# SUBMISSION OF THE ELECTRONIC FRONTIER FOUNDATION ON THE CONSULTATION ON THE EU E-COMMERCE DIRECTIVE (2000/31/EC)

ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street, San Francisco, CA, 94114, USA
Tel: +1 415 436 9333 Fax: +1 415 436 9993
Web: www.eff.org Email: info@eff.org
Contact Person: Gwen Hinze, International Director, Email: gwen@eff.org

The Electronic Frontier Foundation (EFF) is grateful for the opportunity to provide our views to the Commission in its consultation on the eCommerce Directive (2000/31/EC). EFF is an international civil society non-governmental organization with more than 12,500 members worldwide, dedicated to the protection of citizens' online civil liberties, privacy, and freedom of expression. EFF engages in strategic litigation in the United States, and works in a range of international and national policy venues to promote balanced laws that foster innovation and empower consumers. EFF's primary office is located in San Francisco, in the United States of America, but EFF has members in more than 50 countries throughout the world. EFF currently has over 4,3000 members in the EU.

EFF wishes to address a number of questions asked by the Commission in relation to Issue 5, Internet intermediary liability.

## Issue 5: Interpretation of the provisions concerning intermediary liability in the Directive

### *Introduction*

EFF considers that limitations on liability for Internet intermediaries are necessary both for innovation and investment in Internet technology, and also for protection of citizens' fundamental rights, including the right to a private life and freedom of expression. The Internet is one of the most vibrant platforms for enhancing communication the world has seen since Gutenberg's press revolutionized the science of printing. The proliferation of user-generated content has democratized media, allowing any individual to reach out to a vast audience, without the constraints of traditional media. Blogs gain in importance and readership by the content and currency of their news, not their affiliations with the media of old. Through the social Internet, persons with diverse ideas can find online communities of like-minded individuals. Internet intermediaries host information on a vast array of subjects, from politics to health to financial matters to the ordinary issues of day-to-day life, allow people to pass on that information to others who share their interests, regardless of their geographic location. To maximize the economic, social and democratic potential of the Internet, we need policies and legal frameworks that enhance freedom of expression and privacy online.

Imposing liability on Internet intermediaries for the content of third party communications on their networks and platforms, however, provides the opposite incentives. Instead of promoting positive outcomes, it will encourage Internet intermediaries to take potentially overbroad action to reduce their exposure to potential liability, which will have detrimental consequences for citizens' fundamental rights and future Internet innovation. Internet intermediaries will be forced by fear of liability to monitor or surveil all communications passing through their networks and platforms, and will design their technologies to restrict their users from uploading certain sorts of content. This, in turn, will limit citizens' freedom of expression and violate their privacy.

Limitation of liability legal regimes were adopted in many countries around 2000, limiting liability of intermediaries for illegal or infringing content or behaviour by third parties, unless they have actual knowledge or constructive notice of specific infringing activity or content which they must then address. These regimes are now under a great deal of pressure through litigation, proposed legislative reform, and voluntary agreements between copyright rightsholders and Internet intermediaries. Recent efforts by rightsholders to increase Internet intermediary liability via multilateral agreement such as in previous leaked versions of the proposed Anti-Counterfeiting Trade Agreement (ACTA), and to impose new obligations on intermediaries to engage in ex-ante filtering or identification of potential copyright infringing content threaten EU citizens' fundamental rights, including the right to private life and freedom of expression under Articles 8 and 10 of the European Convention on Human Rights (ECHR).

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

EFF believes that the limitation on liability provisions in the eCommerce Directive have facilitated investment and innovation in Internet technologies and provided a sound basis for the development of e-commerce within Europe. The Directive has also created a framework that has, on the whole, protected the fundamental rights of European citizens.

We consider that the Directive generally strikes an appropriate balance between the interests of Internet intermediaries, intellectual property rightsholders, citizens and other stakeholders in the information society. However, we are aware of several areas of uncertainty about the application of the Directive.

In particular, we note that there is considerable uncertainty about:

- what constitutes "actual knowledge" for the purpose of Articles 13 and 14;
- the scope of application of Articles 12, 13 and 14 to newer Internet intermediaries such as search engines, link aggregators and online auction sites;

- the most appropriate approach for expeditiously removing or blocking content that is illegal or infringing while protecting citizens' fundamental rights of privacy and free expression; and
- the scope and legal basis for obtaining injunctive relief against Internet intermediaries, and how that comports with the prohibition against imposing a general obligation to monitor in Article 15.

While we do not consider that it is necessary to revise the Directive, we believe that it would be useful for the Commission to issue a clarificatory communication to Member States to provide greater legal certainty for all stakeholders in these areas of uncertainty.

In particular, we respectfully recommend that the Commission should:

- clarify the relevant standards on actual knowledge for the purpose of Articles 12 and 13;
- provide confirmation that newer Internet intermediaries that play a key role in communication and processing of information on the Internet, such as webhosting platforms, content aggregators and comparative shopping websites, online auction sites, and cloud computing providers should be eligible for protection as hosting providers under Article 14 if they otherwise meet its conditions;
- clarify that search engines should be treated as mere conduits, and with appropriate modifications, on the same conditions, and subject to the protections in Articles 12 and 13; and
- clarify the standards and limitations that national courts should consider in granting injunctions against Internet intermediaries.

