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

SHIELDING THE MESSENGERS: PROTECTING PLATFORMS FOR EXPRESSION AND INNOVATION

Version 2, updated December 2012

This paper examines the impact on free expression, privacy, and innovation of forcing Internet intermediaries to bear liability or assume gatekeeping obligations for third-party content. Intermediary liability arises where governments or private litigants can hold technological intermediaries such as ISPs and websites liable for unlawful or harmful content disseminated by users of those services. Gatekeeping obligations, such as requirements that intermediaries filter or block access to content, force intermediaries to monitor or limit how users access or post material. The threat of either liability or gatekeeping obligations reduces intermediaries' willingness to host user-generated content, leads intermediaries to block even legal content, and inhibits innovation. Limiting such obligations and protecting intermediaries from liability for the expressive actions of third parties expands the space for online expression, encourages innovation in the development of new communications services, and creates more opportunities for local content, thereby supporting development of the information society. Meanwhile, there are ways to address unlawful or harmful online content without burdening intermediaries. Internet advocates everywhere should urge governments to adopt policies that protect intermediaries as critical platforms for innovation, expression, and economic activity.

Contents

SHIELDING THE MESSENGERS: PROTECTING PLATFORMS FOR EXPRESSION AND INNOVATION

The global Internet has become a vibrant and essential platform for economic activity, human development, and civic engagement. Every day, millions of journalists, students, business people, scientists, government officials, politicians, and citizens go online to speak, access information, and participate in nearly all aspects of public and private life. Telecommunications carriers, Internet service providers (ISPs),[1] websites, social networks, and a range of other technological entities play critical roles in transmitting information and ideas across the online world.[2] Often called "intermediaries," these entities facilitate access to content created by others. They provide valuable tools and forums for expression by users.

Given the scale and openness of the Internet, it is inevitable that some users will post content or engage in activity that is unlawful or offensive. As a result, Internet intermediaries often face calls to control or police user activity in a wide range of circumstances, including in response to claims of defamation, obscenity, intellectual property infringement, invasion of privacy, or because content is critical of government. This raises challenging policy questions that will impact the future growth of the online environment: Should technological intermediaries be held liable for content posted by their users and other third parties? Under what circumstances, if any, is it appropriate to require or encourage intermediaries to police or limit access to such content?[3]

This paper examines several possible approaches to the legal treatment of Internet intermediaries and assesses their impact on innovation, economic development, and human rights. We argue that the history of the Internet to date shows that providing broad legal protections for intermediaries is vital to its future. Users should bear legal responsibility for their unlawful online activities, but Internet intermediaries generally should not. Policies that protect intermediaries from liability for third-party content and from obligations to police such content expand the space for expression and innovation and better promote the Internet as a platform for a wide range of beneficial activities. In contrast, policies that force intermediaries to bear liability risks or high costs associated with monitoring or removing content discourage intermediaries from enabling users to post content. This greatly diminishes opportunities for expression and prevents the full benefits of the information society from being realized.

Governments, policymakers, and private actors can and should seek less damaging ways to combat harmful and unlawful material online. This paper's final section discusses some policy alternatives that do not impose burdens on Internet intermediaries.

I. Roles of Intermediaries

The Internet and mobile technologies have amplified individuals' abilities to speak and access

[1] We use the term "Internet service providers" to refer to providers of Internet access – in other words, the entities offering end users wired or wireless connections to the Internet.

[2] There are other kinds of intermediaries online. For example, credit card companies can be thought of as "financial intermediaries." Our analysis focuses on technological intermediaries such as ISPs, web hosts, and content platforms.

[3] *See* Organization for Economic Cooperation and Development, *The Role of Internet Intermediaries in Advancing Public Policy Objectives*, Sept. 2011, http://www.oecd.org/document/34/0,3746,en_2649_34223_48773090_1_1_1_1,00.html.

information in unprecedented ways. This is especially true in the Web 2.0 era, where user-generated content platforms allow individuals with little technical knowledge or money to create, disseminate, and access content in a range of formats and with a worldwide audience.

Consider the following examples:

- A journalist connects to her publication's website through an ISP to upload a story on a natural disaster, and local residents add their own comments on the publication's website.
- A doctor makes a video using her mobile phone, posts the video on YouTube, and uses SMS to send a link to health clinics, where the video can be shown to patients.
- A local entrepreneur applies for a line of credit using a mobile banking application, sells surplus business equipment through an online auction site, and researches a potential business acquisition on the web from his laptop.
- A homemaker connects to a community discussion site to complain about the service at a local business.
- Hundreds of millions of ordinary citizens log on to multiple social networking sites each day to share photos of their lives and interact with distant relatives and friends.

Many different intermediaries are involved in these examples:

- **Network operators and mobile telecommunications providers,** which provide the physical and technical infrastructure for transmission of information
- **Access providers/ISPs**, which provide the service of connecting end users to the Internet (often using their own transmission infrastructure)
- **Registrars and registries**, which respectively operate top-level domains (like .com and .fr) and sell domain names (like cdt.org) to individuals and businesses
- **Website hosting companies**, which rent website space to users for web pages, including for interactive forums
- **Online service providers** including blog platforms, email service providers, social networking websites, and video and photo hosting sites
- **Internet search engines and portals**
- **E-commerce platforms and online marketplaces**, such as eBay and Amazon
- In general, any website that hosts **user-generated content** or allows **user-to-user communications** – for example, newspapers with websites that allow for user comment

Each of these categories includes not only large, well-known service providers with millions of users and worldwide reach, but also countless small, little-known businesses and individuals serving particular geographic areas or communities of interest. For every profit-making enterprise with an extensive revenue stream and budget, there are many other Internet intermediaries operating on shoestring budgets or for non-commercial purposes. A small

blogging platform in a developing nation and a not-for-profit online discussion forum about upcoming local elections are Internet intermediaries no less than the relative handful of online companies that have become household names.

II. Intermediary Liability

A. Sources of Intermediary Liability – Government Sanctions and Exposure to Civil Litigation

For governments, intermediaries represent a potential point of control over content and unlawful behavior. Because the Internet as it currently exists enables relatively anonymous or pseudonymous speech, governments argue it is often difficult or time-consuming to identify individual users who post illegal or offensive content. Individual perpetrators also may be located abroad, beyond the government's jurisdictional reach. In contrast, intermediaries that host or transmit content are much easier to identify, may already be subject to various licensing or regulatory requirements, and are more likely to have local operations that make them subject to the government's jurisdiction. In addition, the speed and scale of Internet communication can pose challenges to effective enforcement against individuals.

Some governments therefore require intermediaries to control prohibited content, threatening them with financial or even criminal sanctions if they host or transmit such content through their services. In essence, the government delegates the task of policing content to the private intermediaries and forces them to scrutinize and limit user activity.

Alternatively or in addition, a legal regime may enable private actors to bring lawsuits seeking damages from intermediaries for hosting or transmitting content supplied by users (for example, in defamation or privacy actions). Intermediaries can be particularly attractive targets for private litigation because they are easier to identify and reach than individual users. Many intermediaries also may be more able to pay damages than are the individuals who post the content (though for smaller and non-commercial intermediaries, this may not be the case). If the law exposes intermediaries to liability in the form of civil damages, intermediaries will be forced to review and limit user content just as they would if subject to direct government fines.

B. Models of Intermediary Liability

The question of who can be held liable for harmful or illegal content arose early in countries with broad Internet adoption. In examining various national and regional approaches, we can observe a general trend: Those governments that have sought to maximize growth of Information and Communication Technologies (ICTs) have tended to limit civil and criminal liability for technological intermediaries. In contrast, governments in the most Internet-restrictive countries often hold intermediaries responsible for illegal content posted by users, forcing intermediaries to become content gatekeepers and hindering innovation. Approaches to intermediary liability can be generalized in three models.

Model 1: Expansive Protections against Liability for Intermediaries

In the mid-1990s, the US enacted a law known as "Section 230" of the Communications Act, which generally protects intermediaries from liability for a wide range of content posted by third

parties (though it does not address intellectual property infringement).[4] This approach to intermediary liability has helped the country develop a vibrant and innovative Internet industry. Examination of the statute offers an informative look at how carefully crafted protections for intermediaries can foster growth in the ICT sector while also enabling voluntary action against harmful content.

Section 230 grants intermediaries broad immunity, largely removing the risk of potentially massive liability for illegal behavior by users.[5] It shields online services against a wide variety of claims, including negligence, violations of federal civil rights laws, and defamation.[6] This protection has enabled the dramatic growth of social networking and other interactive, user-generated content sites that have become vibrant platforms for expression in the US and all over the world.[7] Without Section 230, open-ended liability risks would dramatically raise entry barriers for new Internet services and applications that allow user-generated content, jeopardizing innovation in interactive media. Free expression would suffer as well, because intermediaries would seek to protect themselves by paring back on user-generated content features and engaging in over-cautious screening and blocking of whatever user-generated content they still allow – actions that inevitably would impede legitimate online expression. Section 230, by relieving legal pressure on intermediaries, preserves their ability to function as robust platforms for online speech.[8]

At the same time, Section 230 contains a provision that protects intermediaries from liability when they voluntarily block or take down content they believe could be harmful or objectionable to their users.[9] This often-overlooked portion of the law serves the very interests that advocates

---

[4] 47 U.S.C. § 230, http://www.law.cornell.edu/uscode/47/230.html. 17 U.S.C. § 512 governs intermediary liability when third-party content infringes copyright. *See infra* note 15 and accompanying discussion. Section 230 also has no effect on US Federal criminal law. 47 U.S.C. § 230(e)(1).

[5] Section 230 calls these intermediaries "interactive computer services." 47 U.S.C. 230(c)(1). The statute provides: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C. 230(c)(1).

[6] *See*, *e.g.*, CDT, "CDT Joins Briefs Urging Courts to Properly Apply § 230 of the CDA," *Policy Post 14.4*, March 31, 2008, http://www.cdt.org/policy/cdt-joins-briefs-urging-courts-properly-apply-section-230-cda. *See also* Electronic Frontier Foundation, "Section 230 Protections," *Bloggers' Legal Guide*, http://www.eff.org/issues/bloggers/legal/liability/230.

[7] *See generally* Electronic Frontier Foundation, *EFF's Guide to CDA 230: The Most Important Law Protecting Online Speech*, December 6, 2012, https://www.eff.org/deeplinks/2012/12/effs-guide-cda-230-most-important-law-protecting-online-speech.

[8] *See*, *e.g.*, Electronic Frontier Foundation, *CDA § 230 Success Case: Yelp*, https://www.eff.org/issues/cda230/successes/yelp (Question: "What would happen if CDA 230 did not exist?" Answer: "Absent CDA 230, websites like Yelp would be pressured to avoid liability by removing legitimate, negative reviews, and they would deprive consumers of information about the experiences of others.").

[9] 47 U.S.C. § 230(c)(2) provides, *inter alia*, that "no provider or user…shall be held liable on account of...any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected…." The statute also contains at § 230(b) an explicit policy statement in support of development and use of blocking and filtering technologies ("It is the policy of the United States… to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services; to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material"), and provides safe harbor at §230(c)(2)(B) for any action taken to enable or make available such technologies.

of intermediary liability typically seek to advance – for example, limiting online crime and the dissemination of offensive content.

