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

INTERMEDIARY LIABILITY: PROTECTING INTERNET PLATFORMS FOR EXPRESSION AND INNOVATION

April 2010

This paper examines the impact of intermediary liability on free expression, privacy, and innovation. Intermediary liability arises where governments or private litigants can hold technological intermediaries such as ISPs and websites liable for unlawful or harmful content created by users of those services. The threat of liability inhibits the willingness of intermediaries to host user-generated content; such liability leads intermediaries to block even legal content and could inhibit innovation. Individual users should be held responsible for their unlawful actions, but if the threat of liability discourages Internet intermediaries from allowing users to communicate in the first place, then the opportunities for even lawful expression will be curtailed and the potential of networked technologies will be diminished. Protecting intermediaries from liability for the actions of third parties expands the space for online expression, encourages innovation in the development of new services, and creates more opportunities for local content, thereby supporting development of the information society. Internet advocates everywhere should urge governments to adopt policies that protect intermediaries as critical platforms for innovation and cultural and civic expression.

The global Internet has become a vibrant and essential platform for economic activity, human development, and civic engagement. Every day, millions of journalists, educators, students, business people, scientists, government officials, politicians, and ordinary citizens go online to speak, access information, and participate in nearly all aspects of public and private life. Internet service providers (ISPs),[1] telecommunications carriers, websites, online services, and a range of other technological intermediaries play critical roles in getting information and ideas from one corner of the online world to another.[2] These intermediaries provide valuable forums for expression, from the political to the mundane – forums that are open, up-to-the-minute, and often free of charge.

The openness of the Internet means, of course, that some users will post content or engage in activity that is unlawful or otherwise offensive. Depending on applicable national law, liability for online content can arise in a number of situations, both legitimate and politicized, including for defamation, obscenity, invasion of privacy, intellectual property infringement, or because the content is critical of the government. This reality raises important policy questions that have an impact on the growth of the online environment: Specifically, should technological intermediaries such as ISPs be held liable for content posted by their users and other third parties?

---

[1] We use the term “Internet service providers” to refer to providers of Internet access.

[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.

This paper examines the impact of intermediary liability on innovation, economic development, and human rights. It concludes that, while users should remain responsible for their unlawful online activities, policies protecting intermediaries from liability for content posted by third parties will expand the space for expression and innovation and better promote the Internet as a platform for a wide range of beneficial activities. If, in contrast, private intermediaries are discouraged from allowing users to post content because of liability concerns, then opportunities for speech will be greatly diminished and the full benefits of the information society will remain unrealized. The history of the Internet to date shows that providing broad protections for intermediaries against liability is vital to the future of the Internet.

I. Roles of Intermediaries and Sources of Liability

The Internet and mobile technologies have amplified the ability of individuals to speak and access information in unprecedented ways. This effect is especially true in the Web 2.0 era, where user-generated content platforms allow individuals with little technical knowledge or money to create, reproduce, disseminate, and respond to content in a variety of formats and with a worldwide audience.[3]

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 newspaper's website.
- A doctor makes a video in a local language 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** provide the physical and technical infrastructure for transmission of information.
- **Access providers/ISPs** provide users with access to the Internet.
- **Website hosting companies** rent website space to users for web pages, including for interactive forums.

[3] These Web 2.0, user-generated content platforms are also often referred to as the "participative web," "participative networked platforms," and "interactive media."

- **Online service providers**:
    - Blog platforms
    - Email service providers
    - Social networking websites
    - 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, traditional media like newspapers with websites that allow for user comment

Sources of intermediary liability – direct regulation and exposure to civil litigation

The Internet developed and flourished because of an early U.S. and European policy framework based on competition, openness, innovation, and trust. This framework places power not in the hands of centralized gatekeepers, but in users and innovators at the edges of the network. Importantly, this approach provides broad protections from liability for ISPs, web hosts and other technological intermediaries for unlawful content transmitted over or hosted on their services by third parties (such as users).

Increasingly, however, this policy is being eroded as governments – democratic and authoritarian alike – struggle to address illegal, harmful, or otherwise socially or politically undesirable content online: obscenity, defamation, hate speech, intellectual property infringement, or (more problematically) unpopular speech and speech that is critical of the government.

For governments, each of the intermediaries in the examples above represents a potential point of control over content or unlawful behavior. Because the Internet as it currently exists enables relatively anonymous or pseudonymous speech, it is often difficult or time consuming to identify individual users who post illegal or otherwise offensive content. The bad actor also may simply be out of the government's jurisdictional reach. In contrast, commercial intermediaries that host or transmit the content are much easier to identify and may already be subject to various registration or licensing requirements. Thus, some governments impose legal liability on intermediaries as a way to control content or address bad behavior online. In essence, these policies delegate the task of policing content to the private intermediaries. If an intermediary faces legal responsibility for content hosted, transmitted, or disseminated through its services, it will be forced to scrutinize and limit user content.

