Contribution to the European Commission's consultation on the future of electronic commerce in the internal market and the implementation of the Directive on electronic commerce (2000/31/EC)

Table of contents

Summary of recommendations

1. The concept of “specific” obligations of intermediaries to “prevent” illegal user action should be given up in its entirety. Intermediaries should only be required to remove illegal content upon notification.
2. Service providers should not be required to remove or disable access to information before it has been found illegal by a court of law.
3. The e-commerce directive should be amended to include strict sector-specific privacy rules for information society services.
4. Discrimination against users that legally exercise data protection rights must be prohibited.
5. Providers of information society services should be required to ensure the confidentiality of our Internet use.

I am contributing to the consultation as a private individual and a legal professional.

Before answering some of the specific questions posed by the Commission, I will deal with some points of particular importance.

A. Accessibility of company data protection officer (Art. 5 ECD)

It is becoming more and more important that **queries regarding personal data can be addressed directly to a company data protection officer** where such a person has been appointed. Service providers should therefore provide the details of a company data protection officer, including his electronic mail address, which allow him to be contacted rapidly and communicated with in a direct and effective manner (article 5 ECD to be amended).

B. Protect freedom of speech by stopping pro-active monitoring and "infringement prevention" (Art. 14 (3) ECD)

1. Case study: Unacceptable situation in Germany

The **German Federal Supreme Court** (Bundesgerichtshof) interprets the liability exemptions in the e-commerce directive not to be cover applications for injunctive relief, i.e. to claims for providers to prevent illegal user activity.[1]

In consequence, the **most far-reaching doctrine of contributory "liability"** is being applied by German courts, called "accessory liability" (*Störerhaftung*). According to this doctrine it is not only the wrongdoer himself (direct infringer) and participants (effective promoters or helpers) that can be subject to a claim for refraining from rights infringements, but also mere accessories, including providers of information society services. Responsibility for unlawful user action is extended to all persons who - without necessarily being wrongdoers or participants - deliberately and generally causally contribute to the infringement of a third party's right, provided they have the legal and effective means to detect and prevent the infringement.[2]

According to this doctrine, once an intermediary obtains knowledge of an infringement, it is not only obliged to remove the unlawful content but also to **take all technically feasible and reasonable precautions to prevent future infringements**. In other words, subject to the requirement of reasonableness, service providers are obliged to examine all user content as soon as they obtain knowledge of any unlawful content. The monitoring obligation is not limited to the detection of the unlawful content that was originally notified or to the original publisher of this content.[3]

1 BGH, NJW 2004, 3102 (3103); DG Market, Study on the liability of Internet intermediaries, http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/germany_12nov2007_en.pdf.

2 DG Market, Study on liability of Internet providers, http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf, p. 51.

3 DG Market, Study on the liability of Internet intermediaries, http://ec.europa.eu/internal_market/

In practice, **this jurisprudence effectively forces providers to pro-actively monitor user-generated content**, this being the only way they can avoid indictment.[4] Culpable breach of the monitoring duty is punished by a disciplinary fine or even a prison sentence.

A German court that finds a provider not to have taken sufficient steps to prevent infringements will grant injunctive relief by prohibiting the provider from letting users re-publish the illegal content, without setting out what measures the court deems necessary to prevent such infringement. The extent of the provider's pro-active obligations is determined only when the rights holder initiates a separate procedure for alleged violation of the injunction and applies for a disciplinary fine or a prison sentence to be imposed. So providers are told which steps to take only in the judgement that imposes a fine on them. This jurisprudence causes **unacceptable uncertainty for providers**.[5] It is impossible for intermediaries to anticipate which measures the courts will consider "reasonable".[6]

This doctrine also has **unacceptable repercussions on the freedom of speech** online, because providers threatened by fines will - often using automatic and broad filters - block and prevent any content that they consider might infringe a third party right. This leads to the suppression of controversial but politically very valuable content, as intermediaries to not wish the battle on the legality of the content to be fought at their expense.

Furthermore, German courts tend to **go very far in what measures they impose on providers to prevent future infringements** by their users: It was held that there was a duty to deploy technology to automatically scan all user-generated content for potentially infringing content.[7] Users that have generated illegal content in the past must be subjected to a manual examination of any future content they generate.[8] To this end, all users must be identified and the anonymous use of services must be disabled.[9] All user actions must be logged.[10] Content regarding issues that "provoke illegal reaction" must be examined manually.[11] All of these duties have been imposed not for the prevention of serious crime, but for the mere prevention of infringements of private titles including commercial rights.

