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

ADDITIONAL RESPONSES REGARDING NOTICE-AND-ACTION

Comment regarding Glossary definition of "action"

The questionnaire defines "action" narrowly as "removing (taking down) or disabling access to illegal content," following the text of Article 14 of the ECD. There is a much wider range of actions, however, that can help address illegal content. For example, hosts or access providers could forward notices to their subscribers to alert them of the allegations and the possibility of legal action against them. Such "notice and notice" systems have been successful at deterring copyright violations, for example. In issuing guidance in this area, the Commission should consider a role for actions that stop short of content removal.

Detailed response to Questions 13, 14, and 21: Preventing unjustified notices and unjustified content removal

The consultation document appropriately notes the potential for lawful content to be taken down, either by mistake or due to abusive notices, under a notice-and-takedown system. Notice-and-action policies need to be carefully crafted to minimize mistakes or abuse that can impair the flow of legitimate expression. In many cases, the scale of intermediaries' operations and the volume of notices they receive give the intermediaries little opportunity to scrutinize notices, with the result that even unjustified notices are quickly honored.[1] CDT's preliminary submission to DG Internal Market and Services noted some of the research documenting abuse under the US DMCA.[2]

Because intermediaries often comply with notices automatically and without scrutiny, safeguards are necessary to discourage wrongful notices and to provide recourse in the case of mistakes or abuse. Safeguards should include:

- **Requiring detailed notices.** Setting a high standard for what constitutes valid notice will limit opportunities for abuse in the first place. Notices should include the following features:
  - **Specificity.** Notices should be required to specify the exact location of the material – such as a specific URL – in order to be valid. This is perhaps the most important

[1] Google recently testified that it had processed nearly 5 million copyright notices in 2011, the majority of which were processed within hours through the efforts of a large staff and technical compliance tools. *See* Testimony of Katherine Oyama, Copyright Counsel, Google Inc. Before the House of Representatives Committee on the Judiciary Hearing on H.R. 3261, the Stop Online Piracy Act, 16 November 2011, http://judiciary.house.gov/hearings/pdf/Oyama%2011162011.pdf.

[2] Comments of CDT to the DG Internal Market and Services Regarding Notice-and-Action Procedures by Internet Intermediaries, 29 February 2012, https://www.cdt.org/comments/comments-european-commission-notice-and-action.

requirement, in that it allows hosts to take targeted action against identified illegal material without having to engage in burdensome search or monitoring. Notices that demand the removal of particular content wherever it appears on a site without specifying any location(s) are not sufficiently precise to enable targeted action.

- **Description of alleged illegal content.** Notices should be required to include a detailed description of the specific content alleged to be illegal and to make specific reference to the law allegedly being violated. In the case of copyright, the notice should identify the specific work or works claimed to be infringed.
- **Contact details.** Notices should be required to contain contact information for the sender. This facilitates assessment of notices' validity, feedback to senders regarding invalid notices, sanctions for abusive notices, and communication or legal action between the sending party and the poster of the material in question.
- **Standing:** Notices should be issued only by or on behalf of the party harmed by the content. For copyright, this would be the rightsholder or an agent acting on the rightsholder's behalf. For child sexual abuse images, a suitable issuer of notice would be a law enforcement agency or a child abuse hotline with expertise in assessing such content. For terrorism content, only government agencies would have standing to submit notice.
- **Certification:** A sender of a notice should be required to attest under legal penalty to a good-faith belief that the content being complained of is in fact illegal; that the information contained in the notice is accurate; and, if applicable, that the sender either is the harmed party or is authorized to act on behalf of the harmed party. This kind of formal certification requirement signals to notice-senders that they should view misrepresentation or inaccuracies on notices as akin to making false or inaccurate statements to a court or administrative body.
- **Consideration of limitations, exceptions, and defenses:** Senders should be required to certify that they have considered in good faith whether any limitations, exceptions, or defenses apply to the material in question. This is particularly relevant for copyright and other areas of law in which exceptions are specifically described in law.