Private actors can also threaten expression and innovation online if they can bring civil lawsuits against the intermediaries that host or disseminate expression that the private parties seek to suppress. Thus, it is important to consider laws of civil liability that define the ability of litigants to seek private damages against intermediaries for content posted by others (for example, in defamation or privacy actions). Intermediaries are particularly vulnerable to private action not only because they are easier to identify and reach than individual users, but also because they

are often more able to pay damages than the actual creator of the content. 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 action.

To be clear, the reasons in favor of protecting intermediaries from liability are premised on the notion that the intermediaries themselves did not create the illegal content. As we will discuss in detail below, some countries that provide broad immunity to intermediaries impose various requirements that intermediaries must meet to qualify for immunity. However, these requirements raise their own issues and must be carefully calibrated.

II. Impact of Intermediary Liability on Human Rights and Innovation

Freedom of expression and other rights

When intermediaries are liable for the content created by others, they will strive to reduce their liability risk. In doing so, they are likely to overcompensate, blocking even lawful content. In this way, intermediary liability chills expression online and transforms technological intermediaries into content gatekeepers. Examination of the practices in countries that impose liability on intermediaries demonstrates that such indirect methods of control are as dangerous for free expression and other rights as direct government censorship.

First, holding intermediaries broadly liable for user content greatly chills their willingness to host *any* content created by others. Liability creates strong incentives to screen user content before it is posted online, creating an indirect prior restraint on speech and inevitably leading to less user-generated content overall. In some instances, entire platforms for expression simply could not exist because the sheer volume of content would make it impossible or economically unviable for the company to screen all user-generated content. To illustrate: Users post over twenty-four hours of video to YouTube every minute.[4] If liability concerns compelled YouTube to examine each video before being posted online, YouTube could not continue to operate as an open forum for user expression. The same is true of the countless forums and blogs where users post hundreds or thousands of comments every hour.

In the Web 2.0 era, the consequences of intermediary liability for expression would be severe. Interactive platforms like YouTube, bulletin boards, and social networking sites have become vital not only to democratic participation but also to the ability of users to forge communities, access information instantly, 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 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 threatens the potential of these tools.

Intermediary liability also creates another problematic incentive: Intermediaries will tend to over-block content and self-censor, especially where definitions of illegal content are vague and overbroad. In the face of threatened liability, intermediaries will err on the side of caution in

[4] "YouTube has 24 hours of video uploaded every minute," Reuters MediaFile, March 17, 2010, http://blogs.reuters.com/mediafile/2010/03/17/youtube-has-24-hours-of-video-uploaded-every-minute/; YouTube Fact Sheet, http://www.youtube.com/t/fact_sheet.

deciding what may be allowed. Likewise, when a government official or private litigant demands that a company take down content, intermediaries commonly take the path of least resistance and simply comply with the request rather than challenge or defend against the order in court. This incentive is especially strong (and can cause particular damage) when intermediaries are not able to easily determine if the content is unlawful on its face.[5] And because intermediaries have little incentive to challenge a removal request, intermediary liability also allows room for abuse on the part of the government or private litigant seeking to take down content for unscrupulous reasons.[6] The cost to the intermediary to resist an overreaching attack on particular content will almost always be greater that the cost of simply removing the content.

Finally, the risk of liability creates incentives for intermediaries to monitor their users more extensively, which raises a number of privacy concerns. In order to control their networks, intermediaries may believe that it is necessary to collect more personally identifiable information about their users and to retain this information for longer than they otherwise would. Intermediaries such as ISPs may also decide to surveil their users' Internet usage. Expanded data collection by ISPs about their customers and their online behavior raises serious privacy concerns because such information could end up in the hands of government or private litigants or be misused in other ways.

Innovation and economic development

Intermediary liability also creates disincentives for innovation in information and communications technologies (ICTs). Without protection from liability, companies are less likely to develop new ICT products and services. The threat of liability will also tend to close the market to start-ups, which are often unable to afford expensive compliance staffs. The threat of liability may thereby entrench existing market players, who will be less driven to innovate or improve upon existing business models. Many businesses may simply choose to operate only in countries where ICT intermediaries *are* granted broad liability protections, resulting in less foreign direct investment in those countries that do not grant such protections.

In turn, this harm to innovation can impede economic development and growth more broadly. Efficient and productive markets depend on the free exchange of economic information among businesses and consumers. Internet intermediaries directly contribute to economic growth in a range of ways:[7] The Internet has increased the amount of economic information available to businesses and consumers alike and lowered the costs of accessing such information. Online marketplaces like Amazon or eBay also drive down transaction costs, create new distribution channels, increase competition, lower prices, and help connect global markets. Intermediary liability tends to create barriers to information exchange and inhibit many of these market

[5] For example, while a private party may allege that certain content is defamatory or infringes copyright, such determinations are usually made by judges and can involve factual inquiry and careful balancing of competing interests and factors. ISPs and online service providers are not well-positioned to make these types of determinations.

