Duties of care on the Internet

van Eijk, N.; van Engers, T.; Wiersma, C.; Jasserand, C.; Abel, W.

Publication date
2011
Document Version
Submitted manuscript
Published in
TPRC: the research conference on communication, information and internet policy: 2011 program with paper links

Duties of care on the Internet

Paper presented at the
Telecommunications Policy Research Conference (TPRC)
September 23-25, 2011

Institute for Information Law (IViR)

Leibniz Center for Law

Nico van Eijk

Tom van Engers

Chris Wiersma

Catherine Jasserand

Wiebke Abel

University of Amsterdam, 2011

Contents

1 Duties of care

1.1 Introduction

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.[1] The aim of the study is to analyse specific forms of duties of care in the Netherlands, France, Germany and the United Kingdom. These countries were selected based on the fact that they represent different policy/regulatory systems or because they are known for interesting developments. The European context is also taken into account.

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 regulation, 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.

Duties of care primarily concern the relationship between the government and Internet service providers and usually take the form of regulation or co-regulation. Where this is 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 co-regulation and self-regulation.

The relationship between government and Internet service providers may have consequences for the responsibility and liability of Internet service providers.[4] These (civil-law) aspects are beyond the scope of this study.

---

1 The Study was commissioned by the Dutch Scientific Research and Documentation Centre (*Wetenschappelijk Onderzoeks- en Documentatiecentrum*, WODC). The original version of the report: Prof. Dr Nico van Eijk (IViR, www.ivir.nl/staff/vaneijk.html/) and Prof. Dr Tom van Engers (Leibniz, www.leibnizcenter.org/information/people/tom-van-engers) in collaboration with Wiebke Abel LLM., mr. Catherine Jasserand and mr. Chris Wiersma, *Moving Towards Balance, A study into duties of care on the Internet*, Amsterdam 2010.

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.

4 On the issue of liability, see Van Hoboken (2009).

1.2 Themes and e-commerce directive

The analysis of duties of care takes place from the perspective of five themes with the idea that in principle they represent the most relevant aspects of the underlying problems.

The first theme relates to breaches of Internet security.[5] What kinds 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.

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.[6]

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 copyrights.

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.[7]

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 each other or raise similar issues, for instance with respect to security aspects and applied procedures (such as forms of notice and take down)[8], or in the field of enforcement.

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 a regulated relationship between the government and Internet service providers, and if so, what kind of relationship.

---

5 On security, see for instance Coupez (2010). On security, see for instance Coupez (2010).

6 About child pornography: Stol e.a. (2008)

7 Van der Meulen (2006); De Vries e.a.(2007).

8 Schellekens, Koop & Teepe (2007).

Several themes have strong ties with the E-commerce Directive ('Directive on electronic commerce')[9] of 2000, more in particular with respect to Internet service providers. The Directive comprises a system in which three activities are distinguished: 'mere conduit', 'caching' and 'hosting'.[10] Mere conduit (Article 12) consists of the unmodified 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 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 falls within the scope of this study.

In 2007, the E-commerce Directive was extensively assessed in a report by G. Spindler and T. Verbiest.[11] 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 Spindler/Verbiest report, however, is different and focuses on the liability of intermediaries in a general sense. The report is also part of the background documents of the recent consultation on the revision of the E-commerce Directive.[12]

---

9 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.

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

11 Spindler/Verbiest 2007.

12 http://ec.europa.eu/internal_market/e-commerce/directive_en.htm and http://ec.europa.eu/internal_market/consultations/2010/e-commerce_en.hhttp://ec.europa.eu/internal_market/consultations/2010/e-commerce_en.htmtm. The consultation has been closed, but the comments have not yet been published.

1.3 Methodology

The literature on the legal and policy-based context of the five themes as well as the involvement of Internet service providers has been analysed. The relevant regulations and/or self-regulation have been inventoried and summarized in country-specific studies.[13]

Because of the highly dynamic nature of the subject matter of the study and its ongoing development, a traditional study of literature was deemed insufficient. 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 paid to the selected countries, and interviews were conducted with 6 to 8 stakeholders in each country.

