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

COMMENTS OF CDT TO THE DG INTERNAL MARKET AND SERVICES, REGARDING NOTICE-AND-ACTION PROCEDURES BY INTERNET INTERMEDIARIES

29 February 2012

The Center for Democracy & Technology (CDT) welcomes the opportunity to submit these comments to the Directorate General Internal Market and Services questionnaire regarding online intermediaries' notice-and-action (N&A) procedures with regard to third-party illegal content. CDT is a not-for-profit, non-governmental public policy organization working to promote democratic values and human rights in the digital age. Our mission is to conceptualize, develop, and implement public policies that will keep the Internet open, innovative, and free.

CDT takes as its starting point the strong belief that the ability of online intermediaries to focus on empowering communications by and among users is essential to the continued development of the Internet as a platform for economic growth and the exercise of fundamental rights. Protecting intermediaries from liability and from broad or open-ended obligations to control the behavior of users and third-parties is essential to fostering innovation, access to information services, and free expression on the Internet. In contrast, if intermediaries such as hosts and platforms are discouraged from allowing users to post content because of liability risk or content-policing burdens, then the full benefits of the information society will remain unrealized.[1]

When intermediaries are liable for the content created by others, they will strive to reduce their liability risk, which can lead to over-blocking of legitimate content. Moreover, without protection from liability or the legal certainty that flows from a harmonized approach, companies are less likely to develop new, general-purpose information society services at all. Enforcement obligations that make intermediaries responsible for policing and controlling user behavior – including unbalanced N&A policies that lack effective safeguards against abuse – carry similar risks.

N&A policies to address illegal online content must balance several interests: not just the interest in addressing harms, but also the interest of online intermediaries in offering open, efficient platforms for communication across borders and the fundamental right of users in the free expression that those platforms enable and protection of personal data. These comments offer several principles for achieving that balance, based on CDT's experience monitoring the

[1] For a fuller discussion of the impact of intermediary protections on fundamental rights and innovation, see CDT, *Intermediary Liability: Protecting Internet Platforms for Expression and Innovation*, April 2010, https://www.cdt.org/paper/intermediary-liability-protecting-internet-platforms-expression-and-innovation.

implementation of N&A procedures under the E-Commerce Directive and the United States' Digital Millennium Copyright Act (DMCA). While CDT does not have facts and figures of its own to offer, to the extent possible we have tied the responses below to specific questions in the questionnaire.

Principles for Notice-and-Action Systems

A. Intermediaries need clear guidance regarding what constitutes a valid notice.[2]

When an intermediary receives a notice, it is risky for the intermediary to refuse to act upon it. Receipt of the notice may expose the intermediary to charges that it now has knowledge of whatever activity is described in the notice, and that the intermediary accordingly may be held liable if that activity is held to be illegal. Without guidance, therefore, intermediaries will tend to act with an overabundance of caution, complying without question even to notices that are vague, frivolous, or otherwise best ignored. Unquestioning acceptance of notices in turn invites excessive and abusive notices that constrain lawful expression.

Guidance from the EC can help provide necessary clarity, identifying best practice on how best to structure N&A systems to improve the reliability of notices. At a minimum, notices must clearly and specifically identify the illegal content at issue, the legal justification for action (that is, what legal provision does the content violate), and evidence or attestations of illegality sufficient to warrant action by the intermediary in the absence of judicial involvement.

B. Actions required of intermediaries must be narrowly tailored and proportionate.[3]

Actions by intermediaries must be evaluated in terms of the principle of proportionality and their impact on Internet users' fundamental rights, including rights to freedom of expression, access to information, and protection of personal data. The United Nations Special Rapporteur on freedom of expression and opinion concluded in a 2011 report that the Internet is increasingly an essential tool for exercising these fundamental rights.[4] Actions that have the potential to limit online expression or access to information must be prescribed by law and necessary in a democratic society to achieve a legitimate aim, a high standard requiring the measure be proportional to the aim, no more restrictive than is required for achievement of the aim, and effective for achieving the purpose.[5]

Accordingly, action requirements should be narrowly drawn. Targeted removal of particular content, where appropriate, is preferable to broader actions that risk interfering with legal content (e.g., by targeting entire websites or other Internet resources that may support both lawful and unlawful uses).