This second provision of Section 230, promoting the ability of intermediaries to engage in voluntary and good-faith content removal, enables content platforms and social networking sites to experiment with user-driven flagging systems for identifying and removing content that violates their community guidelines – such as harassment, bullying activity, and sexual content — without fear that doing so might expose the services to liability.[10] Similarly, the provision supports anti-spam and cybersecurity efforts. So long as service providers act in good faith, they may block or remove content that they believe is spam or contains harmful code, without fear of legal action by the senders of such traffic. Similarly, Section 230 also supports intermediaries that voluntarily identify, block, and remove obscene material or apparent child abuse images. All of these self-regulatory activities are allowed, but are not required, under Section 230.

Voluntary blocking by intermediaries can carry risks. Such action can raise due process, accountability, and human rights concerns if undertaken in response to government pressure or coercion, as we explore in Section V below. And even truly voluntary measures targeting harmful activity can have unintended impact on the rights to freedom of expression and privacy, which companies should consider and work to mitigate. For example, companies should make sure that any suppression of content is carried out in a manner that is consistent with their terms of service, transparent, and subject to appeal in appropriate circumstances.[11]

Nonetheless, Section 230 illustrates how a policy of protecting intermediaries from liability is compatible with – and can even serve – other societal interests, such as protecting children.

Model 2: Conditional Safe Harbor from Liability

A second model is to offer intermediaries a conditional "safe harbor." Under this approach, an intermediary receives protection against liability for user conduct, but only if the intermediary meets certain criteria.[12] This model seeks to find a middle ground that recognizes the benefits of liability protection described above while at the same time defining certain roles for intermediaries with respect to unlawful content.

The European Union's E-Commerce Directive (ECD) includes a conditional safe harbor that applies a broad range of content and legal claims.[13] India has nominally adopted a framework loosely modeled after the ECD, though recent regulatory and court actions suggest that it may

[10] *See, e.g.*, YouTube Community Guidelines, http://www.youtube.com/t/community_guidelines.

[11] For further discussion, see Erica Newland, Caroline Nolan, Cynthia Wong & Jillian York, Berkman Center for Internet & Society and the CDT, *Account Deactivation and Content Removal: Guiding Principles and Practices for Companies and Users*, Sept. 2011, https://www.cdt.org/report/account-deactivation-and-content-removal-guiding-principles-and-practices-companies-and-users.

[12] Failing to qualify for safe harbor protection does not make an intermediary automatically liable for third-party content; it simply means that liability will be assessed using generally applicable legal standards, without any special protection.

[13] The text of EU Directive 2000/31/EC can be found at http://ec.europa.eu/internal_market/e-commerce/directive_en.htm.

not provide intermediaries much legal protection or certainty in practice.[14] In the United States, the Digital Millennium Copyright Act (DMCA) established a conditional safe harbor that focuses specifically on copyright infringement claims.[15] Copyright enforcement provisions modeled on this DMCA safe harbor have been included in bilateral free trade agreements between the US and Australia, Bahrain, Central American/Dominican Republic states, Chile, Columbia, the Republic of Korea, Morocco, Oman, Panama, Peru, and Singapore.[16] A recent survey commissioned by the World Intellectual Property Organization identified the conditional-safe-harbor approach as the most widely adopted approach to copyright liability for intermediaries.[17]

Conditional safe harbor regimes typically distinguish between several types of intermediaries, with conditions for safe harbor eligibility varying depending on the category of service an intermediary provides. The main categories of service providers identified in the ECD and DMCA safe harbor regimes are as follows.[18]

- **Providers of transmission/"mere conduit" functions** – The ECD and the DMCA safe harbors generally apply to ISPs (and any other entities whose role is to route and transmit Internet communications), protecting them from liability for content transmitted over their services.[19] To qualify for the safe harbors, however, an ISP must not initiate the transmission, select the recipients, or select or modify the transmitted content. The ISP also must not have stored the content for any longer than reasonably necessary for transmission.

- **Caching providers** – The ECD and DMCA safe harbors both apply to providers of caching, meaning the automatic, intermediate, and temporary storage of content for the purpose

---

[14] Erica Newland, "Shielding the Messengers: Internet on Trial in India," *CDT Policy Beta* blog, Mar. 20, 2012, https://www.cdt.org/blogs/erica-newland/2003shielding-messengers-internet-trial-india; Centre for Internet & Society, *Intermediary Liability and Freedom of Expression*, Sept. 14, 2012, http://cis-india.org/internet-governance/intermediary-liability-and-foe-executive-summary.pdf/view.

[15] 17 U.S.C. § 512. For a good overview of the DMCA safe harbor, see Frequently Asked Questions (and Answers) about DMCA Safe Harbor, http://www.chillingeffects.org/dmca512/faq.cgi. The text of the law can be found at http://www4.law.cornell.edu/uscode/17/512.html.

[16] *See* US Trade Representative, Free Trade Agreements, http://www.ustr.gov/trade-agreements/free-trade-agreements. National legislation implementing these trade agreements, however, can result in safe harbor provisions that differ from US law in significant respects. For an analysis of Chile's recent law regarding the copyright safe harbor, see CDT, *Chile's Notice-and-Takedown System for Copyright Protection: An Alternative Approach*, Aug. 2012, https://www.cdt.org/files/pdfs/Chile-notice-takedown.pdf.

[17] Daniel Seng, *Comparative Analysis of National Approaches of the Liability of the Internet Intermediaries,* World Intellectual Property Organization, 2011, http://www.wipo.int/export/sites/www/copyright/en/doc/liability_of_internet_intermediaries.pdf. For an overview of the intermediary liability landscape in several African countries, *see* Alex Comninos, *The Liability of Internet Intermediaries in Nigeria, Kenya, South Africa and Uganda: An Uncertain Terrain*, Association for Progressive Communications, Oct. 2012, http://www.apc.org/en/node/15649/.

[18] Note that while the two regimes use similar categories and conditions for determining safe harbor eligibility, the scope of the legal protection afforded to qualifying entities is quite different. As discussed above, the ECD safe harbor confers protection against a broad range of legal claims; the DMCA safe harbor confers protection against copyright infringement claims only, because non-copyright claims against intermediaries are already covered by the broad protections of Section 230. In addition, the DMCA prescribes a specific notice-and-takedown system for content removal. By contrast, the ECD safe harbor applies to intermediaries without "actual knowledge" of illegal content, and what constitutes actual knowledge triggering a takedown requirement varies across member states.

[19] Art. 12, E-Commerce Directive, 2000/31/EC; 17 U.S.C. § 512(a).

of making onward transmission more efficient.[20] Conditions for this protection include requirements that a caching provider must not modify the cached content and must remove the content upon learning that it has been taken down (or been ordered to be taken down) from its original source due to properly formed claims that it is unlawful.

- **Hosting providers** – The ECD and DMCA safe harbors both apply to providers of hosting services, protecting them from liability for content stored on their systems at the direction of users.[21] To qualify, a hosting provider must not have actual knowledge of the illegal content. Importantly, the hosting provider is also required to remove the illegal content expeditiously upon learning of it. The DMCA further conditions safe-harbor protection on hosting providers implementing a specific "notice-and-takedown" process for receiving and responding to notices from copyright holders.

  In both the Europe and the United States, there has been some debate about the scope of the hosting provider category. In an Italian criminal case against Google Video, for example, the court ruled that Google Video was not eligible for the safe harbor because the service, rather than merely providing a space on the Internet where users can publish their content, went further by organizing and promoting videos, showing related advertising, and other activities.[22] In a US suit against YouTube, Viacom made similar arguments against YouTube's eligibility for DMCA safe harbor. But in both the Viacom case and a similar case involving a smaller video-hosting site called Veoh, US appeals courts rejected the idea that only passive providers of raw hosting space qualify for the DMCA safe harbor.[23] These are crucial rulings: limiting safe harbors protections to blank-slate hosting would make them nearly useless, as almost all popular user-generated content websites and services would cease to be eligible.

- **Information location tools** – The DMCA safe harbor extends to "information location tools" such as search engines and directories.[24] Providers of these services get safe harbor from copyright liability under the US law if they lack actual knowledge of infringement, do not directly benefit from infringement they have the right and ability to control, and quickly remove or disable access to links to infringing materials when notified of infringement. While the ECD safe harbor does not cover information location tools, many EU member states have extended protections to them anyway, recognizing their importance to the functioning of the Internet.[25]

Both the ECD and the DMCA also include some general requirements that apply to all of these types of intermediaries. For example, the ECD safe harbor is limited to intermediaries that have

---

[20] Art. 13, E-Commerce Directive, 2000/31/EC; 17 U.S.C. § 512(b).

[21] Art. 14, E-Commerce Directive, 2000/31/EC; 17 U.S.C. § 512(c).

[22] *See* Leslie Harris, "Deep Impact: Italy's Conviction of Google Execs Threatens Global Internet Freedom," *HuffPost Tech*, Feb. 24, 2010, http://www.huffingtonpost.com/leslie-harris/deep-impact-italys-convic_b_474648.html. The court decision, in Italian, can be found at http://speciali.espresso.repubblica.it/pdf/Motivazioni_sentenza_Google.pdf.

[23] *Viacom Int'l v. YouTube,* 676 F.3d 19 (2d Cir. 2012); *UMG Recordings v. Shelter Capital Partners,* 667 F.3d 1022 (9th Cir. 2011). *See also* CDT, *Cases Wrestle with Role of Online Intermediaries in Fighting Copyright Infringement,* June 26, 2012, https://www.cdt.org/policy/cases-wrestle-role-online-intermediaries-fighting-copyright-infringement.

[24] 17 U.S.C. § 512(d).

[25] European Commission, First Report on the application of Directive 2000/31/EC, p. 13.

not been directly collaborating in the illegal acts.[26] The DMCA safe harbor applies only to intermediaries that "reasonably implement" a policy of terminating the accounts of repeat infringers.[27]

A central but also controversial feature of the EU and US conditional safe harbors is the creation of "notice-and-action" or "notice-and-takedown" systems. Under these systems, content hosts (plus search engines, in the US) promptly remove particular material when they receive a notice claiming it is unlawful. The DMCA sets out a specific procedure for notices and potential counter-notices.[28] The ECD does not specify particular procedures, though the European Commission has launched a public consultation on the topic.[29]

These notice-and-takedown regimes put the burden of identifying illegal activity on affected parties rather than on the intermediaries themselves; both the ECD and the DMCA expressly state that intermediaries need not actively monitor their services for unlawful activity.[30] This is a crucial limitation. First, active monitoring of user communications by intermediaries – especially access providers – can raise significant privacy issues. Second, the sense that communications are subject to pervasive surveillance would substantially chill the use of online forums for robust free expression. Third, given the high volume of user participation in many online ventures, it can be extremely costly for online intermediaries engage in active monitoring of user communications. If intermediaries unable or unwilling to bear such costs were disqualified from the safe harbor, many would opt to control their legal risks by eliminating or placing tight constrains on user participation functions and features. Innovation in user-empowering communications tools would suffer dramatically. For all of these reasons, the basic bargain of notice-and-takedown, as enacted in the EU and US, is to ask intermediaries to respond to unlawful content when notified about specific instances of it, but at the same time to make clear that intermediaries are not required to affirmatively monitor the content of user communications.