2. The concept of private policing is failed

These "preventive duties" imposed by the courts violate article 15 of the e-commerce directive, according to which Member States - including their courts - must not impose a general obligation on providers to monitor information which they transmit or store. Injunctions lead to a **de facto obligation to monitor user-generated content**,[12] and thus amount to a general monitoring obligation.

---

e-commerce/docs/study/liability/germany_12nov2007_en.pdf.

4 DG Market, Study on liability of Internet providers, http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf, p. 51.

5 DG Market, Study on liability of Internet service providers, http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf, p. 67.

6 DG Market, Study on liability of Internet providers, http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf, p. 51.

7 BGH, NJW 2007, 2636 (2639 f.).

8 BGH, NJW 2008, 758 (762) – eBay.

9 OLG Hamburg, Urteil vom 02.07.2008 – 5 U 73/07 – Rapidshare.

10 OLG Hamburg, Urteil vom 02.07.2008 – 5 U 73/07 – Rapidshare.

11 OLG Hamburg, Urteil vom 22.08.2006 – 7 U 50/06 – Heise-Forum.

12 DG Market, Study on liability of Internet providers, http://ec.europa.eu/internal_market/e-

At any rate, **the entire concept of "specific" obligations to "prevent" illegal user action is failed**. In a democracy, everybody can trust in the integrity of their fellow citizens, even if it is known that this trust is sometimes abused. Fundamental freedoms constitute the foundation of justice and peace in the world.[13] Freedom is the purpose of all law. Its benefits for every person as well as for society as a whole by far outweigh the harm done by its abuse. A prevention society aimed at eliminating, as far as possible, all potential risks of human behaviour and life is not compatible with European values and freedoms.

According to general principles of civil law, **only those need to prevent harm that have created a hazard source**. The exchange of information is at the roots of human nature. It is a fundamental right (article 11 of the Charter of Fundamental Rights) and can therefore not be considered a "hazard source". The provision of telecommunications services does not create a greater risk of rights infringements than the provision of any product or service. Typical, socially adequate and therefore legal risks do not put their originator in a position of being responsible for intentional violations committed by other people using the products and services provided.

Also information society services are often similar to off-line activity such as personal discussions, noticeboards, CD recorders, photocopying machines or lockers. **Internet users must not be discriminated in a way that puts them under permanent scrutiny and surveillance on-line where similar activities off-line are completely anonymous and confidential**, simply because the Internet makes total control technically possible. The Internet must be kept as free as the rest of our lives. In information society we must defend our freedoms if we do not want to lose them gradually.

Even prevention (or policing) technology that can reasonably be implemented or is industry standard must not be imposed on all service providers because of its devastating effects on freedom of speech. **Filtering technology, for example, will by its nature suppress legal content that is merely similar to illegal content.** This leads to the suppression of controversial but politically very valuable content, for example critical comments on companies and products or "fair use" of intellectual property. Policing is not the job of private companies.

3. Recommendation

The concept of "specific" obligations of intermediaries to "prevent" illegal user action that is accepted in article 14 (3) and recitals 47 and 48 of the e-commerce directive should be given up in its entirety. Intermediaries should only be required to remove illegal content upon notification. The deterring effect of criminal sanctions is sufficient to "prevent" illegal user action.

commerce/docs/study/liability/final_report_en.pdf, p. 51.

13 European Convention on Human Rights, Preamble.

Recommendation:

- Service providers should not be required to "prevent" infringements. To this end, article 14 (3) ECD should read: "*This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate* ~~***or prevent***~~ *an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.*" Recitals 47 and 48 should be deleted.

C. Judicial review is needed to protect freedom of speech (Art. 14 (1) ECD)

The current liability limitations do not sufficiently protect free speech for another reason: A service provider that is notified of allegedly illegal content is not exempted from liability under the current directive even if is has reason to believe that the content may be legal. In practise this situation leads to the **removal of practically any notified content without proper assessment of its legality**, resulting in major damage to free speech on-line. Providers are being put in the position of a judge which they cannot fill. If they remove content which is later considered legal by the courts, they can be faced with high damage claims by the customer/user whose content was removed. If, on the other hand, the providers refuse to remove content which is later considered illegal by the courts, they can be faced with high damage claims by rights holders.