***53. 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?***

***54. Have you had any difficulties with the interpretation of the term "expeditious" in Articles 13(1)(e) and 14(1)(b) with respect to the removal of problematic information?***

As the commissioned 2007 Study on the Liability of Internet Intermediaries by Thibault Verbiest, Prof. Dr. Gerald Spindler, Giovanni Maria Riccio, and Aurelie Van der Perre (the Study) documents clearly, the absence of a definition of "actual knowledge" in the directive has resulted in significant differences in EU Member States' national legislation and court practices on the interpretation of that term and the standards to be applied in the context of civil and criminal liability[i]. As the study also notes, if Internet intermediaries are considered to have actual knowledge upon a "simple" notification, they will be more likely to take down content immediately without any consideration of the

legitimacy of the complaint, in order to avoid the possibility of being sued or prosecuted. This is likely to result in the takedown of lawful content, and have a damaging impact on citizens' freedom of expression.

***Recommendation***

To provide greater legal certainty and meaningful protection of citizens' fundamental rights, it would be beneficial for the Commission to issue a clarificatory communication that an Internet intermediary can only be considered to have "actual knowledge" for the purpose of Article 13 and 14 upon receipt of a court notification or order notifying the Internet intermediary of specific content that is illegal in nature.

***56. What practical experience do you have regarding the procedures for notice and take-down? Have they worked correctly? If not, why not, in your view?***

EFF has significant experience with the copyright notice and takedown regime established under the United States' Digital Millennium Copyright Act (DMCA). In particular, our organization has brought numerous legal cases under the DMCA's user-protection provisions[ii]. The DMCA and the eCommerce Directive differ in several key respects. The DMCA notice and takedown regime includes several procedural safeguards that were intended to protect against removal of citizens' lawful and non copyright-infringing expression: first, it permits Internet users whose content has been blocked or taken offline by an Internet intermediary in response to a copyright takedown notice to issue a counternotice, which allows the Internet intermediary to put the content back without facing liability unless and until the copyright owner files a lawsuit in respect of the challenged content[iii]; second, section 512(f) of the DMCA allows Internet users whose content has been wrongfully removed on the basis of a knowing material misrepresentation by a copyright holder to bring a lawsuit for financial compensation for content removed. These provisions have provided important protection for online freedom of speech in a series of cases in the US[iv], where intellectual property rightsholders have claimed that they do not have to consider fair use or other applicable copyright exceptions before issuing a takedown notice[v].

However, despite these important procedural protections, the DMCA notice and takedown regime has resulted in the removal of significant amounts of lawful non-copyright infringing expression. Extra-judicial notice and takedown regimes are vulnerable to misuse for private party censorship. The DMCA framework has created a 'heckler's veto'; most Internet intermediaries are not able to bear the costs of hosting critical or unpopular content. Internet intermediaries are incentivized to remove content upon receipt of a notice alleging copyright infringement in order to get the benefit of the safe harbour, rather than to expend resources to investigate whether the complaint is legitimate or whether use of the content would be considered fair use and not copyright infringement under US law. Internet intermediaries often do not have the legal resources to review these notices and are not well placed to make determinations about the legality

of content. As a result, content can easily be taken down for a minimum of 14 days, even if the copyright complaint is baseless.

This has resulted in the removal of a significant amount of non-infringing user generated content, including parody videos. It has also created incentives for misuse of the takedown process to suppress competition and political expression at critical times. A 2006 study of DMCA takedown notices found that 57% of search index takedown notices received by Google were from business competitors. There have been several well-documented instances of misuse to silence critics and political expression. Several weeks before the 2008 US Presidential election, political campaign advertisements for both the McCain and Obama campaigns were taken down from YouTube for 14 days after media companies CBS, Fox News, and NBC networks sent takedown notices for 10 second news clips included in the advertisements[vi].

The risk that extra-judicial takedown notices will harm citizens' fundamental rights is heightened by the increasing volume of notices sent in recent years. While no comprehensive figures exist, evidence suggests the number of notices being sent are increasing exponentially in countries across the world as automated search detection and notification systems are adopted. Accordingly, it would be prudent for the Commission to take this trend into account in its consideration. In the US, Viacom sent 100,000 notices to YouTube on one day[vii]; the Chilling Effects project is currently receiving about 300-400 takedown notices per week for links on Google Search and Blogger, and in 2009 the International Federation of Phonographic Industries sent nearly 400 initial notices, requesting the removal of more than 108,000 unique URLs on more than 25,000 music blogs that discuss and link to pieces of music, and about 300 follow-up notices alleging repeat infringements and requesting removal of links to over 32,000 URLs[viii].

The problems with a notice and takedown regime are magnified when the allegation is a tort, such as defamation. A notice and takedown regime allows for a 'heckler's veto' of free expression. For example, imagine a citizen accuses a political candidate of taking bribes in a comment hosted by an Internet intermediary. If true, this is critical information for the electorate. If false, it would be defamatory. Under a notice and takedown regime, the intermediary is in no position to assess the truth or falsity, and would have no choice but to remove what could be very important speech from the Internet. To protect freedom of expression and promote innovation, the United States enacted Section 230 of the Communications Decency Act to protect intermediaries from claims arising from the actions of their users. This statute does not require the ISP to takedown material after notice, keeping responsibility for posted material with the author. This system has been instrumental in fostering the growth of Internet services in the United States, and provides strong protection for Internet users' fundamental rights of expression and privacy.

