet*, a co-regulatory independent body, has adopted a Recommendation on the specific aspect of the online brokerage of cultural goods. A part of

it relates to the traffic of stolen cultural goods.[175] Inspired by the rules applicable to "offline" auctions, the Forum suggests to maintain a register of cultural goods offered for online sale with a description of the objects and elements enabling the identification of the sellers (adjustment of the current Article 321-7 *code pénal*) and to keep the data for a period of maximum 5 years. The Forum also recommends putting in place an online advertisement prior to the sale as well as reinforcing the cooperation between online brokers and public authorities through the use of technical tools such as a register keeping descriptions of all the stolen cultural goods. The Recommendation does not create any specific duties of care for Internet service providers regarding the trade of stolen cultural goods.

Under this section, another initiative in a field different from the sale of stolen goods on auction websites, but related, can be mentioned. In 2009, the government asked experts[176] to establish a protocol of cooperation between e-commerce platforms (auction websites) and trademark holders regarding the online sale of counterfeit goods. In December 2009, a *Charte pour lutter contre la contrefaçon sur internet* (Charter to fight online counterfeiting) was signed by trademarks holders and e-commerce platforms.[177] The document constitutes a statement of best practices, composed of 17 Articles defining the modalities of cooperation and the measures to be put in place to fight counterfeiting. The parties mutually commit for a period of 18 months to concrete solutions. E-commerce platforms agree to set up technical measures to detect counterfeit goods and sellers of such goods. The Charter creates a system of "Notice and Take down", where trademark holders notify the e-commerce platforms about offers of sales relating to counterfeit goods and the e-commerce platforms remove the offers, prevent any new subscription and sanction the infringers (suspension and termination of accounts). The Charter also provides for rules regarding the detection of a seller likely to sell counterfeit goods and the sale of goods imported in the European Economic Area.

In the absence of specific legal obligations, some auction platforms have elaborated their own internal rules that sellers must comply with in order to offer their products for sale. Stolen goods are a part of the list of prohibited products for sale. On its website, eBay France also recalls the criminal offences applicable to the theft and receiving of stolen goods.[178] In addition, eBay has adopted specific policy rules against the sale of counterfeit goods and introduced the VeRO system (*programme d'aide à la protection de la propriété intellectuelle* – Verified Rights Owners). Under this program, right holders can report to eBay goods that are infringing their intellectual property rights. Notified content is handled by a special team of eBay.

175 Recommandation, le courtage en ligne des biens culturels, juillet 2004, le Forum des droits sur l'Internet

176 Bernard Brochand, President of the National Committee against counterfeiting (CNAC) and Pierre Sirinelli, Professor at University Paris 1 (Panthéon-Sorbonne) and Member of the High Council of Literary and Artistic Property (CSPLA)

177 http://www.economie.gouv.fr/actus/091216charte-internet.html

178 http://pages.ebay.fr/help/classifieds/policies-stolen.html

II. Application of the current regulations

Legislative framework

Regarding the liability of Internet service providers for the trade of stolen goods, the fundamental issue relates to the status of auction websites. Several courts, including the *Cour d'appel de Paris* (French Court of Appeals), have ruled that eBay was a hosting provider as defined by Article 6-I-2 LCEN and not responsible for monitoring a priori "the quality, security, legality of the proposed products as well as the truth and accuracy of ads put online, the capacity of the sellers to sell the goods or services, and the capacity of the buyers to pay for the said goods and services".[179]

This ruling was confirmed by the *Cour de Cassation* (French Supreme Court), although the Court did not have to decide on the status of eBay.[180] It should be mentioned that the *Tribunal de commerce* (Commercial First Instance Court) has developed, in three decisions of 30 June 2008, a different trend. In cases relating to the sale of counterfeit goods, the Tribunal refused to qualify eBay as a hosting provider as it considered that the commercial platform was an intermediary between sellers and buyers and not a mere hosting provider. Article 6-I-2 LCEN was not applicable to eBay, whose liability was based on Articles 1382 and 1383 of the Civil Code. As a broker, eBay had the obligation to ensure that its activity did not facilitate any unlawful activities such as the sale of counterfeit goods. eBay was held liable because of its negligence (lack of surveillance) and failure to act (refusal to put in place efficient and appropriate measures to fight the sale of counterfeit goods).

The status of e-commerce platforms has also been discussed in two reports. The Information Report on the application of the Law on Confidence in the Digital Environment pleads for an adjustment of the hosting providers' liability for web 2.0 platforms.[181] More specifically, concerning eBay and other auction platforms, the report suggests a new status of website manager, which would be liable for setting up a mechanism to fight and prevent counterfeiting but not for the sale of counterfeit goods. The Report on online intermediaries by the *Conseil supérieur de la propriété littéraire et artistique* (CSPLA – High Council of Literary and Artistic Property) discusses the issue of the status of commercial platforms and concludes that the applicable liability regime should depend on the type of activities performed by the e-commerce platform and not on a qualification

179 Cour d'Appel, Paris, 14e chambre, Section B, eBay v. DWC, 9 Novembre 2007 ; TGI Strasbourg, 1ère chambre civile, Jean L. v. eBay France, 15 Décembre 2009;

180 Cour de Cassation, Chambre commerciale, DWC v. eBay, 5 Mai 2009

181 « Rapport d'information de la Commission des Affaires Economiques, de l'Environnement et du Territoire à l'Assemblée Nationale, sur la mise en application de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique » n°627, by M. Jean Dionis du Séjour et Mme Corinne Erhel, 23 January 2008, available at http://www.assemblee-nationale.fr/13/rap-info/i0627.asp

of the actor itself.[182] An e-commerce platform could therefore be held liable under the hosting provider's liability regime for hosting content and under the civil liability regime for other activities such as brokerage.