Even without any monitoring obligation, however, the notice-and-takedown approach leads to numerous removals of content pursuant to the demands and discretion of private parties. Proponents of the approach say that this is what enables it to offer an expedient and much-needed recourse for wrongs that occur through online services: It provides a process that is much faster and much less costly than relying on the courts or other government decision-making mechanisms. In addition, having intermediaries implement a notice-and-takedown system can help ensure that those intermediaries are not actively engaging in or encouraging unlawful behavior. Copyright-based industries claim that, in practice, the vast majority of copyright takedown notices accurately identify infringing content and serve the important aim of

---

[26] ECD Recital 44.

[27] 17 U.S.C. § 512(i).

[28] 17 U.S.C. § 512(c)(3), (g).

[29] European Commission, Notice-and-action Procedures, http://ec.europa.eu/internal_market/e-commerce/notice-and-action/index_en.htm.

[30] Art. 15, E-Commerce Directive, 2000/31/EC; 17 U.S.C. § 512(m). The European Court of Justice has ruled in two cases that Art. 15 (among other Articles) precludes the imposition of content-filtering obligations on both ISPs and user-generated content hosts. *See Scarlet Extended SA v SABAM—Société belge des auteurs, compositeurs et éditeurs SCRL* (Court of Justice of the European Union case C-70/10), Nov. 24, 2011; *see also SABAM v. Netlog NV* (Court of Justice of the European Union, Case C-360/10), Feb. 16, 2012, http://curia.europa.eu/juris/document/document.jsf?text=&docid=119512&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=161927.

promptly removing such content from circulation. If anything, they argue, copyright notice-and-takedown regimes need to be strengthened and streamlined to keep pace with the large volume of unlawful online material.

On the other hand, notice-and-takedown systems are vulnerable to abuse. Fraudulent or bad-faith notices, issued for improper purposes such as to silence critics, can result in the removal of lawful content. Users whose content has wrongly been flagged as unlawful may have little recourse or few resources to challenge the takedown and seek re-posting of their content.[31] Meanwhile, intermediaries often have little or no incentive to question or refuse a takedown request, even if they suspect the notice-and-takedown system is being abused. They cannot afford to risk losing their protection from liability; determining whether particular content is actually illegal would require detailed legal and factual inquiry that they are not equipped to conduct; and the safe harbor regime calls on them to act promptly. Thus, most intermediaries will simply take down the material as soon as they receive the request to do so.[32] Advocates have documented how improper and over-aggressive use of notice-and-takedown systems can harm free expression.[33]

Given the potential risks, policymakers must take care to minimize any negative impact of conditional safe-harbor regimes on free expression.[34] For example, Chile's 2010 copyright law seeks to reduce improper takedowns by requiring takedown notices to come from a court, rather than directly from private parties.[35] It is too early to assess the practical impact this layer of court oversight will have in practice; some copyright holders have expressed concern that it will make the takedown process too slow and cumbersome to serve as an effective tool for fighting the large volume of online infringement. But Chile's law certainly suggests a novel model that departs in significant ways from the EU and US examples.

---

[31] 17 U.S.C. § 512(g) permits users to object to a takedown action by filing a "counter-notice." The process requires disclosure of user information and consent to court jurisdiction. *See* Nart Villeneuve, "Evasion Tactics: Global online censorship is growing, but so are the means to challenge it and protect privacy," *Index on Censorship* 36, issue 4, Nov. 2007, pp. 74–76, http://www.nartv.org/mirror/evasiontactics-indexoncensorship.pdf (describing several case studies where notice-and-takedown systems were exploited to silence online critics).

[32] The Centre for the Internet & Society in India recently tested the real-world impact of India's notice-and-takedown regime by submitting frivolous complaints to seven intermediaries, from search engines to user-generated content platforms. None of the content at the heart of these complaints was illegal or "prohibited," but six of the seven intermediaries removed the content anyway. Pranesh Prakash, *Invisible Censorship: How the Government Censors Without Being Seen*, Centre for the Internet & Society, Dec. 15, 2011, http://cis-india.org/internet-governance/invisible-censorship. *See also* 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.

[33] *See* Electronic Frontier Foundation, "Takedown Hall of Shame," http://www.eff.org/takedowns (documenting abuses of US trademark and copyright law to silence critics or political opponents). *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.*, 2006, p. 612. *See also* http://www.chillingeffects.org.

[34] *See, e.g.,* Ian Brown, "Internet Self-Regulation and Fundamental Rights," *Index on Censorship* 1, March 2010, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1539942 ("While…schemes [to deputise ISPs so as to regulate cyberspace more firmly] are more flexible and less burdensome than statutory regulation, they commonly lack the procedural fairness and protection for fundamental rights that are encouraged by independent judicial and parliamentary scrutiny. Few schemes include any substantive protection for individuals' rights to freedom of expression, association or privacy.").

[35] For an analysis of Chile's approach, see CDT, "Chile's Notice-and-Takedown System for Copyright Protection: An Alternative Approach," Aug. 2012, https://www.cdt.org/files/pdfs/Chile-notice-takedown.pdf.

While the details may vary from country to country, there are some general principles that conditional safe harbor regimes must follow in order to promote innovation in online services and minimize risks to free expression:

Protections must be broadly available to a variety of intermediaries.

To ensure the Internet remains an open, competitive marketplace for communication and innovative services, a wide variety of Internet intermediaries should be eligible to protect themselves from liability. Safe harbors should not be limited to a narrow class of intermediaries performing a narrowly focused set of functions. For example, as discussed above, it would make little sense to restrict the safe harbor only to basic or "passive" hosting that provides raw server space with none of the advanced or innovative features of popular user-generated content sites. By excluding the participatory and interactive services that are at the heart of "Web 2.0," such limits would significantly impair online innovation in any country that imposes them.

Conditions should not be too burdensome.

The reason for limiting intermediaries' liability is to remove impediments (in the form of legal risks) to providing innovative and beneficial services. To avoid replacing these risks with new obstacles, it is crucial that conditions not be too onerous for new and innovative services to meet.

To make safe harbors accessible to the entities that need them, conditions should be clearly articulated and should scale easily with the volume and pace of Internet communication. In particular, they should steer well clear of imposing a direct or de facto obligation to monitor users' content and activity, since ongoing monitoring can be hard to scale and undermines both user privacy and the development of new participatory features and services. Conditions also should reflect key differences between different types of intermediaries. For example, it would make little sense to ask ISPs, which transmit content but do not store it, to implement notice-and-takedown systems. ISPs have no ability to remove specific items of content from the servers where they are stored, and asking them to block access to entire websites would pose grave risks to lawful expression.

Safe harbors need not, however, be readily available to clear "bad actors" that are actively and knowingly aiding or conspiring in unlawful activity. This is why, for example, the ECD and DMCA include conditions that can deny safe harbor protection to entities that collaborate directly in illegal acts, know about specific illegal activity yet fail to respond, or profit directly from unlawful activity they effectively control. The key – and a significant challenge – is to ensure that such limits on safe harbor protection are not implemented and enforced in a manner that excludes or burdens Internet intermediaries operating in good faith.

Any notice-and-takedown regime needs to give intermediaries clear guidance regarding what constitutes a valid notice.

It is risky for an intermediary to refuse to honor a takedown notice. Clear guidance on what constitutes a valid notice is therefore essential to protect lawful expression and ensure that vague, frivolous, or otherwise inappropriate notices will be rejected. Perhaps

most importantly, notices should be required to clearly and specifically identify the illegal content at issue, including its location (such as a specific URL). Notices that demand the removal of particular content wherever it appears on a website are not sufficiently precise to enable targeted action and thus should not be deemed sufficient. At a minimum, notices also should be required to include the legal justification for action (that is, what legal provision does the content violate); contact information for the person or entity sending the notice; and evidence or attestations of illegality sufficient to warrant action by the intermediary in the absence of judicial involvement.[36]

Actions required of intermediaries must be narrowly tailored and proportionate, to protect the fundamental rights of Internet users.

Any actions that a safe-harbor regime requires intermediaries to take 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,[37] and protection of personal data.[38] Laws that encourage intermediaries to take down or block certain content have the potential to impair online expression or access to information. Such laws must therefore ensure that the actions they call for are proportional to a legitimate aim, no more restrictive than is required for achievement of the aim, and effective for achieving the aim.[39] In particular, intermediary action requirements should be narrowly drawn, targeting specific unlawful content rather than entire websites or other Internet resources that may support both lawful and unlawful uses.

Notice-and-takedown must be limited to contexts where illegality is straightforward.

The risk of legal content being taken down is especially high in cases where assessing the illegality of the content would require detailed factual and legal analysis or the balancing of competing fundamental rights and interests. Where the legal issues are complicated, intermediaries will almost never be willing to exercise their own judgment regarding whether particular content is illegal or not. They therefore are likely to honor virtually any takedown notice claiming to identify unlawful content.

To reduce the risk of wrongful takedowns, notice-and-takedown regimes should be limited to cases where the content at issue is manifestly illegal – and then only with necessary safeguards against abuse as described below. In the copyright context, for example, unauthorized postings of entire commercial works can present relatively

[36] For CDT's suggested list of minimum requirements for notices, see CDT, "Additional Responses Regarding Notice-and-Action," 2012, pp.1–2, https://www.cdt.org/files/file/CDT%20N&A%20supplement.pdf.

[37] *See* 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 (concluding that the Internet is increasingly an essential tool for exercising these fundamental rights). *See also* Universal Declaration of Human Rights, Art. 19 (1948); International Convention on Civil and Political Rights, Art. 19 (1966); Convention on the Rights of the Child, Art. 13 (1989); African Charter on Human and People's Rights, Art. 9 (1981); European Convention on the Protection of Human Rights and Fundamental Freedoms, Art. 10 (1950); American Convention on Human Rights, Art. 13 (1969).

[38] *See, e.g.,* Universal Declaration of Human Rights, Art. 12 (1948); International Covenant on Civil and Political Rights, Art. 17 (1966); Convention on the Rights of the Child, Art. 16 (1989); European Convention for the Protection of Human Rights and Fundamental Freedoms, Art. 8 (1950); American Convention on Human Rights, Art. 12 (1969).

[39] 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.

evident instances of infringement. By contrast, in CDT's view, notice-and-takedown will virtually always be inappropriate for allegations of defamation, because whether particular content is indeed defamatory is generally a contentious question and rarely easily apparent.[40] In addition, under a notice-and-takedown regime that covers defamation, any person unhappy about something that has been written about him or her would have the ability and strong incentive to get the content promptly removed simply by issuing takedown notices alleging defamation. This would create a significant potential for content takedowns that undermine free expression and public discourse.

Safeguards are necessary to mitigate risks of abuse.