*Recommendations*

- **Separate Copyright Policy from Tort Policy.** Online copyright issues present fundamentally different problems and solutions from tort issues. Proposals like automated filters simply make no sense for torts (there can be no filter that determines if a statement is true or defamatory). Copyright infringement allegations allow for a side-by-side comparison of the alleged infringement and the original, as well as a fair use analysis based on the comparison and the context. Alleged torts often require a deeper analysis and often facts that require further investigation and evidence. Notice and takedown regimes for claims arising from speech activities allow for worrisome opportunities for mischief designed to suppress freedom of expression. For alleged torts, we recommend a system like Section 230 of the U.S. Communications Decency Act.

- **Judicial Adjudication:** In light of the experience with the US notice and takedown regime, a system that requires, at a minimum, judicial adjudication of requests prior to taking down alleged copyright-infringing or tortuous material will provide greater protection for Internet users' fundamental rights of expression, due process and privacy than a notice and takedown regime.

- **Actual Knowledge Only Upon Receipt of Court Order or Notification:** an Internet intermediary should only be considered to have "actual knowledge" for the purposes of Articles 13 and 14 upon receipt of a court order or notification, after a process of judicial review of the takedown request and upon a prima facie showing by the copyright holder that the challenged content is copyright infringing. We respectfully recommend that this could best be done by the Commission issuing a clarificatory communication on this point.

- **Establish Expeditious Judicial Review Mechanisms in National Regimes:** Internet intermediaries are not well placed to make determinations about the legality of content and requiring them to do so on the basis of private party extra-judicial notices raises significant concerns for transparency and citizens' due process and expression rights. The risk of lawful content being removed inappropriately is magnified by the requirement for Internet intermediaries to act expeditiously on receipt of a notice, even where it is unclear if the content is copyright infringing. To address this, we respectfully suggest that the Commission should recommend that Member States establish processes for timely preliminary judicial review of challenged content in their national laws.

- **Procedural Protections and Penalties for Misuse and Abuse:** If the Commission chooses not to adopt the preceding recommendations and recommends adoption of a notice and takedown approach, the Commission should: (a) require complainants to issue a formal notification, under oath or equivalent level of seriousness, which identifies with precision the allegedly infringing or illegal content that the

complainant wishes blocked or removed; and (b) make Member States aware of the benefits of providing additional procedural protections for citizens' fundamental rights in their national laws, including a strong counternotice and put-back mechanism, and a powerful deterrent against misuse of the takedown process, such as penalties for misrepresentation, and a timely judicial process for obtaining legal redress.

- **Evaluate the Empirical Evidence on the Impact of Takedown Notices on European Citizens' Fundamental Rights:** We recommend that the Commission undertake or commission a study to gather empirical evidence and evaluate the impact of takedown notices issued on citizens' fundamental rights of expression, due process and right to private life and correspondence.

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

We believe that the most effective practices are those we have listed in the recommendations, above. However, we note that the available evidence suggests that notice-notice or notice forwarding regimes are effective at curbing copyright infringement. In 2008 several major U.S. Internet service providers entered into agreements with copyright holders in which they agreed to automatically forward notices from rightsholders alleging copyright infringement to their customers with the corresponding IP address. Verizon Communications reported that in its first year of operation, 70% of the notices it processed were for customers receiving their first notice of alleged infringement.[ix] In the UK in 2008, Virgin and five other ISPs voluntarily agreed to forward rightsholder notices of alleged infringement to their customers for a 10 week trial. A survey commissioned by UK media law firm Wiggin also reported that 70% of all people polled said they would cease sharing files if their ISP notified them that it had detected the practice[x].

However, a notice forwarding regime that requires Internet intermediaries to collect and process personal data, such as how many copyright notices have been received for customers at particular IP addresses, raise privacy and data protection concerns, as noted in the recent consultation on the proposed Code of Obligations under the UK Digital Enforcement Act[xi]. Notice and termination systems which require ISPs to forward notices and to terminate their subscribers' Internet access upon three repeat notices (otherwise described as graduated response/ three strikes regimes) raise concerns for citizens' fundamental rights of privacy, due process and freedom of expression, and bring up a number of broader public policy issues such as proportionality of measures. As the European Data Protection Supervisor recently recognized in his opinion on such regimes in the context of the proposed Anti-Counterfeiting Treaty Agreement:

> *"Although the EDPS acknowledges the importance of enforcing intellectual property rights, he takes the view that a three strikes Internet disconnection policy as currently known — involving certain elements of general application —*

*constitutes a disproportionate measure and can therefore not be considered as a necessary measure. The EDPS is furthermore convinced that alternative, less intrusive solutions exist or that the envisaged policies can be performed in a less intrusive manner or with a more limited scope*."

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

***67. 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?***

At the time when the eCommerce Directive and the US DMCA limitation of liability regimes were adopted there was a clear understanding and trans-atlantic agreement by policymakers on two fundamental principles that should apply to regulation of Internet intermediaries: first, it was agreed that Internet service providers should not have liability where they act as mere conduits, transmitting packets across the Internet, with no selection or editorial control over the content transmitted. To hold otherwise, would have opened the door to unbounded liability for all Internet intermediaries, impeding investment and innovation on the fledgling network. Second, Internet intermediaries should not be required to monitor communications on their networks or to actively search for evidence of infringement. This principle was necessary to protect citizens' fundamental right to privacy and data protection, a human right that is foundational to the rights of freedom of expression and association, and which is enshrined in the International Covenant on Civil and Political Rights, the European Convention on Human Rights, and the Charter of Fundamental Rights of the European Union. From a business and policy point of view, it was also necessary to ensure the workability of the safe harbors and limitations on liability; in order to get the safe harbor, ISPs would not be required to take action that could lead them to obtain the very knowledge that would disqualify them from enjoying the benefit of the safe harbor or limitation. It is for this reason that the prohibition against imposing a general obligation to monitor is incorporated in Article 15 of the eCommerce Directive, in section 512(m) of the US Copyright Act, and in the limitation of liability regimes in many other countries' laws.