[6] *See* Nart Villeneuve, "Evasion Tactics: Global online censorship is growing, but so are the means to challenge it and protect privacy," Index on Censorship, Vol. 36, Issue 4 (Nov. 2007), pp. 74–76 (describing several case studies where notice and takedown systems were exploited to silence online critics), http://www.nartv.org/mirror/evasiontactics-indexoncensorship.pdf.

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

benefits. Moreover, ICT development can play a key role in economic development efforts – for example, in improving access to banking services and credit, connecting developing countries to global markets, and increasing access to educational resources.[8] Inhibiting ICT development or adoption will limit many of these broader economic benefits.[9]

III. Approaches to Intermediary Liability

The question of who can be held liable for harmful or illegal content arose early in those countries with broad Internet adoption. In looking at various national and regional approaches, we can observe a general trend: Those governments that have sought to maximize growth of 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.

United States

Two separate laws embody U.S. policy on intermediary liability: Section 230 of the Communications Act and Section 512 of the Copyright Act.[10]

The U.S. Congress enacted what is now known simply as "Section 230" to advance three policy goals: 1) to promote the continued rapid and innovative development of the Internet and other interactive media; 2) to remove disincentives to voluntary self-screening of content by service providers; and 3) to promote the development of tools (like filters) that maximize user control over what information the user receives online.[11] To advance the first goal, Section 230 gives

---

[8] 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. *Information and Communications for Development 2006: Global Trends and Policies*, xi, p. 4, The World Bank (also citing "[a] recent survey of 56 developed and developing countries found a significant link between Internet access and trade growth"), http://info.worldbank.org/etools/docs/library/240327/Information%20and%20communications%20for%20development%202006%20%20global%20trends%20and%20policies.pdf. *See also Information and Communications for Development 2009: Extending Reach and Increasing Impact*, p. 14, The World Bank (July 2009) (concluding that broadband also "has a significant impact on growth and deserves a central role" in development strategy), http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/EXTIC4D/0,,contentMDK:22229759~menuPK:5870649~pagePK:64168445~piPK:64168309~theSitePK:5870636,00.html, and *World Development Report: Building Institutions for Markets*, p. 193, The World Bank (2002), http://www-wds.worldbank.org/external/default/WDSContentServer/IW3P/IB/2001/10/05/000094946_01092204010635/Rendered/PDF/multi0page.pdf (*see generally* chapter 10 "The Media," pp. 181-193).

[9] Internet-curtailing nations may face charges that barriers to Internet access violate international trade obligations. The European Parliament, for example, has called for using trade agreements to challenge restrictions on Internet free expression. European Parliament resolution of 19 February 2008 on the EU's Strategy to deliver market access for European companies (2007/2185(INI)), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+20080219+ITEMS+DOC+XML+V0//EN&language=EN#sdocta18. While this approach would likely be used first against direct censorship, it may one day also be applied to indirect means of excluding speech.

[10] In addition to these statutory provisions, intermediary protection may derive from the Constitution's protection of free expression. U.S. courts also have created a safe harbor from copyright infringement liability for producers and distributors of technology products under certain circumstances: 1) the product must have substantial non-infringing (that is, lawful) uses, and 2) the distributor must not have actively encouraged infringing uses of its product. *Sony v. Universal Studios*, 464 U.S. 417 (1984); *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster*, Ltd., 125 S. Ct. 2764 (2005).

[11] 47 U.S.C. § 230, http://www.law.cornell.edu/uscode/47/230.html.

intermediaries[12] strong protection against liability for content created by third party users.[13] Section 230 has been used by interactive online services as a screen against a variety of claims, including negligence, fraud, violations of federal civil rights laws, and defamation.[14] It is precisely these protections that led to the dramatic growth of social networking and other interactive, user-generated content sites that have become vibrant platforms for expression in the U.S. and all over the world. Without Section 230, entry barriers for new Internet services and applications that allow user-generated content would be much higher, dampening the innovation we have seen in interactive media.

U.S. copyright law takes a slightly different approach, but one that still limits the scope of liability for copyright infringement for certain types of intermediaries. Section 512 of the Digital Millennium Copyright Act (DMCA) provides a "safe harbor" for online service providers from claims of copyright infringement made against them that result from the infringing conduct of their customers, but only if the service providers meet certain criteria.[15] A broad range of service providers can benefit from this safe harbor, including ISPs, search engines, and content hosting services.[16] The criteria that service providers must meet to qualify for the safe harbor vary depending on the type of provider, but include, for example, taking down infringing material when notified by the copyright owner of its presence on the provider's service.[17] If a service provider meets the relevant requirements, only the individual infringing customer may be subject to liability; if the provider doesn't satisfy the requirements, it loses its safe harbor.[18] The DMCA also provides that this safe harbor is not conditioned on providers' monitoring or affirmatively investigating unlawful activity on their networks.[19] U.S. policymakers have thus sought to strike a balance between protecting the rights of copyright holders and promoting innovation in ICT tools and services.