Other regulatory measures:

To our knowledge, the Recommendation of the *Forum des droits sur l'Internet* has not introduced any changes in the law. It should also be noted that the scope of the Recommendation is limited to the online trade of cultural goods.

Regarding the *Charte pour lutter contre la contrefaçon sur Internet*, the document has only been signed by two French e-commerce platforms: PriceMinister and 2xmoinscher. Amazon and eBay have refused to sign it, which lessens its impact.

182 Rapport, Commission spécialisée sur les prestataires de l'internet, Conseil supérieur de la propriété littéraire et artistique, 21 juin 2008, www.cspla.culture.gouv.fr

2. Advisory Committee

Prof. mr. F.W. Grosheide (chairman)
University of Utrecht - Molengraaff Institute for Private Law

Dr. F.W. Beijaard
WODC

Prof. dr. M.J.G. van Eeten
Delft University of Technology, Faculty Technology, Policy and Management

Mevrouw dr. M. van der Linden
University of Utrecht, Faculty of Law

De heer ing. R. Volf
Ministry of Economic Affairs

De heer drs. ing. G.J.C. Wabeke
KPN

Mevrouw A.H.G. van Zantvoort
Ministry of Justice

3. Interviews

Netherlands

Organisation	Name	Function
Bits of Freedom	Ot van Daalen	Director
eBay.nl	Stefan Krawczyk	Senior Director and Counsel Government Relations Europe
Google	Sarah Greenwood	European Policy Manager
Google Netherlands	Jeroen Schouten	Legal counsel Benelux
ISP Connect	Arnout Veenman	Chairman
KPN Security	Gert Wabeke	Manager 'Justitieel' Aftappen en Monitoren
Marktplaats.nl	Foekje Croles	Head of Legal European Classifieds
Marktplaats.nl/eBay.nl	Chantal Malfeyt	Trust & Safety Manager
Ministry of Economic Affairs	Roman Volf	Policy Advisor
Ministry of Justice	Erik Planken	Senior Policy Advisor beleidsadviseur
Ministry of Justice	Anja van Zantvoort	Policy Advisor

Organisation	Name	Function
OPTA	Daan Molenaar	Head Internet safety & head of communications
Police Limburg-Zuid	Peter Reijnders	Program manager child pornography
Vrije Universiteit (VU)	Rik Kaspersen	Professor/expert
XS4ALL	Margreth Verhulst	Public Affairs & Regelgeving

United Kingdom

Organisation	Name	Function
ISPA UK	Andrew Kernahan	Policy Officer
Ministry for Business, Innovation and Skills	Nigel Hickson	Head of Global ICT Policy
OFCOM	Jeremy Olivier	Head of Multimedia
Queen Mary University/ IWF	Ian Walden	Professor of Information and Communications Law / IWF Independent Vice-Chair
SOCA e-crime unit	Jonathan Flaherty	Technical Senior Officer
	Richard Hyams	Technical Senior Officer
Vodafone	Neil Brown	Legal Advisor
	Stephen Deadman	Executive Solicitor and Vodafone's Group Privacy Officer
	Richard Feasey	Public Policy Director

Germany

Organisation	Name	Function
Bundesministerium für Wirtschaft und Technologie + Bundesministerium für Justiz	Rolf Bender	Department VI B 4 – Medienrecht und Neue Dienste
	Marcus Schladebach	Department für Telecommunications Recht
BITKOM – Bundesverband Informationswirtschaft	Guido Brinkel	Bereichsleiter Telekommunikations- und Medienpolitik
FSM – Freiwillige Selbstkontrolle Multimedia-Dienstanbieter	Sabine Frank	Managing director
eco – Verband der deutschen Internetwirtschaft	Frank Ackermann	Director Self-Regulation eco; Vice President INHOPE
Deutsche Telekom AG	Veronica Frey	Senior Manager Media Regulation
	Andreas Goeckel	Leiter Multimedia- und Internetrecht

France

Organisation	Name	Function
Ministère de l'Enseignement supérieur et de la recherche	Bernard Benhamou	Délégué aux Usages de l'internet
ARCEP (l'Autorité de Régulation des Communications Electroniques et des Postes)	Loïc Taillanter	Directeur juridique adjoint
	Joëlle Toledano	Membre
CNIL (Commission Nationale de l'Informatique et des Libertés)	Gwendal Le Grand	Chef du Service de l'Expertise Informatique
	Leslie Bass	Juriste
OCLCTIC (Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication)	Adeline Champagnat	Commissaire de police
AFA (Association des Fournisseurs d'Accès et de Services Internet)	Quentin Aoustin	Juriste - analyste de contenus
AFA	Nicolas d'Arcy	Juriste - analyste de contenus
Free	Alexandre Archambault	Legal Advisor
	Nicolas Jaeger	Public Relations
Centre National de la Recherche Scientifique (CNRS)	Pierre-Jean Benghozi	Directeur de recherche
Forum des droits sur l'Internet	Laurent Baup	Juriste – Chargé de mission
	Stéphane Grégoire	Juriste – Chargé de mission