Although Article 15 contains a prohibition against imposing a general obligation on service providers to monitor the information which they transmit or store, and against actively seek facts or circumstances indicating illegal activity, as Recital (47) provides, Member States are not precluded from imposing monitoring obligations in a specific case, and in accordance with Recital (48) Member States can impose duties of care on hosting service providers to detect and prevent certain types of illegal activity. If construed broadly, there is a risk that such duties of care could be used by administrative or legal authorities to impose new obligations on Internet intermediaries to pro-actively search for potential copyright-infringing material on their networks and platforms on an ex ante basis, which would undermine the foundational principle contained in Article 15, and cause significant harm to citizens' fundamental rights and the free flow of information on the Internet. In particular, if new ex ante monitoring obligations are

imposed on Internet intermediaries that require them to use Deep Packet Inspection to identify potential copyright-infringing material, this would violate the privacy rights of all Internet users, not just those who may be engaged in copyright infringing activity.

As the Study notes, most EU Member States have implemented the exceptions in Articles 12(3), 13(2), and 14(3) permitting courts or administrative authorities to grant injunctions against Internet intermediaries to terminate or prevent infringements in accordance with their national laws, although the Study authors note that the case law described in the Study dealing with the national implementations of those provisions have restricted exceptions to civil liability for damages or criminal responsibility, and excluded injunctions. But the relationship between Article 15's prohibition against a general obligation to monitor, and the injunctions that can be granted by national courts in relation to copyright enforcement are very much a live issue because Member States have obligations under Article 8(3) of the Information Society Directive (2001/29/EC) and Article 11 of the IPR Enforcement Directive (2004/48/EC) to ensure that rightsholders are in a position to apply for injunctions against intermediaries whose services are being used to infringe copyright. However, while the obligation to make available injunctions is clear, the legal basis on which they may be obtained is not, and varies across EU Member States. And, as the Article 29 Working Party noted in its Working Paper on Data Protection Issues with regard to Intellectual Property of 18 January 2005, an injunction that directed an Internet intermediary to engage in wide-scale, generalized filtering could raise data protection concerns[xii].

Taken together, these provisions leave open the possibility that copyright rightsholders could seek injunctions against Internet intermediaries, or press for judicial interpretations of duties of care of webhosters that will effectively constitute general monitoring obligations, and potentially render meaningless the foundational principle in Article 15. This appears to have been borne out in recent judicial cases, in copyright holders' advocacy with legislative and administrative authorities[xiii], and in international intellectual property enforcement agreements such as the proposed Anti-counterfeiting Trade Agreement[xiv]. There is a clear and observable trend to impose obligations on Internet intermediaries to engage in ex ante filtering for potential copyright infringing material on their networks and platforms, which could undermine the foundational principle in Article 15[xv].

***Cases:***

In 2007 in the case of SABAM v. Tiscali (Scarlet), a Belgian court ordered Belgian ISP Tiscali (now Scarlet) to install filtering software to monitor all live-time communications on its network to detect and block the transmission of copyrighted works through peer-to-peer networks. Although the order could be said to be limited to the detection and blocking of only certain sorts of works, the order would require filtering of all Scarlet customers' Internet communications, and so could not be considered "specific". We note that the provider of the technology that was chosen to be used for this purpose, Audible Magic, has apparently subsequently withdrawn its technology on the grounds that it is not feasible for filtering that volume of communications. We understand that this case was

referred to the European Court of Justice in January 2010 and that the ECJ has been asked to answer whether imposing such a filtering order on an ISP is consistent with Article 15, and if so, whether relevant EU directives require national courts to consider the principle of proportionality when asked to rule on the efficacy and dissuasive effect of the requested measure.[xvi]

We are aware of a second case that has been referred to the European Court of Justice involving a request by Belgian rightsholder organization SABAM for a similar order for ISP filtering directed to social media website Netlog. We understand that it was apparently referred to the European Court of Justice in August 2010 after the Belgian court rejected SABAM's request.[xvii]

We understand that four recorded music companies in the Irish Recorded Music Association sought a similar filtering order in a lawsuit against Irish ISP Eircom, which was subsequently settled on terms requiring Eircom to phase in a three strikes or graduated response policy, where Eircom would automatically disconnect the Internet access of particular subscribers upon receiving three copyright infringement allegation notices from copyright holders.[xviii]

In relation to national courts' approaches to the granting of such injunctions, we are aware of inconsistent decisions in French and German national courts on the question of whether injunctions must comply with the principles of proportionality and subsidiarity[xix].

***Recommendations***

1. To ensure coherence with the foundational principle in Article 15 and to foster the public policy objectives it embodies, the Commission should issue a clarificatory communication confirming that injunctions granted by national courts should be subject to clear limitations, including:
    a. The relief requested must comply with the requirements of proportionality and subsidiarity;
    b. The relief requested must be appropriate and strictly necessary to prevent further damage caused by specific instances of unlawful information.
    c. The relief must not have the effect of rendering meaningless the relevant limitation on liability in practice.