Section 230 and Section 512 of the DMCA represent two distinct approaches to intermediary liability protection:

- Section 230 provides broad immunity for a variety of claims, with no condition that intermediaries implement a system to take down unlawful content once notified of it ("notice and takedown") in order to qualify.

---

[12] Section 230 calls these intermediaries "interactive computer services." 47 U.S.C. 230(c)(1).

[13] 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).

[14] *See*, for example, Center for Democracy & Technology, "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.

[15] 17 U.S.C. 512, http://www4.law.cornell.edu/uscode/17/512.html. For a good overview of the DMCA, see Frequently Asked Questions (and Answers) about DMCA Safe Harbor, http://www.chillingeffects.org/dmca512/faq.cgi. For example, a content hosting provider must, among other things, take down infringing material when notified of its presence on the provider's network by the copyright owner; must not have known about the infringement (or must take down the content if it becomes aware of the activity); and must not receive direct financial benefit from the infringing activity where the provider is able to control the activity. 17 U.S.C. 512(c).

[16] 17 U.S.C. 512(a) – (d).

[17] This is known as "notice and takedown."

[18] Losing safe harbor under the DMCA, however, does not necessarily mean that the intermediary is automatically liable for the third party content. The copyright holder must still prove secondary liability in court.

[19] 17 U.S.C. 512(m).

- In contrast, Section 512 of the DMCA provides protection only against copyright claims and requires certain service providers to employ a notice and takedown system to qualify.[20]

Requiring intermediaries to implement a notice and takedown system is one way to ensure that intermediaries are not actively engaging in or encouraging the unlawful behavior occurring on their services. However, this approach also raises several issues:

- Notice and takedown systems are vulnerable to abuse by both governmental and private actors, who might issue fraudulent or bad-faith notices to chill critics or for other unscrupulous purposes. Users who are notified by the service provider that their content has been flagged as unlawful often have little recourse or few resources to challenge the takedown and seek re-posting of their content.[21]

- Intermediaries have little or no incentive to challenge a takedown request, even if they suspect the notice and takedown system is being abused. The question of whether particular content is actually illegal may involve a factual inquiry, careful balancing of competing interests, and consideration of defenses. Rather than make these judgments, intermediaries will normally not risk liability – they will simply take down the material as soon as they receive the request to do so.

Advocates have documented how these drawbacks can chill free expression.[22] While U.S. copyright law provides some penalty for misuse of the notice and takedown process, the high costs of challenging a notice in court may prevent many users from doing so, diminishing any deterrent effect these penalties might have against abuse.[23]

Section 230's approach, on the other hand, does not encourage overly cautious gatekeeping by service providers. Service providers are under no obligation to take down material, hence there is no need for them to over-comply in ways that could chill legitimate expression. This is not to say that Section 230 provides no incentive for service providers to remove objectionable content from their networks and services. Indeed, there is another, often-overlooked benefit to the approach taken in Section 230: Section 230 may actually serve the very interests that its detractors seek to advance – the interests of limiting online crime and the dissemination of offensive content. As noted above, Section 230 not only protects intermediaries from liability for content posted by users, it also protects intermediaries from liability when they block or take down content they believe is inappropriate. This second rule supports, for example, the anti-spam and cybersecurity efforts of ISPs, allowing them to block traffic that they believe is spam or contains harmful code, so long as they act in good faith.

---

[20] The EU takes a similar approach in requiring intermediaries to implement a notice and takedown system to be eligible for immunity for a range of claims. See discussion below.

[21] *See* Villeneuve, *supra* note 6, pp. 74–76. Section 512 gives users an opportunity to object to the takedown action by filing a "counter-notice." This process requires disclosure of user information and consent to court jurisdiction. 17 U.S.C. 512(g).

[22] *See* Electronic Frontier Foundation, "Takedown Hall of Shame," http://www.eff.org/takedowns (documenting abuses of U.S. trademark and copyright law to silence critics or political opponents) *and* Chilling Effects Clearinghouse, http://www.chillingeffects.org/index.cgi.

[23] 17 U.S.C. 512(f). *See* Eric Goldman, "Rare Ruling on Damages for Sending Bogus Copyright Takedown Notice – Lenz v. Universal," Technology & Marketing Law Blog, February 26, 2010, http://blog.ericgoldman.org/archives/2010/02/standards_for_5.htm.

Likewise, the leading social networks have rules against sexually-explicit material and routinely remove even legal content if it violates their terms of service. The protection against liability also, importantly, insulates from challenge the efforts of intermediaries to identify, block and remove child pornography (child abuse images). Under U.S. law, these self-regulatory activities are taken without government mandate (and would be unconstitutional in many cases if mandated by the government). They illustrate how a policy of protecting intermediaries from liability is compatible with – and can even help serve – other societal interests, such as protecting children.

