KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

SUPPLEMENTAL COMMENTS OF CDT REGARDING THE EUROPEAN COMMISSION PUBLIC CONSULTATION ON THE CIVIL ENFORCEMENT OF INTELLECTUAL PROPERTY RIGHTS

29 March 2013

These comments are intended to supplement CDT's answers to the Commission's survey. They address survey sections or questions for which the survey format did not provide CDT an opportunity to respond. The comments are organized according to the section of the survey to which they relate.

Impact of infringement

Questions 28–30 in section on background information

CDT would caution the Commission not to place too much emphasis on statistics purporting to quantify in specific numerical terms the overall impact of infringement on the economy or even individual parties. As a 2010 report by the U.S. Government Accountability Office concluded, methodologies for estimating economic impact all have limitations, and results are highly sensitive to assumptions.[1] In addition, parties commissioning studies also often have vested interests in the results. Finally, it is it is important to remember that the Internet and digital technologies can be highly disruptive of traditional business models for reasons having nothing to do with infringement. For example, the rise of the Internet may have enabled increased infringement of music recordings, but it also has enabled a shift to selling songs individually, new marketplace options like podcasts and music streaming services, and changing patterns in the way people consume and enjoy music. Although these changes may have harmed some incumbent music providers, the changes were the result of innovation and competition. With so much in flux, it is not easy to devise a controlled experiment to isolate the impact of infringement. In short, statistics in this area are likely to be less than reliable.

Right of information

CDT understands and appreciates the interest of rights holders in being able to identify suspected infringers. That interest, however, cannot be allowed to override the fundamental privacy rights of Internet users.

Internet users reasonably expect that their activities online can be anonymous or pseudonymous when they visit health information sites, make political

[1] US Government Accountability Office, Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods, April 2010, http://www.gao.gov/new.items/d10423.pdf.

statements, become online whistleblowers, or engage in many other private and personal communications.

Revealing the identities of Internet users can mean revealing users' health status, political beliefs, what they read, or with whom they socialise. It can chill legitimate free expression. For these reasons, it is appropriate to have significant restrictions on when service providers may be required to turn over user identities to the government or to private parties. Any process that makes it easy for private parties to unmask the identities of Internet users simply by claiming a possible IPR violation would open the door to mistakes, abuse, and ultimately significant privacy violations.

Any action in this area, therefore, would need to respect privacy law and to include careful safeguards for privacy and due process. Potential safeguards would include giving users advance notice of possible identity disclosure, so that they have the opportunity to object to inappropriate disclosures before they happen; penalties for parties that misuse the process to obtain information for inappropriate reasons; compensation to service providers for the cost of disclosure, to further discourage frivolous requests; limitations on how user information can be used and how long it can be retained; and reporting requirements and oversight to monitor any signs of problems or abuse.

Mechanisms to inform about the alleged infringement and to impede access to goods and services allegedly infringing IPRs

Question 7: Could notification mechanisms be a useful tool to inform the infringer/alleged infringer of the infringing/allegedly infringing character of his activity?

Informational efforts aimed at educating or warning users can sidestep many of the more serious concerns associated with actions taken by intermediaries. This is because purely educational measures can be structured to avoid directly impairing individual rights, even in cases where they are applied in a somewhat imprecise or overbroad manner. Receiving a warning notice need not significantly impair a user's speech or privacy rights. The key is for notification mechanisms to be educational in focus, not punitive.

There is a crucial role for education, because much of the challenge in reducing infringement lies in changing norms about what constitutes normal and appropriate behavior. Some Internet users lack sufficient understanding of their rights and responsibilities under copyright law; a recent Ofcom study, for example, found that forty-four percent of Internet users over 12 years old claimed to be either "not particularly confident" or "not confident at all" regarding what online behaviour is legal and what is not.[2] Other Internet users may believe that their online behaviour cannot be traced to them. Still others may be unaware of infringing behaviour by others using their account (such as a teenage child). In all of these cases, efforts to educate or warn users may have potential to change behavior and reduce infringement. It is important however, that educational notices or programs present a balanced view of copyright, including information on available defenses, limitations, and exceptions, so that they provide recipients with an accurate picture of what is and is not legal.

