Duties of care on the internet

van Eijk, N.

Publication date
2012
Document Version
Proof
Published in
Cyber safety: an introduction
License
Other

20 Duties of Care on the Internet[66]

Nico van Eijk

20.1 Introduction

Internet Service Providers currently find themselves in the spotlight, in both 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 chapter focuses on duties of care in respect of the relationship between government and Internet Service Providers (ISP). It provides an overview of 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. The analysis of duties of care takes place from the perspective of three themes. The first theme relates to breaches of internet security.[69] What kinds of duty of care are provided for in order to deal with privacy breaches or malware placement? 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; ISPs have been closely involved in this aspect.[70] Copyright is the third theme. 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.

68 This chapter is based on the study *Moving Towards Balance: A study into duties of care on the Internet*, N.A.N.M. van Eijk, T.M. van Engers, C. Wiersma, C.A. Jasserand and W. Abel, WODC/University of Amsterdam, 2010, 125 p. Online: http://www.ivir.nl/publications/vaneijk/Moving_Towards_Balance.pdf.

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

70 About child pornography: Stol et al. (2008).

Box 20.1 ISPs, mere conduit, caching and hosting

ISPs' is understood to mean market parties engaged in providing access to the internet to end-users. In terms of telecommunications regulation, the activity in question consists of a 'public telecom service'. The E-commerce Directive ('Directive on electronic commerce') of 2000 comprises a system in which three activities are distinguished: 'mere conduit', 'caching' and 'hosting'. 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.

20.2 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) are required to take appropriate technical and organisational measures to safeguard the security

of the services provided.[71] 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 extended in the context of the revision of the European framework for the communication sector.[72] 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. 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 four 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 organisational measures to safeguard internet security. The second pertains to informing end-users about

71 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).

72 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').

specific risks and measures that can be taken to minimise 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. The new European rules, as described at the beginning of this paragraph have been implemented in the Dutch Telecommunications Act. OPTA, together with the Radiocommunications Agency ('Agentschap Telecom')[73] are responsible for supervision the rules.

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.[74]

Many Dutch internet service providers have entered into a covenant in which 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 email. This document is not compulsory for the members.
In Germany, a provision in the national telecommunications act deals with the organisational measures required of Internet Service Providers; the provision focuses on the prevention of interruptions, the effects of external attacks and

73 www.agentschaptelecom.nl.
74 Dumortier & Somers (2008).

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.

The French Government has drafted 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).

Respondents in our study (Van Eijk et al. 2011) emphasise 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[75] 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. Internet Service Providers may face blacklisting due to botnets, causing certain services, such as email, 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

75 By using Deep Packet Inspection (DPI), for instance. For research on the deployment of DPI, see: http://dpi.ischool.syr.edu/Home.html.

of the public sources mentioned is also difficult.[76] 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.

20.3 Child pornography

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.[77] A special Directive has been adopted.[78] Article 25, section 2 of the directive provides that member states should take measures to block access to child pornography.[79] This blocking should come with the necessary guarantees. Furthermore, member states are to take measures to remove child pornography from the

76 In this context, see Van Eeten et al. (2010).
77 Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography, JO L 13/44, 20.1.2004.
78 Directive 2011/92/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, JO L335/1 (17 December 2011).
79 On blocking, i.e.: Callanan et al. (2009).

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[80] programme, and various forms of cooperation between Europe and the United Stated (where apparently most child pornography is hosted) have been put into plac. 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.

20.4 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)[81] for the communication sector about the 'three strikes' – or graduated response – issues.[82] 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)[83] have not led in the end to European regulations. It should also be noted that Article 3a of the Framework Directive[84] stipulates 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.

80 Cospol Internet Related Child Abusive Material Project (www.circamp.eu).
81 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).
82 See also TNO/SEO/IVIR (2009) and Van Eijk (2011).
83 In some countries, e.g. the Netherlands, downloading is not punishable; in other countries it is. See the literature in the previous note.
84 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).

The regulations laid down in the E-commerce Directive are the decisive legal framework for the copyright theme in all four countries. On the basis of this, the duty of care of Internet Service Providers only pertains to measures for the 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 have given rise to a further discussion on the limits of the duty of care of Internet Service Providers. These cases 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, the court ordered an Internet Service Provider 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 of 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 purposes is a permitted act, has recently been under discussion at 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. 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, 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 bringing 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 (*Haute Autorité pour la Diffusion des Oeuvres et la Protection des Droits sur Internet*), has introduced 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 for that purpose. Such measures are included in a list prepared by the HADOPI authority, 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 the event 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 emails to end-users (stating that the unauthorised 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.

In French jurisprudence the interpretation 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. As 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. Concerning the HADOPI legislation, interviewed stakeholders in the study by Van Eijk and Van Engers (2010) 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. The same technology could then be used to share illegal content. Some emphasised that Internet Service Providers should not be put in the position of having to monitor internet traffic or 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 cyber crime. Many parties also pleaded for restraint when it comes to adopting HADOPI-like legislation.

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.

20.5 Internet Service Providers: general observations and conclusions

The environment of the subject under study – duties of care on the internet – is dynamic. Nevertheless, some general observations are provided here, and conclusions formulated.

Value chain

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 three 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. At first sight, placing the responsibility on the Internet Service Providers seems to be a simple option. After all, it is Internet Service Providers 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 becoming increasingly less compatible with the dynamics of the internet (such as the involvement 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.[85] 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 their direct relationship with end-users. At any rate, other parties in the value chain agree that in many cases Internet Service Providers are not the party on whom the duties of care should rest, and take a stand themselves as well. This is apparent, for instance, in their involvement in the fight against child pornography and in enforcing copyright.

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 email. It is clear that sufficient

85 OECD (2010); Dommering & Van Eijk (2010); Rand Europe (2008); Ofcom (2008).

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 distributors, cannot be held responsible for the content of what they transport.

As distributors 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 suggestthat, 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 with – 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 Providers as an access provider be strictly separated from the Internet Service Providers 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.

Local context

From the stocktaking and analysis of national regulations, it becomes clear that national circumstances are to some extent 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 broad outline, the Dutch practice seems to be close to the German position. There is self-regulation, and it works, more particularin the case of child pornography. The code of conduct for 'notice and take down' provides

some added value but also has its weak aspects, such as a wide potential for interpretation and the absence of an enforcement mechanism.

Conclusions

A varied picture emerges, which indicates that developments, including improving the balance within the value chain, are still in progress. 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 scarcely yet 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 four 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 of the new rules, and Van Eijk et al. (2011) show that the actual enforcement possibilities are also subject to much criticism.

Key concepts

- Mere conduit
- Caching
- Hosting
- Internet security
- Child pornography
- Copyright