European Union

The European Union also provides significant immunity for ISPs under the Electronic Commerce Directive.[24] EU policymakers considered these provisions indispensable for safeguarding free information flows, encouraging e-commerce development, and promoting broader use of ICTs. The Directive shields several kinds of intermediaries from liability for content posted or transmitted by others:

- "Mere conduits"[25] – The Directive immunizes ISPs from liability for information transmitted over their service as long as the ISP did not initiate the transmission, select the intended recipients, or select or modify the transmitted information. In addition, the ISP must not have stored the information for any longer than reasonably necessary for transmission.

- "Caching"[26] – The Directive immunizes service providers that provide automatic, intermediate, and temporary storage of content, for the sole purpose of making onward transmission more efficient.

- Hosting[27] – The Directive immunizes providers of hosting services for user submitted content, provided that the ISP does not have actual knowledge of illegal activity and that the ISP quickly removes the unlawful content if the ISP is made aware of it.[28]

Note that, in contrast to U.S. law,[29] the Directive does not extend immunity to search engines or portals that provide links to content. However, many EU member states have extended immunity to such service providers in recognition of their importance to the functioning of the Internet.[30]

---

[24] E-Commerce Directive, 2000/31/EC, http://ec.europa.eu/internal_market/e-commerce/index_en.htm. *See also* OpenNet Initiative, Europe - Regional Overview (2009), http://opennet.net/research/regions/europe.

[25] Art. 12, E-Commerce Directive, 2000/31/EC.

[26] Art. 13, E-Commerce Directive, 2000/31/EC.

[27] Art. 14, E-Commerce Directive, 2000/31/EC.

[28] The Directive expressly encouraged self-regulation by industry (rather than imposing a mandate) in creating appropriate notice and takedown procedures for several reasons: 1) it is difficult for static law to adequately respond to the rapidly changing ICT industry, and 2) to allow ISPs room to develop appropriate models that ensure a balance between legitimate interests of users, third parties, and free expression. Recital 40, E-Commerce Directive, 2000/31/EC. *See also* First Report on the application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on the Directive on Electronic Commerce at pp. 14–16, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0702:FIN:EN:PDF.

[29] 47 U.S.C. 512(d).

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

Finally, the Directive provides that states cannot impose on intermediaries a general obligation to monitor content hosted or transmitted on their services, nor a general obligation to actively investigate possible unlawful activity.[31] The class of liability that is preempted is meant to be broad, covering both civil and criminal liability for all types of unlawful activities initiated by third parties.[32] The originator of the unlawful content remains liable, of course, and the Directive does not prevent states from requiring a service provider to stop or prevent specific, identified unlawful activity. In addition, to qualify for immunity, intermediaries must not have been deliberately collaborating in the illegal acts.[33]

It seems clear that EU policymakers intended these provisions to apply to user-generated content services.[34] However, the Directive was passed before the advent of the Web 2.0 era, and only in recent years have cases begun to filter through the courts applying intermediary liability provisions to user-generated content sites. Application in national courts has been mixed so far: Some courts have treated user-generated content sites as hosts under the Directive (and thus eligible for immunity). However, the same courts have often imputed knowledge of unlawful activity to the service provider so that it loses its immunity. In other cases, user-generated content sites have been held liable as publishers instead of hosts because they embedded user content into related content, provided an overall structure for user content (as with a discussion forum or MySpace page), or profited from advertising.[35]

China

The Chinese government has constructed a very sophisticated system of online information control. In addition to technical filtering at the Internet backbone and service provider level, the government imposes responsibility for unlawful content on entities at every layer of access, from the ISP to the online service provider, website, and host company.[36] If any of these intermediaries publishes or distributes content that regulators deem harmful, 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. In addition, the categories of content that regulators consider unlawful are broadly and vaguely defined (for example, content that "harms the interests of the nation" is illegal),[37] actual enforcement varies over time, and government officials often do not follow prescribed legal procedures when issuing

---

[31] Art. 15, E-Commerce Directive, 2000/31/EC.

[32] First Report on the application of Directive 2000/31/EC, p. 12.

[33] Recital 44 of the Directive states: "A service provider who deliberately collaborates with one of the recipients of his service in order to undertake illegal acts goes beyond the activities of 'mere conduit' or 'caching' and as a result cannot benefit from the liability exemptions established for these activities." http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:NOT.

[34] First Report on the application of Directive 2000/31/EC, note 64.

[35] *See,* for example, ILO, "Web 2.0: Aggregator Website Held Liable as Publisher," June 26, 2008, http://www.internationallawoffice.com/newsletters/detail.aspx?g=4b014ec1-b334-4204-9fbd-00e05bf6db95 *and* Crowell & Moring, "Recent French and German case-law tightens the liability regime for Web 2.0 platform operators," July 9, 2008, http://www.crowell.com/NewsEvents/Newsletter.aspx?id=951#mediaisp2.