---

[2] This section addresses concerns raised under Questions 6, 8, 10, 11, 12, and 28.

[3] This section addresses issues raised in Questions 16, 17, 18, 20, and 28.

[4] United Nations, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/17/27, 2011, http://www2.ohchr.org/english/bodies/hrcouncil/17session/reports.htm.

[5] United Nations, Report of the SR on the promotion and protection of the right to freedom of opinion and expression, A/HRC/14/23, 2010, http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.23.pdf.

As discussed below, action requirements for conduit Internet service providers (ISPs) carry especially high risk of overbroad and disproportionate impact. But this is not to say that there is no narrowly tailored and proportionate role that ISPs can play. "Notice-and-notice" systems, in which ISPs forward notices of infringing activity to subscribers, raise fewer problems and can have a meaningful impact.[6] Such notices alert subscribers that their activity is not anonymous and offer an opportunity to educate subscribers about potential consequences, without subjecting all users' entire traffic stream to ongoing surveillance or impairing the availability of lawful content.

C. Safeguards are necessary to mitigate risks of abuse.[7]

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 (as suggested by the reference to automated takedown in question 12), 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.[8]

In regards to question 10, the existence of abuse of the US's DMCA takedown process in the form of unjustified notices is well documented. It is difficult to assess with precision the proportion of unjustified notices, but advocates and scholars have catalogued many examples. The Electronic Frontier Foundation has created a "Takedown Hall of Shame" to publicize unwarranted and frivolous notices, including cases where infringement was highly doubtful and where the interest motivating the demand had nothing to do with copyright and thus was outside the intended scope of the notice-and-takedown regime.[9] The website chillingeffects.org maintains a database of notices in an effort to document and expose the stifling impact for free expression of questionable notices.[10] And CDT wrote a report in October 2010 demonstrating that notices are sometimes used to silence lawful political messages by campaigns.[11]

---

[6] The ISP and entertainment industries in the United States have announced a "Copyright Alert" system of notices, designed with a primarily educational goal. *See* Press Release at http://www.copyrightinformation.org/node/704. *See also* Joint Statement of CDT and Public Knowledge, 7 July 2011, https://www.cdt.org/pr_statement/cdt-public-knowledge-joint-statement-copyright-alert-system.

[7] This section addresses issues raised in Questions 8, 10, 12, 13, 20, 21, 22, 23, 24, 26, and 28.

[8] For example, YouTube's global user base uploads 60 hours of video per minute. "Holy Nyans! 60 hours per minute and 4 billion views a day on YouTube," *Broadcasting Ourselves: The Official YouTube Blog*, 23 January 2012, http://youtube-global.blogspot.com/2012/01/holy-nyans-60-hours-per-minute-and-4.html. Google, which owns YouTube, 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.

[9] https://www.eff.org/takedowns.

[10] http://www.chillingeffects.org; *See also* Jennifer M. Urban & Laura Quilter, *Efficient Processes or Chilling Effects? Takedown Notices under Section 512 of the Digital Millennium Copyright Act*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 612 (2006).

[11] *See, e.g.*, CDT, *Campaign Takedown Troubles,* October 2010, https://www.cdt.org/files/pdfs/copyright_takedowns.pdf; *See also* Wendy Seltzer, *Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects on the DMCA on the First Amendment*, 24 HARV. J.L. & TECH., author's draft at http://wendy.seltzer.org/media/seltzer_free_speech_unmoored.pdf.