Meetings took place with representatives of (interest groups of) Internet service providers, governments, regulatory and supervisory bodies, social organizations and independent experts.

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.

13 These country studies are available as appendices to the original part.

2 Findings

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 co-regulation exist.[14]

2.1. Internet security

By virtue of Article 4 of the Directive on privacy and electronic communications adopted in 2002, 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.[15] 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.[16] 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

14 In an appendix to the original study, more extensive country reports are made available. These country-specific studies also include references to relevant parliamentary documents, literature and jurisprudence.

15 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 or e-privacy directive) OJ L 201/37 (31 July 2002).

16 Amendments to the Framework Directive and the Universal Service Directive: Directive 2009/136/EC of 25 November 2009, OJ L 337/11 (18 December 2009) ('Citizens' Rights Directive') and Directive 2009/140/EC of 25 November 2009, OJ L 337/37 (18 December 2009) ('Better Regulation Directive') .

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. 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 a national level. In addition, the European Commission can adopt technical implementing measures.

In all countries, 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. However, 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 defined any further in regulations or jurisprudence.

In the Netherlands, on the initiative of the Independent Post and Telecommunication Authority (*Onafhankelijke Post en Telecommunicatie Autoriteit*, OPTA), a process has been started 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.[17]

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

17 Dumortier and Somers (2008).

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 on 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 reporting clients. 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 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 a 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 (e.g. web transactions, financial services).

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 generally indicated that Internet traffic inspections[18] 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

18 By using Deep Packet Inspection (DPI), for instance.

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.[19] Quarantine measures for such computers seem to be necessary, but limiting Internet access also has an adverse 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 arose whether the national government could play an active role in instructing end-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. Besides the national telecommunications regulator, other authorities in the field of privacy and national defence could play a role.

19 In this context, see Van Eeten e.a. (2010).

2.2 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.[20] 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. 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 against the proliferation of child pornography.[21] A proposal has been published to replace the Framework Decision by a directive.[22] 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.[23] 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[24] programme, and further cooperation between Europe and the United Stated (where apparently most child pornography is hosted) has been announced.[25] Which form is used for blocking, 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 the 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.

Even before the adoption of the E-commerce Directive, the theme of child pornography received ample attention. In practice, notice and take down is

20 International Association of Internet Hotlines, www.inhope.org.

21 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.

22 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.

23 On blocking, i.e.: Callanan e.a. (2009).

24 Cospol Internet Related Child Abusive Material Project (www.circamp.eu).

25 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

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 an international level. Most of the time, Internet service providers send their notifications directly to these hotlines.

EU-initiatives to make filtering of child pornography obligatory raised serious concerns about proportionality and effectiveness. Original plans were abandoned by the European Parliament in February 2011.[26]

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 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*), originally support plans for filtering Internet traffic for child pornography. These

26 http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+IM-PRESS+20110131IPR12841+0+DOC+XML+V0//EN&language=EN

plans have been abandoned based on similar arguments as put forward by the European Parliament.

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, including 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 signalling 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.[27] 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 (such as copyright).

In general, the interviewees were satisfied with how the INHOPE hotline system is functioning. One of the benefits mentioned 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 for the purpose of finding child pornography 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. Interviewees 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.

27 The Forum was closed down in December 2010, because its funding was terminated (http://www.foruminternet.org/)

2.3 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. 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] eventually have 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 freedoms are to be observed by member states when taking measures on access to, or the use of, services and applications by end-users.

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 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.

In the Netherlands, a number of court decisions establishing the liability of certain Internet (service) providers for copyright infringement has 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 did not 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 had unlawfully facilitated a copyright breach. In the literature, there is much criticism on this decision.

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 Van Eijk (2011).

30 In some countries, e.g. the Netherlands, downloading is not punishable; in other countries it is. See the 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).