[36] OpenNet Initiative, China Country Profile (2009), http://opennet.net/research/profiles/china. *See also*, Rebecca MacKinnon, "Commentary: Are China's Demands for Internet 'Self-Discipline' spreading to the West?", McClatchy Washington Bureau, January 18, 2010, http://www.mcclatchydc.com/opinion/story/82469.html.

[37] Congressional-Executive Commission on China, Freedom of Expression – Laws and Regulations, http://www.cecc.gov/pages/virtualAcad/exp/explaws.php#vaguelaws.

filtering or takedown orders. Increasingly in recent years, private defamation suits have also been used to silence online criticism of local businesses or government officials.

In all, this legal regime creates strong incentives for intermediaries to over-block content and monitor user activity at multiple layers. It also encourages self-censorship by users themselves, all designed to manage and suppress expression that threatens state control or is critical of powerful commercial interests.[38]

Looking forward: trends

On a final note, in recent years, Internet policy and human rights advocates have observed with concern growing pressures to transform the role of technological intermediaries. As governments grapple with a range of complex policy challenges – from child protection to national security and copyright enforcement – some have proposed or adopted solutions that enlist technological intermediaries in ways that force them to assume greater gatekeeping and policing functions.

This trend is not limited to authoritarian or "Internet-restricting" countries: there have been some very troubling recent steps towards tightening the liability regime even in democratic states. As noted above, some national courts in Europe that have interpreted national law transposing the E-Commerce Directive to user-generated content sites have begun chipping away at the broad protections for intermediaries that the Directive was meant to provide. In addition, in February 2010, an Italian court convicted three Google executives for a video posted by a user on the (now defunct) Google Video service, even though the video was taken down within hours of notification by Italian law enforcement.[39] Also emerging from Italy is a proposal that may impose new broadcast-style regulations on video hosting sites, including a potential liability regime – precisely the kind of mandate that would make it impossible for video-hosting sites to operate.[40]

---

[38] For example, entering "Tiananmen massacre 天安门屠杀" into an image search engine within China results in pictures of smiling tourists in Tienanmen Square, but not the iconic Tank Man image from 1989. *See* a round up of tests at Rebecca MacKinnon, "China censorship: Yahoo, Google and Microsoft compared," RConversation, June 16, 2006, http://rconversation.blogs.com/rconversation/2006/06/china_censorshi.html. In March 2010, Google announced that it would stop censoring results on its Google.cn China search service. David Drummond, "A New Approach to China: an Update," Official Google Blog, March 22, 2010, http://googleblog.blogspot.com/2010/03/new-approach-to-china-update.html.

[39] "Google bosses convicted in Italy," BBC News, February 24, 2010, http://news.bbc.co.uk/2/hi/8533695.stm. *See also* Leslie Harris, "Deep Impact: Italy's Conviction of Google Execs Threatens Global Internet Freedom," Huffington Post, February 24, 2010, http://www.huffingtonpost.com/leslie-harris/deep-impact-italys-convic_b_474648.html; Arthur Bright, "Will Italy's Conviction of Google Execs Stick?", Citizen Media Law Project, March 2, 2010, http://www.citmedialaw.org/blog/2010/will-italys-conviction-google-execs-stick. The Italian case against Google exposes an uneasy and apparently unresolved relationship among four EU directives: the E-Commerce Directive, which seems to grant broad immunity to intermediaries; the Directive on data protection, 95/46/EC and 97/66/EC; and the Audiovisual Media Services (AVMS) Directive, 2007/65/EC. The E-Commerce Directive states, in Article 1.5(b), that it does not apply to "questions relating to information society services covered by Directives 95/46/EC and 97/66/EC." The issues highlighted by the Google case require further research — and advocacy. *See also* Frank Jordans, "Privacy battle looms for Facebook, Google," Associated Press (via MSNBC.com), March 24, 2010, http://www.msnbc.msn.com/id/36017434/.

[40] Colleen Barry, "Berlusconi moves to impose Internet regulation," AP (via Yahoo! news), January 22, 2010, http://news.yahoo.com/s/ap/20100122/ap_on_hi_te/eu_italy_google_censorship. Daniel Flynn, "Internet companies voice alarm over Italian law," Reuters (via Washington Post), January 26, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/01/26/AR2010012601622.html. *See also* Vera Franz, "Italy's Alarming New Proposed

Finally, escalating concerns about online copyright infringement are creating pressures to transform ISPs into copyright enforcers.[41] France recently passed the HADOPI law, which targets unlawful Internet file sharing by enlisting ISPs in copyright enforcement.[42] In addition, several countries (including the U.S. and members of the European Union) are currently negotiating the Anti-Counterfeiting Trade Agreement (ACTA), a multilateral trade agreement that could potentially encourage more countries to impose liability on intermediaries without counterbalancing protections and could lead to increased monitoring by ISPs.[43]