***Public Policies Promoted by No General Obligation to Monitor Principle***

Finally, we wish to provide several insights on the public policy value of the foundational no general obligation to monitor principle from our experience with the similar provision in United States' law. Section 512(m)(1) of the US Copyright Act (17 U.S.C. § 512(m)(1)) makes it very clear that a service provider need not monitor its service or affirmatively seek facts indicating copyright-infringing activity in order to benefit from the safe harbors[xx]. This limitation has benefited Internet users, service providers and copyright owners. It has fostered the growth of the Internet as a vehicle for free speech

and commerce by helping provide legal certainty for service providers; without it, general information that some infringement was occurring might be interpreted to impose an obligation on service providers to devote considerable resources to finding and stamping out infringement. This would effectively shift the burden of copyright enforcement from the copyright owner, who has traditionally undertaken it and is best positioned to do so, to the service providers. Many innovative services would not exist today if they were saddled with that burden. Moreover, investigation and monitoring is likely to lead ISPs to over-block in order to avoid any possibility of litigation, which means lawful content will inevitably be taken down.

At the same time, service providers have strong market incentives to voluntarily develop better technologies to detect and prevent copyright infringements on their web sites. While the DMCA safe harbors provide an important baseline of legal protections and fairly clear rules for fledgling service providers, they do not guarantee service providers reliable access to big-budget entertainment content. The DMCA safe harbors, and particularly the clear statement in the DMCA that ISPs need not investigate, gives online service providers a business incentive to police for copyright infringement as part of voluntary commercial arrangements struck with major content owners in exchange for authorized access to their content. For instance, YouTube has devoted substantial efforts to such new acoustic and video fingerprint filtering technologies through its "Content ID" system. Other service providers have also agreed to implement new technologies on a voluntary basis to limit intellectual property infringements[xxi]. If the law penalized service providers for undertaking these efforts, (for instance by treating the adoption of such arrangements as implying knowledge for the purpose of secondary liability or by imposing a requirement to investigate), these developments might never have occurred. Thus, a clear prohibition against a general obligation to monitor actually fosters opportunities and provides incentives for copyright policing by service providers, rather than hampering it.

***59. 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?***

The evaluation of the effectiveness and specificity of filtering methods depends on the technological context in which they are deployed. From the technological perspective, there is a clear distinction between three different types of filtering mechanisms, each of which requires separate analysis:

1. Filtering mechanisms for network requests, such as HTTP requests to websites (Network-level filtering);
2. Filtering mechanisms for specific content types hosted on *video-specific* or *audio-specific* file hosting services; and
3. Filtering mechanisms for file hosting services that are not content-specific.

***Network-Level Filtering of Web Traffic***

We are not aware of any effective, specific filtering mechanisms for network requests. As a matter of technology, all methods for filtering traffic on the Internet will either not be specific, or will not be effective, or both. They will not be specific because they are likely to impact significant amount of lawful, non-copyright infringing content. At the same time, network-level filtering methods will not be effective because they will be unable to filter large amounts of infringing content.

There are three possible points in the Internet infrastructure at which network filtering could be attempted: (a) through the Domain Name system (DNS); (b) via IP addresses; and (c) at the level of TCP/HTTP connections; or through some combination of these.

DNS-based filtering methods are either non-specific or ineffective. Filtering via the DNS system requires a decision to filter or not-filter each entire domain in the World Wide Web (e.g. www.nytimes.com or www.dropbox.com ). If a domain contains a combination of copyright-infringing and non-infringing material, both categories must be treated in the same way. Non-infringing content may be blocked if the domain it is hosted on is subject to DNS filtering. Accordingly, DNS filtering is not specific.

At the same time, DNS filtering is not effective at blocking all copyright-infringing content on the Internet because it has no impact on communication mechanisms that do not use the domain name system, such as BitTorrent and other peer-to-peer protocols, and numerous other Internet communications channels that could be used to transmit copyrighted materials, such as chatrooms and instant messaging networks.

IP address-based filtering methods are also non-specific and/or ineffective. Since "virtual hosting" has become a widespread (and in many places, the standard) method for operating websites, a single IP address is typically shared by many domains. As a result, technological interdiction of connections to an IP address will frequently take not just an entire domain offline, but would block other, unrelated websites as well. Like DNS-based filtering methods, IP address filtering methods are incapable of affecting communication mechanisms that do not have a static client-server architecture, including P2P protocols and "darknet" systems[xxii],[1] without causing significant and broad-scale collateral damage.

The most specific method of filtering is to use a proxy or similar technology to examine the content of the TCP/HTTP connection itself and determine if the particular requested file is to be blocked. While this filtering method operates more specifically[xxiii], it is also ineffective because it can be defeated by encryption or other obscuring data transformation. Although a proxy can impersonate the true server by means of a "man in the middle" attack on encrypted protocols like HTTPS, performing this attack can be expensive and legally problematic. At the same time, it would still not be able to filter content that was encrypted or otherwise obscured separately from HTTPS.

***Content-specific filtering mechanisms for file-hosting websites***

Some audio and video hosting websites and platforms such as Google's YouTube and Veoh have voluntarily adopted mechanisms to filter content submitted for posting to these platforms against a database of acoustic and video fingerprints provided to hosting platforms by intellectual property rightsholders, with the goal of identifying files containing copyrighted audio or video material.

While it is feasible for hosting providers who work with specific media types to identify copyrighted material included in the database through this type of filtering of stored content, this type of filtering is not "effective" or "specific" because it cannot distinguish between infringing and lawful non-infringing uses of copyrighted works (for instance, that would be considered to be fair use and not copyright infringement under U.S. law) and cannot identify works that might be considered defamatory by their subjects. These systems may therefore result in the over-blocking of lawful, non copyright-infringing material, and the under-blocking of potentially defamatory or other material that would raise potential liability concerns for platform hosters. Accordingly, these types of systems cannot be considered "effective" for those reasons.