[2] Ofcom, Online copyright infringement tracker benchmark study, Q3 2012, http://stakeholders.ofcom.org.uk/market-data-research/other/telecoms-research/copyright-infringement-tracker/.

Questions 11 and 14, regarding whether notification mechanisms are mandatory for intermediaries and whether rights holders can use the notification mechanism to ask an intermediary to impede access to goods or services he considers to be infringing his IPRs

Intermediaries should not be required or expected to take punitive action, such as impeding access to goods or services or terminating subscriber accounts, upon receiving unadjudicated allegation of infringement.[3] Any such regime would be highly susceptible to mistakes and abuse, with serious negative consequences for free expression. It would enable virtually any party to silence speech or speakers that he or she does not like, simply by making an accusation.

Forcing intermediaries to assume new functions in actively policing their networks would undermine free expression in less direct ways as well. Policies protecting intermediaries from liability or "gatekeeping" responsibilities have been a tremendous success, driving investment in innovative services and communications networks.[4] Society benefits from these empowering technologies in the form of increased opportunities for expression, access to information, collaboration, civic engagement, and economic growth. Mandating new policing obligations would create new barriers to innovation and competition in communications offerings and force existing service providers to focus on gatekeeping and surveillance functions instead of investing in valuable new services.

Voluntary cooperation between right holders and intermediaries regarding IPR enforcement presents a more complex question. There are many types of intermediaries, and the roles they play relative to content dissemination and infringement can vary greatly. Broad legal mandates may therefore prove costly, technically infeasible, or ineffective in many contexts. Voluntary approaches, on the other hand, can be tailored to specific contexts and adjusted to changing circumstances.

This flexibility, however, carries risks. Voluntary, private action may be less transparent than government action, making it more difficult for affected parties to evaluate and respond reasonably to whatever actions are taken. In addition, there may be less obligation to follow fair procedures, including recourse for erroneous decisions.[5] There is less substantive protection for individual rights such as freedom of expression, association, or privacy. Finally, there is less accountability, since private actors are not subject to democratic checks and balances.

For all of these reasons, private voluntary enforcement may be susceptible to unfair or mistaken application – whether due to sloppiness, resource constraints, competitive motives, or outright abuse. The extent of this risk will vary depending on the type and details of the proposed voluntary action, but all must be approached with caution. Drawing the line between constructive private-sector action and risky vigilantism is a crucial challenge for any effort to address

[3] We note that the Commission has excluded content hosts and "notice and action" policies from this inquiry. See CDT's earlier comments in that proceeding for a detailed examination of those issues, https://www.cdt.org/blogs/andrew-mcdiarmid/1109shielding-messengers-notice-and-action.

[4] CDT, *Shielding the Messengers: Protecting Platforms for Expression and Innovation*, December 2012, https://www.cdt.org/paper/shielding-messengers-protecting-platforms-expression-and-innovation.

[5] *See* European Digital Rights, "The Slide from 'Self-Regulation' to Corporate Censorship: The Scale and Significance of Moves to Entrust Internet Intermediaries with a Cornerstone of Democracy – Open Electronic Communications Networks," Jan. 2011, http://www.edri.org/files/EDRI_selfreg_final_20110124.pdf at 5 (warning that private companies "cannot reasonably be expected to provide the same level of impartiality, transparency and due process" as traditional government regulatory and law enforcement processes).

infringement through voluntary action. At a minimum, it is essential that voluntary measures be developed through open processes that include civil society and other relevant stakeholders, and that strong procedural safeguards are included, such as the right to contest and appeal allegations of infringement.[6]

Injunctions imposed on intermediaries

In the present consultation, the Commission has set aside issues related to "notice and action" policies related to content hosts covered under Article 14 of the E-Commerce Directive, but it is not clear whether notices to other ECD intermediaries, namely "mere conduits" under Article 12, fall within the scope of the current inquiry. To the extent that questions regarding injunctions imposed on intermediaries are meant to include blocking orders served on conduit service providers, CDT offers the following comment.