While entities like ISPs certainly have some role to play in achieving legitimate policy objectives, some of these new developments threaten to undermine the original policy framework that enabled the rise of Web 2.0 platforms. In fact, the trends outside the U.S. towards imposing greater liability on intermediaries may already be endangering the user-generated content model and innovation in a broad range of Web 2.0 applications altogether. One recent report found that, although Web 2.0 applications are used by individuals almost as much in Europe as in the U.S. and Asia, U.S. companies overwhelmingly dominate the market with their innovation: about two-thirds of major Web 2.0 applications are provided by U.S. companies, with Europe lagging far behind in revenue and innovation indicators.[44]

Democratic countries must also be mindful of how even well-intentioned policies will be perceived: Forcing intermediaries to assume greater monitoring and gatekeeping roles for matters such as copyright protection sets a very bad precedent because authoritarian regimes will point to such actions to justify their own restrictive policies. Also, if intermediaries develop the technological capability to police their own networks for copyright infringement, those same technological capabilities can just as well be used to police networks for "unlawful" political dissent.

IV. Addressing Potential Concerns

Providing broad immunity for intermediaries does present some potential concerns that can and should be addressed through policy and law.

Internet Laws," Open Society Blog, March 26, 2010, http://blog.soros.org/2010/03/how-the-italian-government-is-trying-to-turn-the-internet-into-television/.

[41] EDRi, "ACTA revealed, European ISPs might have a big problem," EDRi-gram, No. 7.21, November 11, 2009, http://www.edri.org/edrigram/number7.21/acta-revealed-isp-europe. *See also* Michael Geist, "The ACTA Internet Chapter: Putting the Pieces Together," November 3, 2009, http://www.michaelgeist.ca/content/view/4510/125/.

[42] HADOPI requires ISPs to terminate the Internet accounts of repeat infringers. Nate Anderson, "France passes harsh anti-P2P three-strikes law (again)," Ars Technica, September 15, 2009, http://arstechnica.com/tech-policy/news/2009/09/france-passes-harsh-anti-p2p-three-strikes-law-again.ars.

[43] Negotiating parties released a pre-decisional draft of ACTA in April 2010. For analysis of this draft, see David Sohn, Cloak of secrecy lifted as ACTA text goes public," Policy Beta, April 21, 2010, http://www.cdt.org/blogs/david-sohn/cloak-secrecy-lifted-acta-text-goes-public. *See also* Michael Geist, "ACTA draft text released: (nearly) same as it ever was," Michael Geist Blog, April 21, 2010, http://www.michaelgeist.ca/content/view/4972/125/, *and* "EU Data Protection supervisor warns against ACTA, calls 3 strikes disproportionate," Michael Geist Blog, February 22, 2010, http://www.michaelgeist.ca/content/view/4809/125/.

[44] 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. Europe holds around a ten percent share in revenues and innovation indicators (such as venture capital and R&D expenditures) in the Web 2.0 market. *Id.*

Harmful and offensive content

Perhaps the most obvious potential concern is that liability protection will allow some harmful or otherwise distasteful content online because intermediaries will have less incentive to block potentially offensive expression on their networks or services.

However, governments can take steps to address offensive expression – while minimizing any collateral impact on lawful expression and innovation – by empowering users to control what content reaches their screens. The market has produced a broad array of user empowerment tools.[45] These user-controlled tools include filtering software that can help users to block many kinds of undesirable content (for example, pornography) across a range of applications and platforms, including on the web, email, chat, and a variety of wireless devices. Many ISPs offer such tools to customers for free or at low cost. Governments could promote the voluntary use of such tools by users and could subsidize their purchase through vouchers.

The key feature of this approach is *user* control: empowering users to adopt and tailor tools in order to control what they see so that the government need not step in. A government-mandated tool (even if well-intentioned) will ultimately be less effective,[46] intrude on individual autonomy, and raise concerns around transparency and politically motivated content restrictions.[47]

As we explained above in the sections describing U.S. and EU law, some countries address this concern about bad content by requiring that ISPs implement a system to take down unlawful content when notified of it in order to qualify for immunity. However, as we have also discussed, notice and takedown systems are vulnerable to abuse in ways that can chill free expression. The question of whether the benefits of a notice and takedown approach in addressing harmful content outweigh the potential harm to expression may depend on several factors related to the content at issue, including:

- Effectiveness of user-controlled alternatives to address the harm
- Potential for abuse of the notice and takedown system and the chilling effect that may result

For example, to address content like pornography, a notice and takedown system may not be necessary or preferable because user-controlled tools like filters can effectively shield users from unwanted content – without chilling expression. For copyrighted content, however, user-controlled alternatives are not as effective at fighting copyright infringement since the user is often the party seeking out the unlawful material. On the other hand, as noted above, there is a

---

[45] 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/.