Although the identification of copyrighted material through this form of filtering is more targeted than the other methods described above, it is still not "specific" and raises serious policy issues about transparency, and the long-term impact of metered use delivered through such filtering techniques on fair use and other copyright exceptions and limitations that have previously allowed Internet users to lawfully create transformative creative works, parodies, and other types of user generated content that are at the very core of free expression. For instance, in January 2009, numerous user generated videos disappeared from YouTube after negotiations to renew the licensing agreement between YouTube and Warner Music Group broke down. Without warning, the ContentID's automatic blocking function took offline many YouTube videos that had been available for some time with the permission of Warner Music Group, including a presentation on fair use and remix culture by US Law Professor Larry Lessig that used a few seconds of music, and a Canadian's a capella tribute to John Williams' "Star Wars" theme song[xxiv].

EFF has received numerous complaints from YouTube users who have had their videos removed from YouTube. Many of these involved transformative uses of musical and video works that would have been considered non-copyright infringing fair use under US law, or protected under copyright exceptions and limitations in EU Member States' copyright law[xxv]. Requiring all content hosting platforms to adopt these types of filtering technologies would endanger the future of important kinds of online expression, including parodies, remixes and collage art.

Finally, mandating all web-hosting sites to create and/or use filtering technologies like ContentID would impede innovation and competition in the emerging web platform sector. Only incumbents and well-established entities will be able to afford the infrastructure and R&D costs necessary to deploy a system like ContentID. Google has

been able to build the "ContentID" fingerprinting system into the YouTube infrastructure because YouTube has extensive infrastructure for processing all of the video content that it hosts. While Google is able to absorb the costs of negotiating with all of the copyright industries to obtain a database of the acoustic and video fingerprints of the relevant copyrighted works and has sufficient market presence to be able to negotiate reasonable licenses permitting ongoing use and monetization of flagged copyrighted material in UGC uploaded to its platform, even it has had difficulty doing so, and the same options won't be available to start-ups and emerging technology platforms. Many of YouTube's innovative but smaller competitors, which comply with the US copyright law's notice-and-takedown regime, would be put out of business if required to develop and implement ex ante filtering technologies.

***Non content-specific filtering methods by data hosting sites***

We are not aware of any effective specific filtering mechanisms for general-purpose data hosting websites and services, such as www.dropbox.com, www.yousendit.com, www.ifile.it, or www.filesanywhere.com. Since the files uploaded to these services can be in any format, (for instance, ZIP and RAR archives, encrypted PGP files, or audio and video encodings that are not understood and processed by the service provider), in most cases it will be impossible for the hosting service to know what kind of data is contained in any given upload, let alone whether that data contains an infringing copyright work.

***60. 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?***

EFF opposes the imposition of obligations on Internet intermediaries to use technical measures, including filtering, to address online copyright infringement because they are ineffective for their intended purpose, but at the same time are frequently over-board and raise significant concerns for the privacy and expression rights of all Internet users. We are therefore very troubled by the tone of this question and the preceding one, which appear to suggest that the Commission is considering policy measures which are likely to cause considerable harm to citizens' rights and the free flow of information on the Internet

Filtering methods are either ineffective, or over-broad and non-specific, or both, for the reasons outlined in response to the previous question. We note that the authors of the Study have recommended "a mixed co-regulatory model, making reference to the model in Article 13, and referring to industry standards", so that "only where filtering techniques according to those standards were available could providers be ordered to filter and block similar infringements"[xxvi] We do not believe that the development of such standards for filtering technologies via standardization committees or standard setting organizations will address the concerns documented in our response to question 59, above. We also note that developing standards for filtering in cases of alleged defamatory speech does not

make sense from a technological point of view. Standards for filtering that are ineffective and under-protective will have little effect on copyright infringement, because Internet users will quickly migrate to communications channels and methods that are unfilterable. For instance, they are likely to switch from centrally hosted, video-specific services like Vimeo to P2P networks, private darknet sharing services, or more generic hosting sites that do not have the technical capability to know the content of the files hosted. Or, if the filtering occurs at the network level, Internet users will be likely to switch from an unencrypted, HTTP-based service to an encrypted, HTTPS-based one.

On the other hand, standards for filtering that are non-specific - those that censor entire domains by DNS or IP address, or those that take-down both infringing and transformative, non-infringing uses of works - are likely to have the effect of *increasing* piracy in the longer term. Filtering methods that harm legitimate, non-infringing online communications are only likely to strengthen the perception that copyright is overly restrictive and out-of-step with the normative expectations of consumers in modern digital life. Coupled with the fact that no filtering methods are capable of dealing with all of the available channels for infringing communication (see response to question 59), over-protective filtering standards are likely to drive users to the many readily available unfilterable communications channels, thus increasing the total volume of copyright infringement. In short, in a world with readily available darknets, filtering technologies that restrict the uses of content that consumers customarily expect to be able to make will not succeed in limiting copyright infringement, but will instead create incentives that will drive it.