Notice-and-takedown regimes, as well as any other safe harbor conditions that encourage intermediaries to impose sanctions targeting particular individuals or content, must include adequate safeguards against abuse. In particular, it is essential to include counter-notice or similar appeal mechanisms for persons who want to contest a notice or a content takedown. Other safeguards for notice-and-takedown should include: the availability of penalties for submitting unjustified notices;[41] transparent disclosure by intermediaries of notices received and actions taken;[42] and adequate legal flexibility for intermediaries to exercise judgment and to reject unjustified notices when they see fit. An additional safeguard would be to provide for greater involvement by or appeal to a judicial body. As discussed above, for example, Chile's law routes takedown demands through the courts rather than directly to intermediaries.[43]

---

[40] CDT recognizes that international variations in defamation law 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. A hypothetical example illustrates the problem: Imagine that a citizen writes a blog post stating that a particular local government official has embezzled money from the government treasury. The official then serves a takedown notice, claiming the blog post is defamatory. The blog operator has no way at all to determine if the allegation is false (in which case the posting might be defamatory) or true (in which case the posting is a vital instance of citizens seeking to hold their government accountable) – and national law may consider the posting defamatory regardless of its truth or falsity. If a blog operator risked liability only if it were to leave the posting up, the operator would almost certainly remove the post.

[41] Under the US DMCA, parties who make knowing misrepresentations in a notice of infringing material can be liable for damages. 17 U.S.C § 512(f). *See also OPG v. Diebold*, 337 F. Supp. 2d 1195 (N.D. Cal. 2004). The provision has rarely been invoked, however, probably because "knowing misrepresentation" is a difficult legal standard to prove and because challenging a notice in court is costly. *See* Eric Goldman, "Rare Ruling on Damages for Sending Bogus Copyright Takedown Notice – Lenz v. Universal," *Technology & Marketing Law Blog*, Feb. 26, 2010, http://blog.ericgoldman.org/archives/2010/02/standards_for_5.htm. CDT has suggested that a negligence standard would provide a more effective deterrent to erroneous notices. In addition, notice-and-action systems could allow intermediaries to ignore notices from senders who have submitted erroneous notices in the past. *See* CDT, "Additional Responses Regarding Notice-and-Action," *supra* note 36, pp. 2-3.

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

[43] *See supra* note 35 and accompanying text.

Model 3: Blanket or Strict Liability for Intermediaries

Some countries broadly impose liability on intermediaries in order to restrict speech. For example, the Chinese government imposes liability for unlawful content on entities at every layer of a communication, from the ISP to the online service provider, website, and hosting company.[44] If any of these intermediaries publishes or distributes content that regulators deem unlawful, or fails to sufficiently monitor the use of its services, take down content, or report violations, it could face fines, criminal liability, and revocation of its business or media license. The categories of content that regulators consider unlawful are broadly and vaguely defined (including, for example, content that "harms the interests of the nation").[45] In addition, actual enforcement practices and patterns vary considerably over time, and government officials often do not follow proper legal procedures when issuing filtering or takedown orders. In recent years, private defamation suits have also been used to silence online criticism of local businesses or government officials.[46]

In Thailand, Internet intermediaries that transmit or host third-party content face serious liability risks under the 2007 Computer Crimes Act (CCA).[47] The CCA punishes the online publication or knowing dissemination of "false" or publicly accessible "obscene computer data" that is likely to cause injury to a person, the public, or national security.[48] The CCA fails to define many of these terms and its broad language makes it difficult to determine what speech will be held unlawful. Indeed, the CCA has been used to punish political dissent and criticism of the government. In one widely watched case, Chiranuch Premchaiporn, the webmaster of an online news website, was tried and convicted for being too slow to remove user-posted comments deemed insulting to Thailand's monarchy.[49]

---

[44] Measures for Managing Internet Information Services, Article 20 [in Chinese], issued by the State Council on September 25, 2000, effective October 1, 2000. Unofficial English translation available at http://www.chinaculture.org/gb/en_aboutchina/2003-09/24/content_23369.htm. *See also* OpenNet Initiative, *Access Contested*, MIT Press, 2011, http://access.opennet.net/wp-content/uploads/2011/12/accesscontested-china.pdf, pp. 279–80.

[45] For a list of relevant laws, *see* Congressional-Executive Commission on China, "Freedom of Expression – Laws and Regulations," http://www.cecc.gov/pages/virtualAcad/exp/explaws.php#vaguelaws.

[46] Sophie Beach, "Recent Defamation Cases and Abuse of Local Power," *China Digital Times*, April 30, 2009, http://chinadigitaltimes.net/china/defamation/.

[47] Sections 15 of the Computer Crimes Act BE 2550 (Thailand, 2007), English translation available at http://advocacy.globalvoicesonline.org/wp-content/plugins/download-monitor/download.php?id=2; *see also* Sawatree Suksri, Siriphon Kusonsinwut, and Orapin Yingyongpathana, "Situational Report on Control and Censorship of Online Media through the Use of Laws and the Imposition of Thai-State Policies ," *iLaw Project*, December 8, 2010, http://www.boell.de/downloads/ilaw_report_EN.pdf. A draft revision to the CCA, released in 2011, but not adopted as of this writing, would similarly create criminal liability for intermediaries; *see* CDT, Comments on Thailand's Proposed Computer-Related Offenses Commission Act, March 2012, https://www.cdt.org/files/pdfs/Comments-Thailand-CCA-Draft.pdf.

[48] Section 14 of the Computer Crimes Act BE 2550 (Thailand, 2007).

[49] *See e.g.,* Sean W. Crispin, "Internet Freedom on Trial in Thailand," *CPJ Blog*, February 4, 2011, http://cpj.org/blog/2011/02/internet-freedom-on-trial-in-thailand.php; "CDT Objects to Conviction of Thai Webmaster as Threat to Free Expression," May 30, 2012, https://www.cdt.org/pr_statement/cdt-objects-conviction-thai-webmaster-threat-free-expression. *See also* Reuters, "Lerpong Wichaikhammat, US Citizen, Arrested for Insulting Thailand's King Bhumibiol Adulyadej," *HuffPost World*, "Thailand Arrests American for Alleged King Insult," *Associated Press*, May 27, 2011, http://www.huffingtonpost.com/2011/05/27/thailand-arrests-us-citizen-king-bhumibiol-adulyadej-insult_n_867951.html.

Blanket liability greatly limits the ability of intermediaries to offer innovative services, new platforms for expression, and opportunities for participation and interaction among users. It also creates strong incentives to closely monitor user activity and to block content that carries any risk of complaint or controversy. In addition, this kind of regime leads users and service providers to self-censor. Knowing that certain content is likely to be taken down and perhaps result in penalties, users sharply limit what they try to post and service providers sharply limit the kinds of content they solicit or encourage. These indirect methods of control can be just as dangerous for free expression as direct government censorship.

III. Gatekeeping Obligations on Intermediaries

In recent years, there have been growing pressures to transform the role of Internet intermediaries into content gatekeepers. Some governments have sought to do this directly, by affirmatively requiring intermediaries to restrict or police user activity in specified ways.

Proponents of such gatekeeping requirements say that preventing users from posting or accessing unlawful material in the first place is better than just assessing liability after the damage caused by the material has already been done. They believe intermediaries are in a position to prevent people within their jurisdictions from accessing illegal content – even content hosted in foreign jurisdictions beyond the government's reach.[50] Some also see the issue as a matter of fairness: The businesses that benefit from the opportunities the Internet creates, they argue, should play a role in implementing technological solutions to the challenges the Internet poses to (for example) copyright holders and law enforcement.

Imposing gatekeeping obligations on Internet intermediaries, however, can have a profound and negative impact on lawful expression, user privacy, and innovation. We discuss the risks and costs in greater detail in Section IV. The remainder of this section reviews some of the specific gatekeeping obligations that have been proposed or adopted.

A. Website Blocking

Countries are increasingly pressuring ISPs to block access to websites that may host objectionable content.[51] Many counties have quasi-voluntary or law-enforcement-led programs

[50] *See* Hearing on the Stop Online Piracy Act before the US House of Representatives Committee on the Judiciary: Statement of Chairman Lamar Smith, November 16, 2011, http://judiciary.house.gov/news/Statement%20HR%203261.html (arguing for new, intermediary-based copyright enforcement tools "when a rogue website is foreign-based and foreign-operated"); *see also* Internet Watch Foundation, "About Us,", http://www.iwf.org.uk/public/page.103.htm ("As sexually abusive images of children are primarily hosted abroad, we facilitate the industry-led initiative to protect users from inadvertent exposure to this content").

[51] The most extreme example of widespread website blocking is the Chinese government's censorship system. China's two state-owned Internet backbone providers use DNS tampering, IP blocking, and URL blocking to prevent access to pornography, politically sensitive material, and foreign news outlets. *See* OpenNet Initiative, *Access Denied: The Practice and Policy of Global Internet Filtering*, MIT Press, 2008, p. 267, http://opennet.net/accessdenied.

under which ISPs block access to child abuse images.[52] Courts around the world have issued orders for ISPs to block entire Internet sites, particularly file-trading sites and other sites engaged in intellectual property infringement.[53] The Internet Law of Turkey permits administrative orders against ISPs to block access to particular websites.[54] In the US, proposed legislation would have allowed orders requiring ISPs to block the domains of sites found to be dedicated to copyright and trademark infringement, though the legislation was abandoned after it provoked a major public outcry in early 2012.[55]

There are a number of ways that an ISP can attempt to prevent users from visiting certain websites. It can block access to the sites' numeric Internet Protocol (IP) addresses; their domain names; or their individual URLs.[56] However, each of these tactics can undermine the Internet's capacity for promoting free expression and access to information. For example, a single IP address can be shared by dozens or even hundreds of websites and other types of Internet hosts. Similarly, many web-hosting services are constructed such that thousands of individual sites, maintained by thousands of individuals, are hosted at subdomains that share a single parent domain name.[57] This means that blocking particular IP addresses or domain names carries a very high risk that completely legitimate material will be suppressed along with the targeted content. A 2003 blocking law in the US state of Pennsylvania was struck down as unconstitutional in part because of the vast amount of overblocking caused by IP- and domain-

---

[52] *See, e.g.*, Internet Watch Foundation, "IWF Facilitation of the Blocking Initiative," http://www.iwf.org.uk/services/blocking; Comprehensive Operational Strategic Planning for the Police (COSPOL) Internet Related Child Abuse Material Project, "CIRCAMP Overview," http://www.circamp.eu/index.php?option=com_content&view=article&id=11:circamp-overview&catid=1:project&Itemid=2.

[53] For example, a British Court ordered ISPs to block access to Newzbin, a file-sharing site: *Twentieth Century Fox v. British Telecommunications* (High Court of Justice, October 26, 2011), http://www.bailii.org/cgi-bin/markup.cgi?doc=/ew/cases/EWHC/Ch/2011/2714.html&query=newzbin&method=boolean; a Dutch Court ordered two ISPs to block Pirate Bay: *BREIN v. Ziggo/XS4ALL* (The Hague District Court case 374634/HA ZA 10-3184, Jan. 11, 2012), http://zoeken.rechtspraak.nl/detailpage.aspx?ljn=BV0549; and courts have issued similar orders in India: Nikhil Pahwa, "Indian Music Industry Gets Court Orders For Blocking 104 Music Sites," *Medianama*, March 15, 2012, http://www.medianama.com/2012/03/223-india-music-block/.

[54] Regulation of Publications on the Internet and Suppression of Crimes Committed by Means of Such Publication, Law no. 5651, Turkish Official Gazette no. 26030, 23 May 2007, Art. 8. For a fuller analysis, *see* Y. Akdeniz, "Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship," 2010, http://www.osce.org/documents/rfm/2010/01/42294_en.pdf.