[46] ICTs and new media business models evolve at unprecedented speeds. 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.

[47] The proposed Green Dam/Youth Escort initiative in China last year illustrates these concerns. *See* Cynthia Wong, "Ethics v. Opportunity: Google Reopens the China Debate," Index on Censorship, January 14, 2010, http://www.indexoncensorship.org/2010/01/google-china-censorship-free-speech/ *and* 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.

serious risk of abuse, since the host, facing the difficulty of assessing the copyright claim, may be inclined to cooperate with even spurious takedown requests.

The potential that abuse of a notice and takedown system might chill lawful expression seems at its highest with respect to defamatory content, where intermediaries probably have the least ability to assess whether the expression is defamatory (and will thus have strong incentives to simply comply with the takedown request). A hypothetical example illustrates the problem:

- A citizen writes a blog post stating a particular local government official has embezzled money from the government treasury.
- The official serves a take down 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).
- Because the blog operator risks liability only if it leaves the posting up, the operator removes the post.

Moreover, unlike in the copyright context, there is a strong incentive for the official to assert defamation even if the published content is true. Although user controlled filters are also ineffective at blocking potentially defamatory content or addressing the harm the defamation causes, the very strong potential for abuse may make notice and takedown systems especially unsuitable to address defamatory harms.

As a final note, a policy that provides immunity for intermediaries can be structured in a way that encourages voluntary, responsible action by private intermediaries aimed at protecting users. U.S. law takes this approach under Section 230, which grants immunity to intermediaries for any action voluntarily taken in good faith to restrict availability of material that the service provider considers objectionable (for example, obscene, lewd, or excessively violent content).[48] This approach enables sites like YouTube to experiment with user-driven flagging structures for identifying and removing content that violates YouTube's community guidelines – without fear that doing so might expose the service to liability.[49] The approach taken under Section 230, however, does raise transparency and accountability concerns around how private intermediaries implement such voluntary action. In a competitive market for Internet services, users' preferences and ability to switch to a competing service can help act as a check on potential abuse. However, in markets where users have few choices in, for example, choosing an ISP, this approach might raise as many issues as it addresses.[50]

---

[48] The U.S. takes this approach in Section 230 as part of its policy 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." 47 U.S.C. § 230(b)(4) and (c)(2)(A), http://www.law.cornell.edu/uscode/47/230.html.

[49] *See* YouTube Community Guidelines, YouTube – Broadcast Yourself, http://www.youtube.com/t/community_guidelines.

[50] Providing immunity for voluntary company action taken in good faith is meant to be very different from the more problematic practice of encouraging companies to sign "voluntary" self-regulation pledges common in certain countries in order to curry favor with the government. Such pledges are often neither truly voluntary nor implemented in good faith with regard to users' preferences and human rights. *See*, for example, China's various iterations on a "Public Pledge on Self-Discipline for the Chinese Internet Industry," described in Human Rights Watch, *Race to the*

Law enforcement and victim recourse

Law enforcement officials must be able to investigate and pursue criminal wrongdoers, and victims must be able to pursue legitimate individual claims against the actual creators of the content that has caused them harm.

Under existing intermediary liability frameworks, immunity is granted *only* to the intermediary, not the parties that originally created or disseminated the unlawful content. Nothing under the law would prevent either law enforcement agencies or victims from pursuing the original creator of the unlawful speech. Anonymity online is never perfect and many activities leave digital traces. One proper role for intermediaries might be to facilitate private or law enforcement action against users – even anonymous and pseudonymous users – in response to a legitimate court order, with procedures in place to safeguard privacy and the threshold right of anonymity.[51] Of course, in some countries, particularly those where rule of law is weak, government officials or the courts may not be concerned with striking the balance among privacy, anonymity, and facilitating criminal investigations or private action.

Conclusion

Protecting intermediaries from liability is critical for preserving the Internet as a space for free expression and access to information, thereby supporting innovation and economic development goals. 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 force private intermediaries to close down these forums, then the expressive and economic potential of ICT technologies will be diminished. Governments everywhere should adopt policies that protect 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 practical solutions 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:

Cynthia Wong
Ron Plesser Fellow / Staff Attorney
+1 202.637.9800 x135
cynthia@cdt.org

Bottom: Corporate Complicity in Chinese Internet Censorship (August 2006), p. 12, http://www.hrw.org/en/node/11259/section/6, and by Rebecca MacKinnon, "Chinese Bloggers Thumb Their Noses at Self Discipline,"" RConversation, August 28, 2007, http://rconversation.blogs.com/rconversation/2007/08/chinese-blogg-1.html.

[51] Civil litigants can use litigation mechanisms to identity speakers online and courts have the ability to put in place certain procedural safeguards. For example, before breaching anonymity in the U.S., 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 U.S. Constitution. *See, e.g., Dendrite Int'l v. Doe*, 775 A.2d 756 (N.J. App. Div. 2001).