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

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

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

***66. The Court of Justice of the European Union recently delivered an important judgement on the responsibility of intermediary service providers in the Google vs. LVMH case (Joined cases C-236/08 and C-238/08, Google vs. Louis Vuitton Malletier SA, judgement of 23 March 2010). Do you think that the concept of a "merely technical, automatic and passive nature" of information transmission by search engines or on-line platforms is sufficiently clear to be interpreted in a homogeneous way?***

***68. Do you think that the classification of technical activities in the information society, such as "hosting", "mere conduit" or "caching" is comprehensible, clear and consistent between Member States? Are you aware of cases where authorities***

***or stakeholders would categorise differently the same technical activity of an information society service?***

As recent caselaw demonstrates, and the Study also notes, the absence of a specific safe harbor or limitation in the eCommerce Directive for search engines, and the provision of links and location tools, has resulted in divergent court decisions across different countries' courts[xxvii]. In the absence of clear guidance from the Commission about the application of Articles 12, 13 and 14 to new types of hosting and information Internet intermediaries such as cloud computing services (such as those provided by Amazon and Google, SalesForce.com), auction websites, comparative shopping and aggregator sites, and search engines, it seems likely that national court decisions will continue to diverge. This is troubling because, as the Study notes, information location tools are one of the core elements of the Internet and modern communication networks, and serve the important social need of facilitating Internet use.[xxviii]As many of these Internet intermediaries – search engines in particular – play a key role in allowing Internet users to obtain access to knowledge, the lack of legal clarity is also likely to have a harmful impact on citizens' ability to seek and impart knowledge and engage in expression.

***Recommendations***

- To provide greater legal certainty for service providers and for the Internet users who rely on those services to find and impart information, the Commission should issue a clarificatory communication confirming the application of Articles 12, 13 and 14 to these newer types of Internet intermediaries.
- In particular, the Commission should issue a clarificatory communication confirming that:
    - **a.** search engines should be treated as mere conduits, and subject to the same conditions (with appropriate modifications reflecting the technical selection of content to be displayed) and level of protection in Articles 12 and 13, reflecting their limited level of control over, and awareness of, the content for which they are producing links in response to requests; and
    - **b.** newer Internet intermediaries that play a key role in communication and assist citizens to seek, receive, and impart information on the Internet, such as webhosting platforms, content aggregators and comparative shopping websites, online auction sites, and cloud computing providers, should be eligible for protection under Article 14 if they meet the conditions in that Article.

**Gwen Hinze**
**International Director, Electronic Frontier Foundation**
**5th November 2010**

[i] Study, at pp. 14, 34-47.

[ii] Online Policy Group v. Diebold, 337 F.Supp.2d 1195 (N D Cal 2004), the first case brought under 17 USC § 512(f); and Lenz v. Universal Music Group at: **http://www.eff.org/cases/lenz-v-universal**. For details of additional cases, please see: http://www.eff.org/issues/ip-and-free-speech.

[iii] 17 USC §512(g). We note that the DMCA safe harbour regime does not *require* Internet intermediaries to put back content in order to get the benefit of the safe harbour. To provide greater protection for citizens' freedom of expression, EFF, academic institutions and other prominent public interest organizations recommended mandatory put-back/ reinstatement after receipt of a valid counternotice in a set of Fair Use Principles for User Generated Content released in 2007. See: http://www.eff.org/issues/ip-and-free-speech/fair-use-principles-usergen

[iv] See cases described at: http://www.eff.org/issues/ip-and-free-speech.

[v] See Lenz v. Universal Music Group, note ii, supra.

[vi] Wendy Seltzer, Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment, Berkman Center Research Publication No. 2010-3, March 2010, at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1577785

[vii] Viacom International, Inc. et al. v. YouTube, Inc. et al., (SDNY, case no. 07 civ. 3582, Summary Judgment Order and Opinion of June 23, 2010) at: http://www.eff.org/files/filenode/viacom_v_youtube/06-23-10_Summary_Judgment.pdf

[viii] http://www.chillingeffects.org/weather.cgi?WeatherID=635

[ix] Comments of Verizon Communications in Coordination and Strategic Planning of the Federal Effort Against Intellectual Property Infringement: Request of the Intellectual Property Enforcement Coordinator for Public Comments Regarding the Joint Strategic Plan. Vol. 75 Fed. Register, Number 35, FR Doc. 2010-3539, March 24, 2010, at: http://www.whitehouse.gov/sites/default/files/omb/IPEC/frn_comments/VerizonCommunications.pdf.

[x] Nate Anderson, *Survey: warnings from ISPs could slash file-swapping by 70%,* ArsTechnica, March 3, 2008, at: http://arstechnica.com/old/content/2008/03/survey-warnings-from-isps-could-slash-file-swapping-by-70.ars

[xi] Ofcom, Online Infringement of Copyright and the Digital Economy Act 2010 – Consultation document on Draft Initial Obligations Code, at: http://stakeholders.ofcom.org.uk/binaries/consultations/copyright-infringement/summary/condoc.pdf

[xii] See WP 29 Working Document on Data Protection Issues Related to Intellectual Property Rights, WP 104, 18 January 2005, at p.7, at: http://www.dataprotection.gov.sk/buxus/docs/wp104_en.pdf

In considering Article 15 of the eCommerce Directive and Article 8 of 2004/48/EC on the processing of judicial data, the Article 29 Working Party found that:

*"As stated in article 8 of the Data protection Directive, processing of data related to offences, criminal convictions or security measures can be processed only under strict conditions as implemented by Member States. While any individual obviously has the right to process judicial data in the process of his/her own litigation, the principle does not go as far as permitting in depth investigation, collection and centralisation of personal data by third parties, including in particular, systematic research on a general scale such as the scanning of the Internet or the request of communication of personal data detained by other actors such as ISPs or controllers of Whois registries. Such investigation falls within the competence of judicial authorities."*

[xiii] For instance, an IFPI lobbyist memorandum circulated to European Parliament staffers in November 2007 called on the European Parliament to mandate that ISPs block communications using particular Internet protocols, install network-level filtering, and block access to websites that facilitate copyright infringement (see http://www.eff.org/files/filenode/effeurope/ifpi_filtering_memo.pdf); in December 2007, a proposed amendment to European Parliament's CULT committee report would have required ISPs to filter their networks and customer communications in order to find evidence of potential infringement.