A service provider that is notified of allegedly illegal content should therefore **not be required to remove the content before its legality has been assessed by a judge** in a preliminary procedure. Member States can design this procedure to be fast and effective. However its cost must not be borne by the provider as this would again have a chilling effect on free speech. The requirement of a court ruling is not too great a burden on rights holders. A preliminary ruling can be obtained within a day in Germany, for example. As to the cost, needy claimants can apply for legal aid. Also claimants can recover theirlegal expenses by suing the user that generated the content.

I quote the Joint Declaration of the **OSCE Representative on Freedom of the Media** and Reporters Sans Frontières on Guaranteeing Media Freedom on the Internet:[14]

> *"A decision on whether a website is legal or illegal can only be taken by a judge, not by a service provider. Such proceedings should guarantee transparency, accountability and the right to appeal."*

14 https://www.osce.org/documents/rfm/2005/06/15239_en.pdf.

I also quote the Joint Declaration on International Mechanisms for Promoting Freedom of Expression of the **UN Special Rapporteur on Freedom of Opinion** and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression:[15]

> *"No one should be liable for content on the Internet of which they are not the author, unless they have either adopted that content as their own or refused to obey a court order to remove that content."*

Recommendation:

- Service providers should not be required to remove or disable access to information before it has been found illegal by a court of law. To this end, article 14 (1) (b) ECD should read: "*the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information* ***after it has been found illegal by a court of law***."

D. Ensure Internet privacy and anonymity

On the Internet **our every action can be tracked easily and comprehensively**. Also information that was collected on the Internet is routinely lost or stolen. This situation has caused many potential users to refrain from using information society services, or even from using the Internet. For example a German poll[16] found earlier this year that 50% of the polled have "often" refrained from on-line orders because they did not want to provide personal information that was required. 40% of the 19 to 29 year olds say the same. 18% even say they never order anything on the Internet because they do not want to provide personal information. 12% of the 19 to 29 year olds confirmed this.

The collection of unnecessary personal information on the Internet thus constitutes an **obstacle to economic development and employment in Europe**. Looking for short-term profits, companies are often ignoring that their user screening practises are eroding consumer trust and thus the basis of their long-term success. Internet services could be provided with little or no personal data needing to be disclosed. For example anonymous payment can be made on-line by using pre-paid micropayment cards.

For those reasons it is **necessary to establish strict sector-specific privacy rules for information society services**:

1. **The provider of an information society service shall offer the user anonymous use and payment of information society services to the extent technically feasible and reasonable**. The provider shall offer the user anonymous use and payment of its services in particular where services of this kind are already being offered anonymously by competitors. The user shall be informed about these options.

15 http://www.article19.org/pdfs/igo-documents/three-mandates-dec-2005.pdf.
16 Allensbach study in August of 2010, http://www.webcitation.org/5t9uDMnHb.

2. **The provider of an information society service may collect, process and use personal data concerning the use of of an information society services only to the extent necessary to enable the user to use the information society service** (transactional data) or to charge the user for the use of the information society service.
3. **The provider shall ensure that personal data generated in connection with the process of using information society services are erased or rendered anonymous as soon as possible**, at the latest upon the end of each utilization, unless further storage is required for billing purposes.
4. **The provider may not make the provision of an information society service dependent on the supply of personal data that are not necessary** for the provision of the service.
5. **The provider must not make the provision of an information society service dependent on the consent of the data subject to the processing or use of their data for other purposes** than the provision of the service.
6. **Directive 93/13 of 5 April 1993 on unfair terms in consumer contracts should be extended to cover unfair consenting clauses** concerning personal data.
7. **The provider must inform the user about the periods of time for which personal data is typically retained**.

Recommendation:

- **The e-commerce directive should be amended to include strict sector-specific privacy rules for information society services.**

E. Non-discrimination

Users that exercise data protection rights and attempt to end illegal data collection and illegal data processing practises are often **silenced by terminating their contact** or account. This way providers can avoid having to comply with privacy laws.

This situation has **devastating effects** not only on the user whose account was closed, but for all other users of that service whose rights cannot be enforced and also for competitors that respect privacy laws and are unfairly disadvantaged.

Recommendation:

- **Discrimination against users that legally exercise data protection rights must be prohibited**. The e-commerce directive should be amended to this effect.

F. Confidentiality of Internet use

The confidentiality of our Internet use must be protected not only by the access provider, but also by providers of information society services. The e-commerce directive should be amended to include a similar provision to article 5 of directive 2002/58/EC.