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

- **The availability of penalties for unjustified notices.** Under the United States' DMCA, parties who make knowing misrepresentations in a notice of infringing material can be liable for damages.[12] In the first case brought under this provision, a company was ordered to pay damages for takedown notices sent in regard to content not protected by copyright due to the fair use doctrine.[13] Nonetheless, some have raised concerns that the bar for obtaining damages for unjustified notices is too high to deter abuse.[14]

- **The inclusion of an appeal and counter-notice mechanism.** In cases where notice can lead to the removal of content, the affected user or content provider should have a mechanism to appeal the takedown and restore material taken down wrongfully. The DMCA has detailed "counter-notice" procedures for this purpose. The responses provided to questions 21-23 in the Questionnaire will be instructive in how best to structure allowances for counter-notices.

- **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 will deter fraudulent or otherwise unjustified notices. In contrast, without transparency, Internet users may remain unaware that that content they have posted or searched for has been removed pursuant due to a notice of alleged illegality. In a recent example of the role of transparency, a popular blog author discovered that his analysis of a current policy debate had been deleted from Google's search engine results due to a clearly mistaken takedown notice. He discovered this because Google, the intermediary in question, disclosed in its search results that it had removed certain items. Without this disclosure – not required under the law – he apparently would not have known that his content had been suppressed.[15]

- **Flexibility on the part of service providers.** Any N&A system should preserve the ability of intermediaries to exercise judgment and perform some screening of notices received. While concerns over scale and cost will likely prevent many intermediaries from doing so (as the responses to questions 11-14 may reveal), the legal framework should not unduly discourage or bar service providers from exercising their judgment and assessing whether any particular notice is fraudulent or too vague in its allegations.

---

[12] 17 U.S.C. 512(f).

[13] *OPG v. Diebold*, 337 F. Supp. 2d 1195 (N.D. Cal. 2004).

[14] In another case, the judge noted that "there are likely to be few [cases] in which a copyright owner's determination that a particular use is not fair use will meet the requisite standard of subjective bad faith required to prevail in an action for misrepresentation under 17 U.S.C. § 512(f)."

[15] Mike Masnick, "Key Techdirt SOPA/PIPA Post Censored By Bogus DMCA Takedown Notice," *Techdirt*, 28 February 2012, http://www.techdirt.com/articles/20120223/15102217856/key-techdirt-sopapipa-post-censored-bogus-dmca-takedown-notice.shtml.

The EC could play a positive role by identifying best practice for how Member States and intermediaries can mitigate the risk of abuse.

D. Intermediaries should not be required to take actions that would create a de facto ongoing obligation to monitor.[16]

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.[17] 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, 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 the transfer of copyright-infringing files was inconsistent with Article 15.[18] 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.[19] Based on these opinions, guidance from the EC should clarify that "notice-and-stay-down" requirements, which entail the same manner of broad monitoring, are inconsistent with Article 15.

E. Action requirements should take account of differences between conduit and host services.[20]

Questions 16–18 identify several different actions intermediaries may take in response to notices: content removal and three techniques for blocking. Guidance from the EC should be clear that not every action is appropriate for all types of intermediaries.

---

[16] This section addresses issues raised in Questions 15, 16, 17, and 28.

[17] *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.

[18] *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.

[19] *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.

[20] This section addresses issues raised by Questions 16, 17, 18, 27, and 28.

In particular, the guidance should carefully distinguish content removal from the blocking of websites and other online locations. It is tempting to consider content removal and blocking as analogous, with hosts removing content and conduits blocking online locations. But this analogy is inapt: blocking carries additional implications that must be considered. "Notice and takedown" in the context of hosts cannot simply be translated into "notice and block" in the case of conduits.

Content removal by hosting services, when executed with due process and appropriate safeguards, can be particularized to narrowly affect only the intended content. By contrast, directing ISPs to block entire websites by IP address or domain name (as listed in question 18) is very likely to disproportionately limit lawful expression. Many sites share IP addresses, such that blocking an IP address would result in innocent sites' being blocked.[21] The same is true of blocking domains.[22] In addition, domain blocking is trivially circumvented and poses additional risks to the security and stability of the domain name system.[23] Finally, even where it can be assured that only the intended location will be blocked, blocking risks being overly broad. Sites frequently contain a mix of legal and illegal content.