[55] Stop Online Piracy Act , H.R. 3261, 112th US Congress (2011); Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act, S. 968, 112th US Congress (2011). *See also* CDT, Growing Chorus of Opposition to "Stop Online Piracy Act," Jan. 9, 2012, https://www.cdt.org/report/growing-chorus-opposition-stop-online-piracy-act.

[56] All hosts on the Internet have IP addresses (such as 174.143.118.160) and are typically identified by domain names (such as cdt.org). Individual files on a host are accessed using URLs such as http://www.cdt.org/international. Each of these identifiers can be used in a filtering system. For more on filtering/blocking technologies, *see* OpenNetwork Initiative, *Access Denied*, MIT Press, 2008, http://oni-access.net/denied/.

[57] For example, each blog hosted on Blogger shares the same domain name (blogspot.com) but is operated independently by individuals. Blocking individual subdomains (such as subdomain.blogspot.com) is possible and more accurate, but can be more complex and costlier to implement, and does not eliminate all risk of overblocking.

blocking.[58]

In some cases, due to the ways in which data is routed on the Internet, IP-blocking in one country may lead to a website becoming inaccessible for the entire world.[59] In addition, the widespread blocking of domain names in particular would present technical challenges that could undermine the Internet's reliability and security.[60]

Blocking based on specific URLs is more narrowly focused and hence avoids some of these risks. Nonetheless, it too can result in unintended blocking.[61] URL filtering is also the costliest to implement.[62]

B. Domain-name Seizures

In the last several years, US law enforcement authorities have begun seizing domain names of websites charged with unlawful conduct.[63] The government does this by ordering the intermediaries responsible for maintaining the relevant domain name system (DNS) databases to revoke or reassign a website's domain name. Specifically, the government directs seizure orders to domain-name registries (the entities that manage the database of names in top-level domains like ".com" and ".fr") and registrars (those authorized to sell domain names like "cdt.org" to of the public). Often registries and registrars are instructed to point the names to new sites. For example, anyone who attempts to view a website that has had its domain seized by US law enforcement is instead directed to a site explaining that the name has been seized.[64]

Domain-name seizures are susceptible to overblocking for the same reasons as domain-name

---

[58] *CDT v. Pappert*, 337 F.Supp.2d 606 (E.D. Penn. 2004) (overturning The Internet Child Pornography Act, 18 Pa. Cons. Stat. §§ 7621-7630). *See also* CDT, *The Pennsylvania ISP Liability Law: An Unconstitutional Prior Restraint and a Threat to the Stability of the Internet*, February 2003, http://www.cdt.org/speech/pennwebblock/030200pennreport.pdf.

[59] In 2008, a state-owned Pakistani ISP's technique for blocking YouTube resulted in the site being inaccessible to the world for two hours. *See* Declan McCullagh, "How Pakistan knocked YouTube offline (and how to make sure it never happens again)," *CNET*, February 25, 2008, http://news.cnet.com/8301-10784_3-9878655-7.html.

[60] Domain name blocking would conflict with implementations of the DNS Security Extensions (DNSSEC), and circumvention efforts by users would increase security vulnerabilities for networks and users alike. *See* Crocker, Dagon, Kaminsky, McPherson, and Vixie, *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.

[61] For example, Australia's Communications and Media Authority developed a blacklist of URLs to block under a then-planned mandatory national Internet filtering system. When the blacklist was leaked in 2009, it was found to include the URLs of a dentist's office and an anti-abortion activism site. *See* Asher Moses, "Conroy Backtracks on Internet Censorship Policy," *The Age*, April 1, 2009, http://www.theage.com.au/articles/2009/04/01/1238261622790.html. This episode demonstrates that Internet filtering policies can easily be used, inadvertently or otherwise, to suppress legitimate speech – especially if the process for choosing which websites to block is not transparent.

[62] *See* Ofcom (UK Telecom Regulator), *"Site Blocking" to reduce online copyright infringement,* Aug. 3, 2011,

http://stakeholders.ofcom.org.uk/binaries/internet/site-blocking.pdf.

[63] *See, e.g.* US Department of Justice Press Release, "Federal Courts Order Seizure of 150 Website Domains," November 28, 2011, http://www.justice.gov/opa/pr/2011/November/11-ag-1540.html. Some private litigants have used similar tactics in suits over botnets and trademark infringement. *See, e.g.,* Lance Whitney, "With legal nod, Microsoft ambushes Waledac botnet," *CNET*, Feb. 25, 2010, http://news.cnet.com/8301-1009_3-10459558-83.html.

[64] *See, e.g.*, http://tvshack.cc/.

blocking. For example, in February 2011, the US government temporarily seized the domain name "mooo.com," which is a parent domain to thousands of independent subdomains.[65] The government's intent was to target one of those subdomains for alleged violations of child abuse image laws. But the impact was far broader. Until the government realized its mistake, many websites engaged solely in legitimate speech saw their visitors redirected to a banner announcing that the sites had been seized for trafficking in child pornography.

Domain-name seizures also present difficult jurisdictional and procedural problems. When a domain name is seized, the effect is felt worldwide, not just within the jurisdiction where the seizure occurs. Internet users all over the world can no longer reach the original website via that domain name. This can lead to disputes when content is lawful in the jurisdiction where it is hosted, but unlawful elsewhere. Procedurally, governments have often seized domain names without advance notice to the domain name owner and before a court has fully assessed the lawfulness of the associated website.

One of the US seizures illustrates both problems. Rojadirecta.com, the domain name of a Spanish site twice found legal under Spanish law, was nonetheless seized by US law enforcement authorities in 2011. The website's owners challenged the site's seizure in court, arguing that the seizure violated their free expression rights.[66] Eventually, US authorities dismissed the charges and allowed the return of the domain name, but only after the website operators had been deprived of their domain name for nineteen months, impairing access for users not just in the US but worldwide.[67]

C. Licensing Requirements, Content Regulation, and Mandatory Filters

Some countries have saddled Internet intermediaries with broadcast-style regulations, such as licensing requirements and rules demanding "balanced coverage" or other editorial controls. For example, in 2011, Hungary imposed broadcast-style regulations on a wide range of Internet intermediaries[68] and Italy did so for video-hosting sites.[69] The Sri Lankan Media Ministry announced in November 2011 – following accusation that certain sites were defaming public officials – that news websites (domestic or foreign) with "any content relating to Sri Lanka" must

[65] Thomas Claburn, "ICE Confirms Inadvertent Web Site Seizures," *InformationWeek*, Feb. 18, 2011, http://www.informationweek.com/news/security/vulnerabilities/229218959. Examples of innocent subdomains that were effectively seized include greyghost.mooo.com, alec.mooo.com, and fdahlger.mooo.com.

[66] Andrew McDiarmid, "Domain Seizures Amount to Prior Restraint on Speech," *CDT Policy Beta* blog, June 21, 2011, https://www.cdt.org/blogs/andrew-mcdiarmid/domain-seizures-amount-prior-restraint-speech.

[67] David Sohn, "Government Walks Away from Another Controversial Domain Name Seizure," *CDT PolicyBeta* blog, Aug. 29, 2012, https://www.cdt.org/blogs/david-sohn/2908government-walks-away-another-controversial-domain-name-seizure. The practical impact on users was mitigated somewhat by the fact the website quickly reestablished itself at new domain names. But the reappearance of the site also illustrates the ineffectiveness of domain-name seizures as a law enforcement tactic.

[68] CDT, "Legal Analysis of the Proposed Amendments to the 2010 Hungarian Media Laws," March 2, 2011, http://www.cmcs.ceu.hu/files/CDT%20Analysis%20Amendments%20to%20Hungarian%20Media%20Laws.pdf; "Hungary Amends Media Law, Diffusing EU Criticism," *Reuters*, March 7, 2011, http://www.reuters.com/article/2011/03/07/us-hungary-media-vote-idUSTRE7265RN20110307.

[69] Phillip Willan, "Italy's Video Sharing Sites Subject to Broadcast TV Rules," *IDG News Service*, January 4, 2011, http://news.idg.no/cw/art.cfm?id=52DAD36F-1A64-6A71-CEF3C2A212E62B9F.

register with the government.[70] Meanwhile, the Malaysian and Australian governments are considering extending existing media regulations to online media.[71]

In addition, automatic content filters, designed to identify and block specific content rather than entire websites, have gotten the attention of some courts. Some hosting providers, such as YouTube, voluntarily use such filtering technology to reduce copyright infringement.[72] In two cases involving SABAM, a Belgian copyright collecting society, lower courts ordered Internet intermediaries (an ISP and a social-networking site) to install automated content filters to prevent the distribution of copyrighted content. Fortunately, the European Court of Justice ruled that such filtering mandates violate users' data-protection and access-to-information rights, as well as ECD Article 15's prohibition against general obligations to monitor content.[73]

Licensing requirements, content regulation, and filtering mandates necessarily limit expressive opportunities online and undermine the Internet's role as an open medium for speakers of all kinds. They provide governments with powerful levers of control over content. This is a lesson already apparent to China's Internet users; China requires local ISPs to deliver only licensed websites, and uses the license process to ensure censorship and self-censorship by websites.[74]

D. Warning or Punishing Individual Users

Finally, escalating concerns about online copyright infringement are creating pressures to enlist ISPs in threatening or punishing individual users who appear to be engaged in infringement. For example, France's HADOPI law targets unlawful file-sharing by requiring ISPs to forward warning notices to subscribers identified by rightsholders as likely infringers. Where subscribers ignore the warnings and engage in repeat infringement, ISPs may be ordered to disconnect

---

[70] Reporters Without Borders, "Government Blocks Critical News Websites, Says They Have to Register," Nov. 8, 2011, http://en.rsf.org/sri-lanka-government-blocks-critical-news-08-11-2011,41367.html.

[71] *See* "New law to control press, and a promise to hobble Internet," *Uppercaise: Malaysian Media Matters,* March 31, 2012, http://uppercaise.wordpress.com/2012/03/31/new-law-to-control-press-and-a-promise-to-hobble-internet/; *See also* R. Finkelstein, Report of the Independent Inquiry into the Media and Media Regulation to the Minister for Broadband, Communications and Digital Media, February 28, 2012, http://www.dbcde.gov.au/__data/assets/pdf_file/0006/146994/Report-of-the-Independent-Inquiry-into-the-Media-and-Media-Regulation-web.pdf.

[72] *See* http://www.youtube.com//t/contentid. Notably, such automated systems are not always accurate. *See, e.g.*, Geeta Dayal, "The Algorithmic Copyright Cops: Streaming Video's Robotic Overlords," *Wired's Threat Level* blog, September 6, 2012, http://www.wired.com/threatlevel/2012/09/streaming-videos-robotic-overlords-algorithmic-copyright-cops/all/ (criticizing automated copyright takedown systems and noting some high-profile takedown mistakes).

[73] *Scarlet v. SABAM* and *SABAM v. Netlog*, supra note 30.