- **An effective appeal and counter-notice mechanism.** A notice-and-action regime should include counter-notice procedures so that content providers can contest mistaken and abusive notices and have their content reinstated if its removal was wrongful.
- **Penalties for unjustified notices.** Senders of erroneous or abusive notices should face possible sanctions. In the US, senders may face penalties for knowingly misrepresenting that content is infringing, but the standard for "knowingly misrepresenting" is quite high and the provision has rarely been invoked.[3] A better approach might be to use a negligence standard, whereby a sender could be held liable for damages or attorneys' fees for making negligent misrepresentations (or for repeatedly making negligent misrepresentations). In addition, the notice-and-action system should allow content hosts to ignore notices from senders with an established record of sending erroneous or abusive notices or allow them to demand more information or assurances in notices from those who have in the past submitted erroneous notices. (For example, hosts might be deemed within the safe harbor

[3] In one case, the judge noted that "there are likely to be few [cases] in which a copyright owner's determination . . . will meet the requisite standard of subjective bad faith required to prevail in an action for misrepresentation under 17 U.S.C. § 512(f)." *See* Lenz v. Universal Music Corp et al. (Case 5:07-cv-03783 JF).

if they require repeat abusers to specifically certify that they have actually examined the alleged infringing content before sending a notice.)

- **Transparency.** Disclosure by service providers of notices received and actions taken can provide an important check against abuse. In addition to providing valuable data for assessing the value and effectiveness of a N&A system, creating the expectation that notices will be disclosed may help deter fraudulent or otherwise unjustified notices. In contrast, without transparency, Internet users may remain unaware that content they have posted or searched for has been removed pursuant due to a notice of alleged illegality. Requiring notices to be submitted to a central publication site would provide the most benefit, enabling patterns of poor quality or abusive notices to be readily exposed.

Additional comments on what actions can be required (related to Question 17)

Intermediaries should not be required to take actions that would create a de facto ongoing monitoring regime. Article 15 of the ECD expressly prohibits Member States from obligating intermediaries to monitor the information they transmit or store, or to seek out indications of illegal activity. This provision is essential to the ability of intermediaries to offer robust and participatory online services that facilitate communication without jeopardizing user privacy. Any actions required by N&A policies must conform with Article 15.

Despite this prohibition, some national courts have imposed duties on content hosts to prevent the reposting of particular content once the service provider has removed it.[4] Such "notice-and-stay-down" requirements effectively create an ongoing obligation to monitor all transmissions or user-generated content in order to prevent reintroduction of the prohibited content and are thus inconsistent with Article 15. While this kind of obligation may be particularized to specific, previously identified content (e.g. a list of specific movies or songs), it nonetheless requires an intermediary to monitor *all* content in order to identify and prevent reposting of the targeted content for an unlimited period.

The European Court of Justice recently ruled in *Scarlet v. SABAM* that an injunction requiring an ISP to install a filter to prevent future transfers of copyright-infringing files was inconsistent with Article 15.[5] The ECJ then applied the same rationale in *SABAM v. Netlog*, stating that a similar injunction imposed on a social networking host service was also inconsistent with Article 15, as it creates a de facto, ongoing obligation to indiscriminately monitor the activity of all users for an unlimited period.[6] Based on these opinions, guidance from the Commission should clarify that "notice-and-stay-down" requirements, which entail the same manner of broad monitoring, are inconsistent with Article 15.

---

[4] *See, e.g.*, Agnès Lucas-Schloetter, "Google face à la justice française et belge: Nouvelles décisions en matière de droit d'auteur," 2 (2011) JIPITEC 144, http://www.jipitec.eu/issues/jipitec-2-2-2011. *See also DailyMotion v. Zadig* Productions, Cour d'Appel de Paris, 3 December 2010.

[5] *SABAM v. Scarlet*, C-70/10, ¶¶34-40, http://curia.europa.eu/juris/document/document.jsf?text=&docid=115202&pageIndex=0&doclang=EN&mode=doc&dir=&occ=first&part=1&cid=996022.

[6] *SABAM v. Netlog*, C-360/10 (European Court of Justice), http://curia.europa.eu/juris/document/document.jsf?text=&docid=119512&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=161927. In its opinion, the ECJ also raised concerns about the proportionality of the injunction related to access to information, data protection, and the freedom of Netlog to conduct its business.