[xiv] We note that some US intellectual property rightsholders in submissions to the Office of the United States Trade Representative on the proposed Anti-Counterfeiting Trade Agreement in March 2008 requested that ACTA include obligations for Internet Intermediaries to use filtering and technical measures. See, for example, RIAA comments, at: https://2974639497112273069-a-1802744773732722657-s-sites.googlegroups.com/site/iipenforcement/riaa-20080317.pdf?attachauth=ANoY7cqGYwmiQ7_XIBBDW4tVYh1lvzLQYNjiJ7TVi5c2OFVWA7Mb5H-_N4_BKtgu_6ikU8rd9X65a0gh4L55DO4cHgRhm-3RynxuLnIvx8AJrZlGq5xC34206DsegZBwVt8aoONRTDzgVdtlqvRKECo2N6gBPCGvxSOkOH3wbJ1ohjQYGmMJzpm4rEp6y9tucr2JEMuEk-NEYsPIBSw8vXQlt_3D4XOe-Q%3D%3D&attredirects=0

[xv] See Jeremy DeBeer and Christopher Clemmer, *Global Trends in Online Copyright Enforcement: A Non-Neutral Role for Network Intermediaries?,* Jurimetrics, Vol. 49, No. 4, 2009, at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1529722

[xvi] TJ McIntyre, SABAM v. Scarlet: Belgian ISP released from obligation to filter network for illegal downloads, IT Law in Ireland Blog, October 26, 2008, at: http://www.tjmcintyre.com/2008/10/sabam-v-scarlet-belgian-isp-released.html; Sabam v Tiscali goes to the ECJ on ISP Filtering, IPKat blog, February 11, 2010, at http://ipkitten.blogspot.com/2010/02/sabam-v-tiscali-goes-to-ecj-on-isp.html

[xvii] SABAM v. Netlog, ECJ Case Number C-360/10; *Another ECJ reference on monitoring and SABAM*, 1709 Blog, August 17, 2010, at: http://the1709blog.blogspot.com/2010/08/another-ecj-reference-on-monitoring-and.html

[xviii] Tim Healy, *Eircom may face music in illegal files row*, Independent (Ireland), March 11, 2008, at: http://www.independent.ie/national-news/eircom-may-face-music-in-illegal-files-row-1313154.html; *IRMA v. Eircom – Why ISP Filtering for the music industry is a bad idea,* Digital Rights Ireland Blog, March 11, 2008, at: http://www.digitalrights.ie/2008/03/11/irma-v-eircom-why-isp-filtering-for-the-music-

industry-is-a-bad-idea/; Danny O'Brien, *Irish ISP Agrees to Three Strikes Against Its Customers,* EFF Deeplinks blog, January 28, 2009, at: http://www.eff.org/deeplinks/2009/01/irish-isp-agrees-three-strikes-against-its-users

[xix] Study, page 50.

[xx] 17 U.S.C. § 512(m)(1)

[xxi] See Io Group, Inc. v. Veoh Network, Inc., 586 F. Supp. 2d at 1138 (defendant voluntarily implemented a "hash," or digital "fingerprint," technology to prevent infringements).

[xxii] A "darknet" is an encrypted system with a limited membership. They are inherently difficult to identify and shut down. The significance that these networks have in terms of limiting the feasibility of digital copyright enforcement was first recognized by researchers at Microsoft; *see* Peter Biddle, *et al, The Darknet and the Future of Content Distribution,* Proc. ACM Conference on Digital Rights Management, 2002, at: http://msl1.mit.edu/ESD10/docs/darknet5.pdf

[xxiii] The anti-child pornography blacklist run by the UK Internet Watch Foundation employs a hybrid of filtering types (a) and (c). It demonstrates that method (c) can be overbroad and non-specific; *see* Peter Eckersley, *Internet Censors Must Be Accountable for The Things They Break*, Electronic Frontier Foundation Deeplinks blog, December 9, 2008, describing how the Internet Watch Foundation's attempt to block a particular allegedly indecent image on a band album cover on a Wikipedia page had the unintended consequence of making the entire Wikipedia uneditable by anyone in Britain for a period of time, at: http://www.eff.org/deeplinks/2008/12/internet-censors-must-be-accountable-things-they-b.

[xxiv] Fred von Lohmann, *YouTube's January Fair Use Massacre*, EFF Deeplinks blog, February 3, 2009, at: http://www.eff.org/deeplinks/2009/01/youtubes-january-fair-use-massacre.

[xxv] Fred von Lohmann, *YouTube's Content ID (C)ensorship Problem Illustrated,* EFF Deeplinks Blog, March 2, 2010, at: http://www.eff.org/deeplinks/2010/03/youtubes-content-id-c-ensorship-problem

[xxvi] Study, pp. 22-23.

[xxvii] Study, p. 17.

[xxviii] Study, p. 17.