[74] Once a website license is granted, the grantee is responsible for monitoring site content and engaging in self-censorship. PRC Telecommunications Regulations, [2000] State Council Order No. 291 [中华人 民 共 和 国电信 条 例, 2000] 国务院 令 第 291 号, http://www.isc.org.cn/20020417/ca38931.htm. *See also China's Information Control Practices and the Implications for the United States: hearing before the US-China Econ. & Sec. Review Comm'n*, testimony of Rebecca MacKinnon, Visiting Fellow, Ctr. for Info. Tech. Policy, Princeton Univ., June 30, 2010, http://www.uscc.gov/hearings/2010hearings/written_testimonies/10_06_30_wrt/10_06_30_mackinnon_statement.php

them.[75] A few countries have adopted similar laws.[76] In contrast, Canada and Chile have adopted laws under which ISPs will forward warning notices to suspected infringers, but will not be expected to disconnect subscribers from the Internet or otherwise impose punishment.[77] In addition, as discussed in Section V.A below, some ISPs have adopted notice-forwarding processes voluntarily, without any legal requirement.

Warning systems can serve a beneficial educational purpose, informing subscribers about the law and the potential consequences of their actions. To the extent such systems call on private intermediaries to impose actual penalties, however, they can raise difficult questions about the necessity and proportionality of those penalties and the fairness of the process by which penalties are applied.[78]

IV. The Impact of Intermediary Liability and Direct Gatekeeping Obligations on Human Rights and Innovation

A. Freedom of Expression and Access to Information

Imposing liability or enforcement obligations on Internet intermediaries can significantly impair online free expression in a number of ways. Foremost among the risks to free expression is the likelihood of overblocking. When intermediaries are liable for or obligated to police content created by others, they will carefully screen and limit user activity in an effort to protect themselves. In doing so, they are likely to overcompensate, blocking even some lawful content out of an abundance of caution. Material that is controversial, likely to prompt complaints from powerful or litigious entities, or simply susceptible to being mistaken for unlawful material would be at greatest risk.

---

[75] France's Haute Autorité pour la Diffusion des Oeuvres et la Protection des Droits sur Internet (HADOPI, http://www.hadopi.fr/) is empowered to seek orders for ISPs to terminate the Internet accounts of repeat infringers. *See also* Nate Anderson, "France passes harsh anti-P2P three-strikes law (again)," *Ars Technica*, Sept. 15, 2009, http://arstechnica.com/tech-policy/news/2009/09/france-passes-harsh-anti-p2p-three-strikes-law-again.ars. As of July 2012, HADOPI had submitted 14 repeat-infringer cases to courts for judgment. *See* Megan Geuss, "French anti-piracy agency Hadopi only sued 14 people in 20 months," *Ars Technica,* Sept. 5, 2012, http://arstechnica.com/tech-policy/2012/09/french-anti-piracy-agency-hadopi-only-sued-14-people-in-20-months/. France's new President reportedly has suggested that he may seek to repeal or modify the law. *Id.*

[76] South Korea Copyright Act, art. 133-2, translation at http://hurips.blogspot.com/2010/10/facts-and-figures-on-copyright-three.html; New Zealand Copyright (Infringing File Sharing) Act of 2011, http://www.legislation.govt.nz/act/public/2011/0011/latest/whole.html?search=ts_act%40bill%40regulation%40deemedreg_copyright+act__25_h&p=1; UK Digital Economy Act of 2010 §§ 3–18, http://www.legislation.gov.uk/ukpga/2010/24/crossheading/online-infringement-of-copyright,

[77] Canadian Bill C-11 (Assented to June 29, 2012), http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=5697419&Mode=1&Language=E, § 47 (amending § 41 of the Canada's Copyright Act); Chilean Law 20,430 (modifying Law 17,336 on Intellectual Property), Diario Oficial D.O., May 4, 2010 (English translation available at https://www.cdt.org/files/file/ChileanLaw20430-ModifyingLaw17336.pdf) Article 85U.

[78] *See, e.g.*, French Constitutional Council, Décision n° 2009-580 DC, June 10, 2009, http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/2009/decisions-par-date/2009/2009-580-dc/decision-n-2009-580-dc-du-10-juin-2009.42666.html (ruling portions of France's original Hadopi law unconstitutional); *see also* Joint Statement of CDT and Public Knowledge, July 7, 2011, https://www.cdt.org/pr_statement/cdt-public-knowledge-joint-statement-copyright-alert-system.

Overblocking could also be triggered by takedown demands from government officials or private parties. Intermediaries facing legal exposure have powerful incentives to comply with takedown demands without question, even though some demands may be unwarranted or sent in bad faith. For the intermediary, the potential cost of resisting an overreaching attack on particular third-party content will almost always be greater than the cost of simply removing the content upon request.[79]

The end result is that online platforms become much less reliable as platforms for speech and more vulnerable to having legitimate expression curtailed. The risk of overblocking is especially high where obligations or definitions of illegal content are vague, or where assessing the content requires careful legal judgments.[80] The harder it is for intermediaries to tell precisely what content they have a legal obligation to block, the more they will have to err on the side of overblocking to ensure they are in full compliance.

The threat of liability and content-policing rules can also greatly diminish intermediaries' capacity and willingness to host content supplied by others. Internet services operate at tremendous speed and scale. These are among the medium's great strengths and are a big part of what makes it so revolutionary. But imposing new burdens on intermediaries can undermine their ability to take advantage of these strengths. To illustrate: Users post over seventy-two hours of video to YouTube every minute.[81] If the legal regime effectively compelled YouTube to manually examine each video before it could be posted online, YouTube could not continue to operate such an open and large-scale forum for user expression. The same is true of the countless forums, blogs, and social networks where users post hundreds or thousands of comments every hour. Non-manual forms of review, such as automatic filters, carry their own financial and operational costs—and can also lead to accidental takedown of legitimate content.[82] Faced with mandates to police all user content, websites and online services would pare back their user participation features substantially, and in many cases would probably eliminate them entirely.

Even for platforms that host a smaller volume of content, filtering, licensing, or enforcement obligations can have grave consequences. The marketplace for online services has flourished in large part because barriers to entry are so low. But new content policing mandates could impose significant new compliance costs on would-be innovators. Start-ups and smaller, niche services will often lack the resources to comply with such mandates. Saddling them with new costs would dramatically alter the competitive market for online services and reduce the availability of platforms for expression.

In the Web 2.0 era, the consequences of impairing interactive and participatory speech platforms would be severe. Interactive platforms have become vital not only to democratic participation but also to the ability of users to forge communities, access information, and discuss issues of public and private concern. The right to freedom of expression is an enabling right that facilitates the exercise of other rights: it is core to individual fulfillment, scientific

---

[79] *See* Villeneuve, "Evasion Tactics," *supra* note 31 (describing several case studies where notice-and-takedown systems were exploited to silence online critics).

[80] For example, Internet intermediaries are not well-positioned to determine whether particular content is defamatory. *See supra* note 40 and accompanying text.

[81] "It'sYouTube's 7th birthday . . . and you've outdone yourselves, again," *Official YouTube Blog*, May 20, 2012, http://youtube-global.blogspot.com/2012/05/its-youtubes-7th-birthday-and-youve.html.

[82] *See supra* note 72.

inquiry, and participation in economic and community development. In short, by creating rich and abundant avenues for communication, interactive platforms increase the capacity of individuals to fully participate in all aspects of social, political, and economic life. Intermediary liability and gatekeeping obligations threaten the potential of these tools.

Democratic countries must also be mindful of how well-intentioned policies that nonetheless reduce opportunities for expression will be perceived across the globe. Forcing Internet intermediaries to assume new roles in actively monitoring user communications sets a dangerous precedent, even if the immediate purposes (for example, identifying copyright infringement or extremist material) seem largely benign. Inevitably, authoritarian regimes will point to such actions to justify their own restrictive policies.[83] And if intermediaries develop and deploy the technological capability to police their own networks for unlawful content such as copyright infringement, those same technologies can be used to police networks for "unlawful" political dissent.

B. Privacy

Imposing liability or gatekeeping obligations on Internet intermediaries can seriously undermine user privacy. Intermediaries will feel compelled to actively police their services for unlawful content – which in turn may require them to broadly surveil their users' activities. For ISPs in particular, policing bad behavior will generally require broadly inspecting the Internet communications of users, including perfectly lawful private communications.[84] In addition, intermediaries taking on increasingly active enforcement roles may decide to collect more personal information about their users and retain this information for longer than they otherwise would have, to facilitate potential legal actions against offending users.

Pervasive surveillance of users' activities and extensive collection of users' data and would violate users' reasonable expectations of privacy in their use of online services. It would open the door to major abuses of seemingly private information by companies, litigants, computer hackers, or governments. It may also conflict with a country's privacy or data-protection laws.[85] And it can have a broad chilling effect on legitimate Internet activity and speech. If Internet users learn that their ISPs or other key intermediaries are monitoring and perhaps recording every step they take online, this could damage confidence in the medium and make users more reluctant to use the Internet for beneficial but sensitive purposes such as academic, financial, or

[83] *See* Letter from human-rights advocates to US Representatives Lamar Smith and John Conyers regarding H.R. 3261, the Stop Online Piracy Act, Nov. 15, 2011, https://www.cdt.org/files/pdfs/SOPA-letter-from-Intl-human-rights-community.pdf.

[84] For a discussion of the privacy consequences of ISPs employing "deep packet inspection" (DPI) technology to inspect and analyze users' online communications, see Alissa Cooper, "The Singular Challenges of ISP Use of Deep Packet Inspection," 2010, http://www.deeppacketinspection.ca/the-singular-challenges-of-isp-use-of-deep-packet-inspection/.

[85] Examples of such privacy laws include European national laws implementing the Data Protection Directive, 95/46/EC, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:NOT, and the US Electronic Communications Privacy Act, 18 U.S.C. ch. 119.

health services.[86] Similarly, some users may be reluctant to engage in robust online expression if intermediaries are tracking and retaining detailed personal information; speakers' ability to remain anonymous is a valuable enabler of online free expression.

C. Innovation and Economic Development

Intermediary liability and gatekeeping obligations discourage innovation in the information and communications technology (ICT) industry. Small companies and start-ups often cannot afford the expense of compliance staff and legal defense teams. The risk of major future liability based on the possible actions of users deters investment in the development of new ICT products and services.[87] So does the prospect of bearing significant financial costs for content policing, licensing, or enforcement activities. Implementing an automated filtering system, for example, requires an ISP or hosting platform to make upfront investments in hardware and software and then incur additional ongoing costs for maintenance and support costs, including personnel to handle questions and disputes. It also can degrade network performance, thus requiring additional infrastructure investment to reach the desired level of service performance or speed.

For all of these reasons, liability risk and enforcement obligations create new barriers to entry that can effectively close the market to start-ups. Moreover, innovative ICT businesses may choose to operate only in countries where ICT intermediaries are granted strong liability protections and do not face burdensome gatekeeping regulations or even the risk of arrest.[88] The result is less foreign direct investment and less ICT sector competition, innovation, and growth in those countries that do not grant such protections.[89]

Reducing ICT investment, innovation, and competition can impede economic development and

---

[86] For a discussion of the relationship between consumer trust and privacy, see CDT, Comments to the Department of Commerce NTIA Internet Policy Task Force: In the Matter of Information Privacy and Innovation in the Internet Economy, June 14, 2011, http://www.cdt.org/comments/comments-cdt-department-commerce-information-privacy; Department of Commerce (Internet Policy Task Force), *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, Dec. 16, 2010, http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf.