Courts in several Member States have issued orders requiring conduits to block access to particular websites adjudicated to be infringing copyright.[7] Such blocking orders appear to be in tension with ECD Article 15's prohibition on placing general monitoring obligations on service providers, because implementing the orders requires monitoring *all* traffic in order to identify which particular traffic is going to or from the prohibited site.[8]

Moreover, blocking by conduits carries serious risks to free expression. Some implementations can be dramatically overbroad, inadvertently blocking more than just the intended site. Moreover, website blocking is a very blunt instrument. Rather than enabling targeted action against specific infringing content, it targets entire platforms, which may contain a mix of lawful and infringing content. Issuing blocking orders for such platforms – even those that may have come to be commonly used for infringement – can impair the ability of some users to access lawful material. Domain-name blocking in particular poses additional risks to the security and stability of the domain name system.[9]

There are also serious questions regarding the ultimate effectiveness of blocking by conduits. A 2010 study by the UK telecom regulator Ofcom noted that "[c]ircumvention of a block is technically a relatively trivial matter irrespective of which of the techniques used."[10]

---

[6] For more on voluntary measures, see CDT, *Shielding the Messengers*, *supra* note 4.

[7] *See, e.g., Twentieth C. Fox v. BT* (re: Newzbin2) judgment, 2011 EWHC 1981 (Ch), United Kingdom, http://www.bailii.org/ew/cases/EWHC/Ch/2011/1981.html; *Dramatico Entertainment v. British Sky Broadcasting et. al.* (re: The Pirate Bay) judgment, 2012 EWHC 268 (Ch), United Kingdom, http://www.bailii.org/ew/cases/EWHC/Ch/2012/268.html; *BREIN v. Ziggo and XS4all,* LJN: BV0549, District Court of The Hague, 374634 / HA ZA 10-3184, Netherlands, http://zoeken.rechtspraak.nl/detailpage.aspx?ljn=BV0549; Injunction against telecommunications firm "3", Court of Frederiksberg case FS 11-18685/2011, Denmark, http://www.domstol.dk/frederiksberg/nyheder/domsresumeer/Pages/Fogedforbudnedlagtoverforteleselskabet3.aspx

[8] *See* CDT, *Cases Wrestle with Role of Intermediaries in Fighting Copyright Infringement,* June 26, 2012, https://www.cdt.org/policy/cases-wrestle-role-online-intermediaries-fighting-copyright-infringement.

[9] *See* Steve Crocker et. al, *Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill*, May 2011, http://domainincite.com/docs/PROTECT-IP-Technical-Whitepaper-Final.pdf.

[10] Ofcom, *'Site Blocking' to reduce online copyright infringement*, August 3, 2011, http://stakeholders.ofcom.org.uk/binaries/internet/site-blocking.pdf.

Use of IPR enforcement measures for frivolous and/or anti-competitive purposes

In connection with this topic, it is important for the Commission to be aware that there is a long history in the United States of copyright enforcement mechanisms being used to attempt to stifle new and emerging technologies. Examples of technologies that have been targeted include VCRs, portable mp3 players, search engines for images, video-sharing websites, and more.[11] Thus, the experience in the United States shows that strong IPR enforcement policies in practice can be used not just to try to thwart true "bad actors," but also to try to slow down or gain control over the development of new information-related technologies. The risk of harm to technology innovation, and ultimately to the general public that enjoys the benefits of technology innovation, can be significant.

The point here is obviously not that IPR enforcement should be abandoned, but rather that it needs to be crafted in ways that narrowly target true "bad actors." Broad, vague, or excessively powerful enforcement mechanisms can be dangerous for innovation, growth, and users in the information technology sector.

[11] CDT described this history in greater detail in comments to the U.S. Department of Commerce in 2010. See https://www.cdt.org/files/pdfs/CDT%20Comments%20to%20NTIA%20Copyright%20Task%20Force.pdf.