Nor are ISPs well positioned to recognize which individual items of content are unlawful and to take action against those items only. For ISPs to filter particular content requires deep-packet inspection or other techniques that are damaging to user privacy and impose additional costs on ISP services. *Scarlet v. SABAM* held that content filtering obligations on IPS, in addition to contravening Article 15, are too costly, disproportionate, and invasive to users' privacy to be consistent with EU law. Any N&A guidance issued by the EC should reflect this inconsistency.

F. Actions that result in content takedown must be limited to contexts where illegality is straightforward.[24]

Notwithstanding that the ECD applies horizontally to all types of illegal content, indiscriminately blocking or removing content on the basis of mere allegations of illegality raises serious concerns for free expression and access to information.[25] Intermediaries are likely to err on the side of caution and comply with most if not all notices they receive, since 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 so 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.

---

[21] *See CDT v. Pappert,* 337 F. Supp. 2d 606 (E.D. Pa. 2004).

[22] *id.*; *See also* "CDT Warns Against Widespread Use of Domain-Name Tactics to Enforce Copyright," https://www.cdt.org/policy/cdt-warns-against-widespread-use-domain-name-tactics-enforce-copyright.

[23] 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.

[24] This section addresses issues raised in Questions 12, 13, and 15.

[25] CDT recognizes that not all Member States' implementations require court orders for content removal. Here we focus on those transpositions where notices can come from private parties.

To reduce this risk, removal of content based on unadjudicated allegations of illegality 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."[26] 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.[27] 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.[28] CDT believes that online free expression is best served by narrowing what is considered manifestly illegal and subject to takedown upon notice. For instance, CDT views takedown as inappropriate for allegations of defamation, because whether particular content is indeed defamatory is hardly incontrovertible and rarely immediately apparent.[29] In addition, 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 notices that undermine free expression.

G. Notice-and-action requirements must avoid undermining the ECD's liability protections.

As discussed above, N&A frameworks carry some risk to free expression. Streamlined processes for targeting content offer a tempting vehicle for anyone who might take issue with particular content, even in cases where that person's concerns are illegitimate and/or the content is legal. Safeguards are essential, again as discussed above. But where N&A policies seek to enable prompt relief following notice of content a private actor believes is illegal, the risk of abuse cannot be fully eliminated. A streamlined process for taking action, especially where that action is the removal of content, will result in some level of mistakes that can impact legitimate expression.

In both Europe and the United States, the legal framework counterbalances this risk to free expression by coupling N&A regimes with provisions giving Internet intermediaries strong protections from liability. These protections foster and enhance free expression by giving intermediaries the legal certainty they need to offer innovative services and provide new forums for communications and content distribution by Internet users.

---

[26] 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.

[27] 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.

[28] *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.

[29] 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.

Given that N&A policies are part of an overall policy balance that includes strong liability protections for intermediaries, N&A policies should not be implemented or interpreted in ways that would undermine those liability protections. Guidance should state this general principle clearly.

This principle also means that EU members should evaluate the likely practical impact of N&A policies on intermediaries. Policies should be rejected if they would undermine the legal certainty that liability protections are intended to create. In particular, the certainty provided by liability protections is only as strong as the clarity of the conditions on which such protections are granted. To the extent that implementing an N&A policy is prerequisite to protection, laws and guidelines need to clearly define intermediaries' obligations under the N&A framework. Where N&A obligations are too vague, making it unclear what an intermediary needs to do to qualify for protection, the certainty intended by the liability protections would be lost.

For More Information

CDT appreciates the opportunity to offer these principles for notice-and-action frameworks to address illegal content online. More information can be found at http://www.cdt.org, or by contacting Jim Dempsey, jdempsey@cdt.org, Cynthia Wong, cynthia@cdt.org, or Andrew McDiarmid, andrew@cdt.org.