[87] A 2011 study found that increasing copyright liability on intermediaries would shrink early investment in Internet companies by up to 81%. Booz & Co., *The Impact of US Internet Copyright Regulations on Early-Stage Investment*, http://www.booz.com/media/uploads/BoozCo-Impact-US-Internet-Copyright-Regulations-Early-Stage-Investment.pdf.

[88] *See* Bradley Brooks and Juliana Barbassa, "Arrest of Google Brazil head stirs debate over Web," , September 27, 2012, ; *see also supra* note 22 (discussing prosecution of Google executives in Italy) and Kevin Bankston, "Shielding the Messengers: CDT Travels to Thailand to Argue Against Intermediary Liability," *CDT Policy Beta* blog, April 5, 2012, https://www.cdt.org/blogs/kevin-bankston/0504shielding-messengers-cdt-travels-thailand-argue-against-intermediary-liabil (discussing how weak intermediary liability protections discourage ICT investment).

[89] For example, one of the reasons Google gave for leaving China was the difficulty of managing the liability risks. *See* James Fallows, "An Interview with David Drummond of Google," *The Atlantic Online*, March 23, 2010, http://www.theatlantic.com/technology/archive/2010/03/an-interview-with-david-drummond-of-google/37896/. Moreover, one recent report found that despite heavy use of online services throughout Europe, the US, and Asia, US companies overwhelmingly dominate the market: About two-thirds of major Web 2.0 applications are provided by US companies. Europe (which has weaker protections for intermediaries that the US) holds around a ten percent share with respect to revenues and other innovation indicators (such as venture capital and R&D expenditures) in the Web 2.0 market. Sven Lindmark, *Web 2.0: Where does Europe stand?*, Joint Research Centre, Institute for Prospective Technological Studies, European Commission, 2009, p. 12, http://ftp.jrc.es/EURdoc/JRC53035.pdf. *See also* Study on the "Economic Impact of the E-Commerce Directive," *Copenhagen Economics*, Sept. 2007, Box 2.3 on page 22, http://ec.europa.eu/internal_market/e-commerce/docs/study/ecd/%20final%20report_070907.pdf.

growth more broadly.[90] Internet intermediaries facilitate growth across the economy in a range of ways.[91] They foster new opportunities for increasing productivity. They promote the efficient functioning markets by making better economic information more readily and cheaply available to businesses and consumers alike. They create new online marketplaces, like Amazon or eBay, which drive down transaction costs, create new distribution channels, increase competition, and lower prices. They can play a key role in economic development efforts by improving access to banking services and credit, connecting developing countries to global markets, and increasing access to educational resources.[92] Inhibiting ICT development or adoption undermines these functions and hence stifles the Internet's potential to promote broader economic gains.

V. Alternative Ways to Address Harmful and Unlawful Material Online

Some fear that providing broad protections for intermediaries will foster an explosion of harmful and unlawful content online, with little if any recourse. However, governments can take steps to address harmful and unlawful online activity while minimizing any undue impact on lawful expression and innovation.

A. Empowering or Educating Users

Governments can take steps to empower users to control what content reaches their screens. The market has produced a broad array of user empowerment tools that can help users themselves block content they deem undesirable or harmful (for example, pornography, hate speech, or materials promoting illegal activity).[93] Many ISPs offer such tools to customers for free or at low cost. Governments can, for example, promote the voluntary use of such tools by users or subsidize their purchase through vouchers. In the US, Section 230 includes an explicit

---

[90] A January 2012 study estimated that the activities of online intermediaries contributed 310 billion Euros to the European GDP – 160 billion directly, and 150 billion indirectly via productivity gains. The authors concluded that "these contributions to the economy would not be possible without the liability regime as it is currently designed. Consequently, any adverse changes to the liability regime – such as increased legal obligations on intermediaries – could have a chilling effect on innovation and the economic activity of online intermediaries, putting this value at risk." Martin H. Thelle and Svend Torp Jespersen, "Online Intermediaries: Assessing the Economic Impact of the EU's Online Liability Regime," *Copenhagen Economics*, January 2012, http://www.europeandigitalmedia.org/uploads/Press/documents/Copenhagen%20Economics-Online%20Intermediaries-201201.pdf.

[91] *See* Organization for Economic Co-operation and Development, *The Economic and Social Role of Internet Intermediaries*, DSTI/ICCP(2009)9/FINAL, April 2010, pp. 37–40, http://www.oecd.org/dataoecd/49/4/44949023.pdf.

[92] A 2006 World Bank study highlighted the empirical evidence of ICT's "vital role in advancing economic growth and reducing poverty," citing the growing consensus around ICT's importance for global integration, public sector effectiveness, as well the positive link between ICT and investment and trade. The World Bank, *Information and Communications for Development 2006: Global Trends and Policies*, xi, p. 4, http://info.worldbank.org/etools/docs/library/240327/Information%20and%20communications%20for%20development%202006%20%20global%20trends%20and%20policies.pdf. *See also* The World Bank, *Information and Communications for Development 2009: Extending Reach and Increasing Impact*, July 2009, p. 14, http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/EXTIC4D/0,,contentMDK:22229759~menuPK:5870649~pagePK:64168445~piPK:64168309~theSitePK:5870636,00.html (concluding that broadband also "has a significant impact on growth and deserves a central role" in development strategy).

[93] Adam Thierer, *Parental Controls & Online Child Protection: A Survey of Tools and Methods*, http://www.pff.org/parentalcontrols. *See also* GetNetWise, Tools for Families, http://kids.getnetwise.org/tools/.

policy statement encouraging the development of user-controlled filtering and blocking technologies, as well as a provision requiring ISPs to notify new subscribers about the availability of such tools.[94]

The key feature of this approach is *user* control: empowering users to select and tailor technological tools according to their own needs and preferences. Where users have sufficient control to protect against whatever content they consider offensive or unsafe for themselves or their children, the government need not step in.[95] In contrast, any government-mandated technology may ultimately be less effective,[96] intrude on individual autonomy, and raise concerns around transparency and politically motivated content restrictions.[97]

Internet intermediaries may play a useful role not only by informing users about empowerment tools, but also by educating or warning users about the risks or legal obligations users face online. This is particularly true in the area of copyright, where making lasting progress against infringement will likely require convincing many users to modify their behavior. As discussed above, Canada and Chile have passed laws calling on ISPs to forward warning notices to users that copyright holders believe are engaging in infringement.[98] Many US ISPs have been forwarding warning notices to users for some time, and a private "Copyright Alert System" worked out between US-based ISPs and major copyright-holders seeks to build on this model.[99] When ISPs forward warnings from copyright holders to users, this informs the users that their behavior carries more legal risk than they may have realized.[100] It may even alert some users to behavior that they were not aware of, such as unlawful activity traceable to the user's children, a botnet infection, or interlopers on an unsecured wireless connection.

This is not to say that informational measures are inevitably benign. There is a possibility that skewed or incomplete information could paint an inaccurate picture of copyright or other relevant laws, misinforming the public rather than educating it. There is likewise a possibility that

---

[94] 47 U.S.C. 230(b)(3)-(4), (d).

[95] User-controlled tools may have limited effectiveness, however, in reducing access to content that users affirmatively want to receive, as may be the case with respect to material that infringes copyright.

[96] The development of effective user empowerment tools is unlikely to keep pace with the rate of technological change unless there is an open and competitive market for such tools for users to choose from, which will drive innovation and continuous improvement in these tools.

[97] The proposed Green Dam/Youth Escort initiative in China in 2009 illustrates these concerns. *See* Rebecca MacKinnon, "Green Dam is breached…. Now what?", *RConversation*, July 2, 2009, http://rconversation.blogs.com/rconversation/2009/07/green-dam-is-breachednow-what.html.

[98] *Supra* note 77.

[99] Center for Copyright Information, Memorandum of Understanding, http://www.copyrightinformation.org/sites/default/files/Momorandum%20of%20Understanding.pdf. *See also* David Sohn, "ISPs and Copyright Owners Strike a Deal," *CDT PolicyBeta* blog, Jul. 7, 2011, https://www.cdt.org/blogs/david-sohn/isps-and-copyright-owners-strike-deal. Crucially, the ISPs participating in the Copyright Alert System have committed to educational and mitigation measures that stop short of terminating a user's Internet connection. *See* Jill Lesser, The Copyright Alert System: Moving to Implementation, Oct. 18, 2012, http://www.copyrightinformation.org/node/709 ("[T]ermination of a consumer's Internet service is not a part of any ISP's Copyright Alert System program. Contrary to many erroneous reports, this is not a "six-strikes-and-you're-out" system that would result in termination. There's no "strikeout" in this program.").

[100] A 2007 Canadian study found notices effective at deterring infringement. *See* "E-mail warnings deter Canadians from illegal file sharing," *CBC News*, Feb. 15, 2007, http://www.cbc.ca/consumer/story/2007/02/14/software-warnings.html.

overaggressive warnings could discourage recipients from engaging in fair use or other legitimate activities. Nonetheless, educational efforts have the potential to play a positive role in shaping public understanding, expectations, and norms in ways that discourage illegal and harmful online activity.

B. Law Enforcement and Victim Recourse

Law enforcement officials should be able to investigate and pursue criminal wrongdoers, and victims should have the right to pursue legitimate individual claims against the parties who actually posted the content that has caused them harm. Under existing frameworks that protect intermediaries, protection is granted *only* to the intermediary, not the parties that originally created or disseminated the unlawful content. Thus, strong intermediary safe harbors are perfectly consistent with legal actions by law enforcement agencies or victims against the original creator of unlawful content.

There can be practical challenges to pursuing such legal actions, but they are not insurmountable. Anonymity online is never complete and many activities leave digital traces. One proper role for intermediaries might be to help law enforcement or private litigants follow those traces and identify users – even anonymous and pseudonymous users – in response to legitimate court orders, with procedures in place to safeguard privacy and the threshold right of anonymity.[101] Of course, such a role would be appropriate only in countries with strong rule-of-law protections – including transparent and accessible enactment of law, fair process for applying and enforcing the law, and independent review of enforcement decisions.[102] In countries where such protections are absent or weak, government officials and courts would be unlikely to strike an appropriate balance among privacy, anonymity, and law enforcement.

C. Empowering or Encouraging Voluntary Enforcement Actions by Internet Intermediaries

Governments may seek to encourage Internet intermediaries to take voluntary action to control harmful or unlawful online content. For example, as discussed in Section II.B above, Section 230 in the US protects intermediaries from liability for voluntarily removing content they deem objectionable. In addition, in recent years US authorities have affirmatively encouraged private parties to negotiate cooperative, multi-party agreements under which categories of intermediaries (e.g., large ISPs) jointly pledge to "act as check points for infringing activity and reduce the distribution of infringing content."[103]

Promoting voluntary enforcement action by private intermediaries has some advantages, but also carries significant risks. The principal advantage is that voluntary approaches are flexible. They do not burden existing services and future innovators with government mandates that in some contexts may prove technically infeasible, too costly, awkward to implement, invasive of privacy or other user interests, or simply ineffective. Different intermediaries can tailor their

---

[101] In civil litigation, there are mechanisms for identifying online speakers, but courts can impose procedural safeguards. For example, before breaching anonymity in the US, courts usually require that plaintiffs establish that they have a strong case and that the need to pierce anonymity is not outweighed by the right to anonymous speech that is protected by the US Constitution. *See, e.g., Dendrite Int'l v. Doe*, 775 A.2d 756 (N.J. App. Div. 2001).