Recommendation:

- The e-commerce directive should be amended as follows: "*Member States shall ensure the confidentiality of the usage of information society services and the related transactional and subscriber data, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of usage and the related traffic and subscriber data by persons other than users, without the consent of the users concerned, except when legally authorised to do so. This paragraph shall not prevent technical storage which is necessary for the provision of a service without prejudice to the principle of confidentiality.*"

G. Question 52: interpretation of the provisions on liability

Overall, have you had any difficulties with the interpretation of the provisions on the liability of the intermediary service providers? If so, which?

According to articles 12-14 ECD, these liability limitations do not affect the possibility for a court or administrative authority of requiring the service provider to prevent "an infringement". **It is unclear what is meant by "an infringement".** Apparently the legislator is referring to a specific infringement and not to any infringement of a kind. But what means can the provider be required to employ to "prevent an infringement"? Can ineffective measures be required that can easily be circumvented?

According to article 15 ECD, this provision does not prevent Member States from imposing a monitoring obligation on service providers "in a specific case" or from imposing "duties of care [...] in order to detect and prevent certain types of illegal activities". **It is unclear what is meant by a "specific case" and by "certain types of illegal activities".** How "specific" does a monitoring duty need to be? Can it extend to all users, to all content and to an unlimited period of time without being considered a "general obligation" in the sense of article 15 (1) ECD? It is also unclear what means the provider can be required to employ in order to "detect and prevent certain types of illegal activities". Can ineffective measures be required that can easily be circumvented? Can measures be required that have severe side-effects on legal use, user privacy and free speech? Can measures be required that are unthinkable for similar off-line services, simply because they are technically feasible on-line?

All in all **the idea of private policing and infringement detection should be abandoned** as explained above.

H. Question 53: “voluntary” efforts to detect illegal activities

Have you had any difficulties with the interpretation of the term “actual knowledge” in Articles 13(1)(e) and 14(1)(a) with respect to the removal of problematic information? Are you aware of any situations where this criterion has proved counter-productive for providers voluntarily making efforts to detect illegal activities?

The interpretation of the term “actual knowledge” is controversial because it is **unclear whether knowledge of the illegal nature of the content is required**. If a provider is notified of allegedly illegal content, it often has no knowledge of whether that content is legal or not. For this reason a court should always decide on the matter as explained above.

The knowledge criterion **does not prove counter-productive** for providers voluntarily making efforts to detect illegal activities, because those practises can be regulated in the provider's terms of service. Obviously those contract terms must be subject to a fairness test according to directive 93/13.

In my opinion, **private efforts to detect illegal activities should not be facilitated** but, to the contrary, made compliant with the rule of law. The removal of content without the consent of its author should be banned unless ordered by the judiciary, after hearing the user. The law may provide for interim orders issued by the judiciary. Those orders should expire if not confirmed in the ordinary procedure after a certain period of time. Providers must not be allowed to remove content in their own right because this has proven to have disastrous effects on the freedom of speech.

I quote the Joint Declaration of the **OSCE Representative on Freedom of the Media** and Reporters Sans Frontières on Guaranteeing Media Freedom on the Internet:[17]

> *“A decision on whether a website is legal or illegal can only be taken by a judge, not by a service provider. Such proceedings should guarantee transparency, accountability and the right to appeal.”*

I also quote the Joint Declaration on International Mechanisms for Promoting Freedom of Expression of the **UN Special Rapporteur on Freedom of Opinion** and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression:[18]

> *“No one should be liable for content on the Internet of which they are not the author, unless they have either adopted that content as their own or refused to obey a court order to remove that content.”*

17 https://www.osce.org/documents/rfm/2005/06/15239_en.pdf .
18 http://www.article19.org/pdfs/igo-documents/three-mandates-dec-2005.pdf.

I. Question 57: practices other than notice and take down

Do practices other than notice and take down appear to be more effective? ("notice and stay down", "notice and notice", etc)

I regret the fact that this question exclusively aims at "effectiveness". **Proportionality and fundamental rights must be the point of departure** when considering the procedure for the removal of content.

J. Question 58: general monitoring or filtering obligations

Are you aware of cases where national authorities or legal bodies have imposed general monitoring or filtering obligations?