Detailed response to Question 24: Different policy approaches for different categories of illegal content

Uniform notice-and-action procedures should not apply horizontally to all types of illegal content. In particular, CDT believes notice-and-takedown is inappropriate for defamation and other areas of law requiring complex legal and factual questions that make private notices especially subject to abuse.

Blocking or removing content on the basis of mere allegations of illegality raises serious concerns for free expression and access to information. Hosts are likely to err on the side of caution and comply with most if not all notices they receive, because evaluating notices is burdensome and declining to comply may jeopardize their protection from liability. The risk of legal content being taken down is especially high in cases where assessing the illegality of the content would require detailed factual analysis and careful legal judgments that balance competing fundamental rights and interests. Intermediaries will be extremely reluctant to exercise their own judgment when the legal issues are unclear, and it will be easy for any party submitting a notice to claim a good faith belief that the content in question is unlawful. In short, the murkier the legal analysis, the greater the potential for abuse.

To reduce this risk, removal of or disablement of access to content based on unadjudicated allegations of illegality (i.e., notices from private parties) should be limited to cases where the content at issue is manifestly illegal – and then only with necessary safeguards against abuse as described above.

France's implementation of the ECD includes the notion that determining the legality of certain content can be so difficult that a judicial decision may be required to compel intermediaries to act; intermediaries need to take down content upon private notice only when it is "manifestly illegal."[7] One French court found that a claim that comments denying the Armenian genocide constituted a violation of plaintiffs' dignity under principles of international law, but was not manifest since it was not reflected in law.[8] In that case, a court order was required to compel action by the intermediary.

Such cases appear to be the exception, however. French courts have found illegality to be "manifest" in a wide range of cases, and the concept that private notice-and-takedown obligations should be limited to particular narrow categories is not widely present in Member State implementations.[9]

CDT believes that online free expression is best served by narrowing what is considered manifestly illegal and subject to takedown upon private notice. With proper safeguards against abuse, for example, notice-and-action can be an appropriate policy for addressing online copyright infringement. Copyright is an area of law where there is reasonable international consensus regarding what is illegal and where much infringement is straightforward. There can be difficult questions at the margins – for example concerning the applicability of limitations and exceptions such as "fair use" – but much online infringement is not disputable.

---

[7] Loi pour la confiance dans l'économie numérique, n° 2004-575 du 21 juin 2004, http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005789847&dateTexte=vig.

[8] Comité de défense de la cause arménienne v. Aydin & France Telecom, Paris Court of Appeal, November 8, 2006, http://www.foruminternet.org/telechargement/documents/ca-par20061108.pdf.

[9] *See* European Commission Staff Working Paper, "Online services, including e-commerce, in the Single Market," 11 January 2012, http://ec.europa.eu/internal_market/e-commerce/docs/communication2012/SEC2011_1641_en.pdf.

Quite different considerations apply to the extension of notice-and-action procedures to allegations of defamation or other illegal content. Other areas of law, including defamation, routinely require far more difficult factual and legal determinations. There is greater potential for abuse of notice-and-action where illegality is less manifest and more disputable. If private notices are sufficient to have allegedly defamatory content removed, for example, any person unhappy about something that has been written about him or her would have the ability and incentive to make an allegation of defamation, creating a significant potential for unjustified notices that harm free expression. This and other areas where illegality is more disputable require different approaches to notice and action. In the case of defamation, CDT believes "notice" for purposes of removing or disabling access to content should come only from a competent court after full adjudication.[10]

In cases where it would be inappropriate to remove or disable access to content based on untested allegations of illegality, service providers receiving allegations of illegal content may be able to take alternative actions in response to notices. Forwarding notices to the content provider or preserving data necessary to facilitate the initiation of legal proceedings, for example,[11] can pose less risk to content providers' free expression rights, provided there is sufficient process to allow the content provider to challenge the allegations and assert his or her rights, including the right to speak anonymously.

[10] CDT recognizes that differences in US and EU law on defamation will inform whether allegedly defamatory content is considered manifestly illegal. Nonetheless, we believe that defamation is too subjective an area of law to be appropriate for notice-and-takedown systems given the potential for abuse.

[11] Canada has just passed an update to its copyright laws that includes notice-forwarding and data retention requirements (upon notice) for online content hosts.