[102] *See* World Justice Project, *What is the Rule of Law?*, http://worldjusticeproject.org/what-rule-law.

[103] 2011 US Intellectual Property Enforcement Coordinator Annual Report on Intellectual Property Enforcement, Mar. 2012, p. 46, http://www.whitehouse.gov/sites/default/files/omb/IPEC/ipec_annual_report_mar2012.pdf.

approaches to their specific circumstances. They can also respond to changing circumstances much more easily than when their actions are dictated by legal rules or court orders.

On the other hand, voluntary, non-governmental enforcement schemes lack the established safeguards that apply to government processes in most democratic countries. Voluntary action by private intermediaries may be less transparent than government action, making it more difficult for affected parties to evaluate and respond reasonably to whatever actions are taken. There is less of an obligation to follow fair procedures, including recourse for erroneous decisions.[104] There is less substantive protection for individual rights such as freedom of expression, association, or privacy. There is less accountability, since private intermediaries are not subject to democratic checks and balances. Finally, there is a risk that nominally voluntary enforcement may provide a vehicle for government to circumvent legal constraints on its action and achieve through indirect pressure things it would be prohibited from doing directly.[105] All of these risks are compounded in countries where enforcement of the law is arbitrary or vulnerable to corruption, and procedural safeguards are weak; in such contexts, currying favor with the government may require intermediaries to sign "voluntary" self-regulation pledges that are neither truly voluntary nor respectful of users' preferences and rights.[106]

One important factor in evaluating voluntary action by intermediaries is the extent of the potential impact on users. Measures aimed at educating users, for example, need not significantly impair anyone's rights even if they are applied in a somewhat imprecise or overbroad manner. By contrast, voluntary actions that impose concrete sanctions on individuals, entities, or websites effectively put private parties into a quasi-judicial role. At a minimum, this makes strong safeguards essential. Especially serious are voluntary actions that directly interfere with user's communications, such as by restricting users' Internet access or blocking access to particular websites. These types of voluntary actions can impose major burdens on free expression rights – the rights both to impart and receive information.

It is also important to distinguish independent, voluntary actions by individual intermediaries from actions that are based on a broadly adopted common framework. There has been a trend towards formalizing and standardizing private action through voluntary industry-wide or multi-stakeholder frameworks. Indeed, the OECD in 2011 endorsed "multistakeholder co-operation" as a successful model for Internet policymaking generally.[107]

Industry-wide or multi-party approaches may offer an opportunity to develop sound best practices. Ideally, the resulting actions would be less ad hoc, more fair, and more broadly understood and accepted. Broad participation may also make multi-party frameworks more

---

[104] *See* European Digital Rights, *The Slide from 'Self-Regulation' to Corporate Censorship, supra* note 32, p. 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).

[105] *See* Ian Brown, "Internet self-regulation and fundamental rights," *Index on Censorship* 1, Mar. 2010, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1539942 (arguing that self-regulatory actions "are often introduced under the threat of legislation or litigation, agreed and operated behind closed doors 'in the shadow of the law'").

[106] *See*, e.g,, China's various iterations of a "Public Pledge on Self-Discipline for the Chinese Internet Industry," described in Human Rights Watch, Race to the Bottom: Corporate Complicity in Chinese Internet Censorship, Aug. 2006, p. 12, http://www.hrw.org/en/node/11259/section/6.

[107] OECD, *Communiqué on Principles for Internet Policy-Making,* June 28–29, 2011, p. 4, http://www.oecd.org/internet/innovation/48289796.pdf.

effective at achieving their goals than uncoordinated action by individual intermediaries.

A common framework, however, also magnifies the risks. Any users unfairly harmed by private action may have nowhere to turn for relief if the entire industry is following the same approach. Perhaps even more important, industry-wide and multi-stakeholder frameworks are to some extent stand-ins for government action; they carry broad impact and may address questions that, but for the voluntary framework, would have commanded more government attention. The more multi-party voluntary agreements stand in for government action, the more they raise questions about the legitimacy of whatever rules and decisions they adopt.[108]

At a minimum, therefore, any joint framework for private, voluntary action should seek to emulate key aspects of democratic, government-based process. It should be formulated with input from all interested stakeholders, including Internet users. It should adhere to principles such as due process, transparency, and respect for free expression and privacy. It should target only egregious and straightforward cases of unlawful activity. It should provide the opportunity to respond to allegations and to appeal decisions. And it should consider a wide range of factors including potential hardship, unintentional violations, and impact on innocent third parties.

In sum, there may be ways that some Internet intermediaries can help address unlawful or harmful online content through private, voluntary action. But drawing the line between constructive private action and risky vigilantism is a crucial challenge. So is drawing the line between governmental encouragement of voluntary action and more aggressive forms of government pressure or threats that effectively coerce private action and amount to indirect regulation. Voluntary initiatives, and government efforts to encourage them, should be approached with caution.

D. Enforcement by Financial Intermediaries ("Follow the Money")

Another possible approach is to call for action by *financial* intermediaries, such as payment processors and ad networks. This approach could be preferable in some respects to measures relying on Internet intermediaries, but it carries significant risks as well.

If a criminal website cannot make money – either through payments from users or from advertisers – then it likely cannot operate at a substantial scale.[109] Several examples, including US legislation regarding online gambling and the ongoing effort to stop commercial spammers, illustrate the potential effectiveness of an approach targeting offenders' money flows.[110]

---

[108] CDT explored some of the key legitimacy-related question raised by multistakeholder organizations in CDT, *Multistakeholder Organizations, Legitimacy, and Rights: A Supplementary Research Agenda,* Feb. 2012, https://www.cdt.org/files/pdfs/Multistakeholder-Organizations-And-Legitimacy.pdf.

[109] *See* Mark McCarthy, "What Payment Intermediaries Are Doing About Online Liability and Why It Matters," 25 *Berkeley Journal Technology Law Journal* 1039, July 5, 2010, http://www18.georgetown.edu/data/people/maccartm/publication-47784.pdf.

[110] The Unlawful Internet Gambling Enforcement Act, which bars payment networks from processing illegal gambling transactions, has effectively denied gambling websites access to the US market (*see* 31 U.S.C. §§ 5361–5367). Computer scientists analyzing spam found that credit card payment systems offer a viable chokepoint for controlling spam whereas technical filtering and blocking efforts have failed (*See* John Markoff, "Study Sees Way to Win Spam Fight," *New York Times*, May 19, 2011, http://www.nytimes.com/2011/05/20/technology/20spam.html). For a review of other payment-network efforts to fight illegal online activity, see McCarthy, *supra* note 109.

Moreover, financial blockades generally are more difficult to circumvent than blocking or filtering by Internet intermediaries.[111]

Focusing on the business relationships that enable sites to profit from illegal activity may avoid some of the negative side effects of focusing on the communications infrastructure. For example, "follow the money" remedies do not interfere with the Internet's addressing system or other technical architecture, and therefore can avoid unintended technical consequences such as undermining cybersecurity or balkanizing the global Internet.[112]

If applied too broadly, however, financial sanctions could seriously undermine free expression. The impact of cutting off a website operator's revenue can be severe. For example, in October 2011, Wikileaks announced that it was suspending all publishing because of the financial blockade against it,[113] illuminating the significant speech implications of allowing financial intermediaries to decide such difficult questions.

Moreover, the threat of financial cutoff could prompt websites and online services to engage in substantial self-censorship. For example, for a brief time earlier this year, the financial intermediary PayPal threatened to cut off its services to an e-book platform unless it removed books with certain categories of sexual content.[114] This would have forced the platform and its authors to censor lawful content in order to avoid losing access to an important sales channel. PayPal wisely changed course, but the episode demonstrates that threatening websites and online services with private financial sanctions based on their users' behavior can chill online speech in much the same way as threatening to impose liability for it.

These are risks that would need to be carefully addressed before any effort to encourage financial intermediaries to take action against unlawful or harmful content. At a minimum, there would need to be careful process to ensure that financial sanctions are used only against true bad actors in egregious and straightforward cases, while carefully avoiding more complicated situations where lawful and unlawful content are comingled. There would also need to be ample legal process and safeguards to protect against mistakes.

---

[111] Websites can cycle through domain names or IP addresses rapidly and build simple software tools to evade Internet filters. Bypassing the established financial system is not so trivial. Users rely on a relative handful of major payment networks; the overwhelming majority of users will not be willing to enter into transactions when these customary payment options are not available, and a website cannot rapidly cycle through banking relationships with anywhere near the ease, speed and frequency with which it can cycle through domain names. Nor can it repeatedly shrug off the loss of access to major ad networks without a significant hit to its bottom line.

[112] *See Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites, Part I: Hearing before the Subcommittee on Intellectual Property, Competition, and the Internet of the House Comm. on the Judiciary*, 112th US Congress, 1st Session, (2011) (statement of David Sohn, Senior Policy Counsel, Center for Democracy & Technology), http://judiciary.house.gov/hearings/pdf/Sohn03142011.pdf.

[113] Hayley Tsukayama, "WikiLeaks stops publishing, cites low funds," *Washington Post*, Oct. 24, 2011, http://www.washingtonpost.com/business/technology/wikileaks-stops-publishing-cites-low-funds/2011/10/24/gIQAAwtcCM_story.html. Notably, technical efforts to censor WikiLeaks – relying on Internet intermediaries rather than financial ones – had shown little if any lasting impact. *See* Ravi Somaiya, "Hundreds of WikiLeaks Mirror Sites Appear," *New York Times*, Dec. 5, 2010, http://www.nytimes.com/2010/12/06/world/europe/06wiki.html?_r=1&ref=world.

[114] *See* Mark Coker, "PayPal Revises Policies to Allow Legal Fiction," *Smashwords Official Blog*, Mar. 13, 2012, http://blog.smashwords.com/2012/03/paypal-revises-policies-to-allow-legal.html; CDT, PayPal Changes Course After Censorship Controversy, Mar. 13, 2012, https://www.cdt.org/pr_statement/paypal-changes-course-after-censorship-controversy.

VI. Conclusion

Protecting Internet intermediaries from both liability and gatekeeping obligations with regard to content posted or transmitted by others is critical for preserving the Internet as a uniquely accessible medium for free expression. It supports widespread public access to information, innovation in information and communications technology, and economic development. User-generated content sites in particular have become vital forums for all manner of expression, from economic and political participation to forging new communities and interacting with family and friends. If liability concerns and content- and user-regulation requirements force private intermediaries to close down or sharply restrict these forums, then the expressive and economic potential of ICT technologies will be diminished. Governments everywhere should adopt policies that protect Internet intermediaries as critical actors in promoting innovation, creativity, and human development.

About the Center for Democracy & Technology // www.cdt.org
The Center for Democracy & Technology is a non-profit public interest organization working to keep the Internet open, innovative, and free. With expertise in law, technology, and policy, CDT seeks to enhance free expression and privacy in communications technologies. CDT is dedicated to building consensus among all parties interested in the future of the Internet and other new communications media.

For more information, please contact: **Kevin Bankston, Director of CDT's Free Expression Project, kbankston@cdt.org**
David Sohn, Director of CDT's Copyright and Technology Project, dsohn@cdt.org
Andrew McDiarmid, Senior Policy Analyst, amcdiarmid@cdt.org