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 purposes is a permitted act, has recently been under discussion at a parliamentary level. Such an exception (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. 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. New regulations might include the abolition of the private use exception and the introduction of enhanced enforcement mechanisms (primarily aimed at commercial and large-scale infringements).

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. By virtue of the Digital Economy Act, however, which was recently passed, Internet service providers are to forward notifications of rightful claimants to alleged infringers actively. 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 impose 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 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 afore-mentioned 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 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, the interpretation is usually 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.

2.4 Identity fraud

Identity fraud on the Internet is understood to mean appropriating somebody else's identity with the intention of committing unlawful acts. 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. 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.

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.[32]

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 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.

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.[33] 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.

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

33 http://www.idenoum.com/.

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. 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 was mentioned several times as a major element in countering identity fraud and has led in various countries to public campaigns, among other things.

2.5 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,[34] where the issue is not stolen goods but the sale of articles that breach intellectual property rights. Recently, the European Court of Justice decided in this case that service providers who play an active role cannot rely on the exemption of the E-commerce directive.[35] An active role can consist of actions such as to giving knowledge of, or control over, the data relating to the offers for sale, when providing assistance which entails, in particular, optimizing the presentation of the online offers for sale or promoting those offers. The impact of the case is yet unclear (the national court now has to take a final decision), but it seems justified to conclude the decision will affect the position of intermediaries.

It should be kept in mind that the following paragraphs describe the situation prior to the L'oréal/eBay decision.

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. Auction and selling platforms are the 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

34 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.

35 ECJ 12 July 2011, Case C-324/09 (L'oréal and Others v eBay).

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 (owned by eBay) 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, 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.

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 to set 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 eBay has invested in particular.[36] This procedure also relates to the identification of rightful claimants and to identifying relations with advertisements on the platforms afterwards.

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

3 Analysis and conclusions

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

3.1 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).[37] 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 and platform providers (auction sites, social networks), 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, play an important role in this context. 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 need to be taken into account. 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.

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

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

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. Imposing 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,[38] 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.

38 OECD (2010); Dommering and Van Eijk (2010); Rand Europe (2008); Ofcom (2008).

3.2 Internet access/service 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 regime 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 a "separate" contractual relationship with the end-users. In this context, it is important 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 net 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.

3.3 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 regimen 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),[39] 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 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 (see section 1.2).

3.4 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 statutory 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 practice 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.

39 See Van Hoboken (2009) and the European Commission (2003).

3.5 Enforcement

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,[40] 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.[41] 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. Recent developments show that filtering is no longer seen as the ultimate remedy. Initiatives on the European and national level have been abandoned.

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

40 Stol e.a. (2008).

41 See for instance Stol (2008); Callanan e.a. (2009).

models. Finally, several parties have expressed their concern that peer-to-peer technology 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.

3.6 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 system 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 statutory law) is generally not deemed necessary. The sale of stolen goods via platform providers (e.g. 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 following conclusions can be drawn:

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 assessed 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.[42] What might work in one specific context, might not be the right solution for others due to difference in regulatory and/or judicial traditions.

3. Deployment of enhanced 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 co-regulation. 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.

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

42 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.

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.

4 Bibliography

(indicative)

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.

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. (Convergence in regulation: Reflections on electronic communications)

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 softw*are, 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.

Van Eijk (2011)

File Sharing, note written at the request of the European Parliament's Committee on Legal Affairs, 2011 (http://www.ivir.nl/publications/vaneijk/pe432775_en-rev-fin.pdf).

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).

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.

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.

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.

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. (Filtering Child Pornography on the Internet An Investigation of National and International Techniques and Regulations. English Summary: http://www.wodc.nl/images/1616_summary_tcm44-117165.pdf).

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.

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.

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. (Identity Fraud; a demarcation, an international comparison of terminology and an analysis of national criminal offences, English Summary: http://www.wodc.nl/onderzoeksdatabase/identiteitsfraude.aspx?cp=44&cs=6796).

V.1.10