German courts are imposing general monitoring or filtering obligations all the time. In order to detect potentially illegal content of a kind (e.g. Rolex imitations), they require providers, for example, to force all users to register and to prove their identity. Courts have required providers to log all user actions, to filter all user-generated content for keywords, to manually review all content generated by certain users or relating to certain topics. These requirements are far-reaching enough to make providers delete any remotely suspicious content or account, or even to move to a country outside the EU.

K. Question 59: filtering

From a technical and technological point of view, are you aware of effective specific filtering methods? Do you think that it is possible to establish specific filtering?

Filtering is not effective. The various methods such as checksums, keywords, manual review, user identity or examining external links have all been discussed in detail and rejected.[19] If rights holders believe filtering to be effective they are free to search the Internet and use such technology themselves in order to give notice to the provider of any infringement. Policing and the enforcement of private titles is not the job of intermediaries, but of the rights holder, the police and courts. Intermediaries must be neutral where conflicting interests are colliding.

19 Breyer, http://www.daten-speicherung.de/index.php/verkehrssicherungspflichten-von-internetdiensten-im-lichte-der-grundrechte/.

L. Question 60: technical standards for filtering

Do you think that the introduction of technical standards for filtering would make a useful contribution to combating counterfeiting and piracy, or could it, on the contrary make matters worse?

The introduction of technical standards for filtering or even of filtering at all would be a catastrophe from a freedom of speech point of view. Instead **filtering should be prohibited.**

I quote the Joint Declaration of the **OSCE Representative on Freedom of the Media** and Reporters Sans Frontières on Guaranteeing Media Freedom on the Internet:[20]

> *"In a democratic and open society it is up to the citizens to decide what they wish to access and view on the Internet. Filtering or rating of online content by governments is unacceptable. Filters should only be installed by Internet users themselves. Any policy of filtering, be it at a national or local level, conflicts with the principle of free flow of information."*

I quote the Joint Declaration on International Mechanisms for Promoting Freedom of Expression of the **UN Special Rapporteur on Freedom of Opinion and Expression**, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression:[21]

> *"Filtering systems which are not end-user controlled – whether imposed by a government or commercial service provider – are a form of prior-censorship and cannot be justified."*

M. Question 62: liability for hyperlinks

What is your experience with the liability regimes for hyperlinks in the Member States?

The ECD liability exeptions are not being applied to hyperlinks by German courts. This has, for example, resulted in an on-line press publication being ordered to remove a hyperlink to the website of a manufacturer of software that can be used to circumvent copy protection technology, although the website can still be identified in seconds by using a search engine.

The liability exeptions should be extended to cover hyperlinks.

N. Question 63: liability for search engines

What is your experience of the liability regimes for search engines in the Member States?

The ECD liability exeptions are not being applied to applications for injunctive relief by German courts. The liability exeptions should be extended to outlaw prevention orders.

---

20 https://www.osce.org/documents/rfm/2005/06/15239_en.pdf.
21 http://www.article19.org/pdfs/igo-documents/three-mandates-dec-2005.pdf.

O. Question 64: liability for Web 2.0 services

Are you aware of specific problems with the application of the liability regime for Web 2.0 and "cloud computing"?

The operator of a weblog that allows for user comments or the operator of a wiki where users can post information should be considered hosting user-generated content. Yet is is unclear whether article 14 ECD covers these services. The article should be clarified or an amendment be inserted to make sure that user-generated content is covered by article 14.

P. Question 67: obligation to monitor

Do you think that the prohibition to impose a general obligation to monitor is challenged by the obligations placed by administrative or legal authorities to service providers, with the aim of preventing law infringements? If yes, why?

"Preventive duties" imposed by courts in specific cases violate article 15 of the e-commerce directive. Injunctions lead to a de facto obligation to monitor user-generated content, and thus amount to a general monitoring obligation. Service providers should not be obliged to prevent infractions at all. This in explained in more detail above.

Q. Question 69: investment in law enforcement with regard to the Internet

Do you think that a lack of investment in law enforcement with regard to the Internet is one reason for the counterfeiting and piracy problem? Please detail your answer.

I think that a "war on counterfeiting and piracy" cannot be won any more than the "war on drugs" that has been waged for decades. Illegal drugs today are available as easily and cheaply as never in the past today despite all efforts. The same applies to counterfeiting and copyright infringement. Beyond the traditional powers of law enforcement, all other measures to contain counterfeiting and copyright infringement cannot be demonstrated to effectively reduce these practices.

05/11/10