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 INTERNET PLATFORMS FOR EXPRESSION AND INNOVATION (Summary)

December 13, 2012

This summary provides a brief overview the impact on free expression, privacy, and online innovation of forcing Internet intermediaries—the often-private networks and content platforms that facilitate Internet communications—to assume liability or gatekeeping obligations for third-party content. The threat of liability or gatekeeping obligations reduces intermediaries' willingness to host user-generated content, leads intermediaries to block even legal content, and inhibits investment. 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. Internet advocates everywhere should urge governments to adopt policies that protect intermediaries as critical platforms for innovation, expression, and economic activity.

Intermediaries Are Critical to the Success of the Internet

Every day, hundreds of millions of people around the world go online to access information, to create and disseminate content, and to participate in nearly all aspects of public and private life. For example:

- A journalist uploads a story on a natural disaster to her publication's website through an Internet service provider (ISP), and local residents add their own comments.
- A doctor makes a video in a local language using his mobile phone, posts it on YouTube, and uses SMS to send a link to health clinics so they can show the video to patients.
- A local entrepreneur sells surplus business equipment through an online auction site.
- A homemaker connects to an online community discussion site to complain about the service at a local business.

In these and countless other cases, Internet users depend on one or more technological intermediaries to transmit or host information. These intermediaries include ISPs, mobile telecommunications providers, website hosting companies, online service providers (such as blog platforms, email service providers, social networking websites, and video and photo hosting sites), Internet search engines, and e-commerce platforms. 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, all of which provide

valuable forums for commerce, personal expression, community building, political activity, and the diffusion of knowledge.

Inevitably, some individuals will use such intermediaries to transmit or post content that is unlawful or otherwise offensive. Clearly, people who send or post unlawful content should be subject to penalties provided by criminal or civil law. However, there is a temptation in many countries to try to control objectionable content by punishing not only those individuals but also the intermediaries who transmit or host it. This is known as "intermediary liability." It arises where governments (or private individuals through lawsuits) can hold technological intermediaries such as ISPs and websites responsible for unlawful or harmful content created or selected by their users and other third parties. In addition, some governments have sought to affirmatively require intermediaries to restrict or police user activity in specified ways.

The history of the Internet to date shows that intermediary liability and gatekeeping obligations pose a threat to innovation and free expression. High risk of liability makes it difficult or impossible for intermediaries to offer free or low cost services. Burdensome obligations can discourage investment in innovative services that empower free expression and access to information, can raise privacy concerns, and potentially have an overbroad impact on lawful content. Protecting intermediaries against liability and policing obligations is vital to the future of economic activity, access to information, and communication on the Internet.

For CDT's full analysis of the importance of protecting intermediaries from liability and obligations to police their users' activity, see "Shielding the Messengers: Protecting Platforms for Expression and Innovation" [https://www.cdt.org/ZZ2].

Models for Protecting Intermediaries from Liability

The Internet has flourished in countries that limit the civil and criminal liability of technological intermediaries. Most notably, early in the development of the Internet, both the United States and the European Union adopted policy frameworks that protect ISPs, web hosts, and other intermediaries from liability for unlawful content transmitted over or hosted on their services by third parties. Intermediary protections, which have been adopted in various forms in other jurisdictions over the past fifteen years, generally follow one of two models.

Model 1: Broad immunity. In the US, Section 230 of the Communications Act (47 U.S.C. § 230) protects all Internet intermediaries against being treated as the speaker or publisher of third-party content. This provides protection against a variety of claims, including negligence, fraud, violations of federal civil rights laws, and defamation. Because of this broad protection, intermediaries are free to develop new and innovative services that facilitate users' exchange of information without worrying about exposing themselves and their investors to crippling legal risks. Free expression can flourish as well, because intermediaries do not feel compelled to protect themselves by, for example, paring back on user-generated content features or engaging in over-cautious screening and blocking of user-generated content. Users remain legally accountable for their own online activities – but not the intermediaries that facilitate those activities.

Model 2: Conditional "safe harbor." Under laws that follow the model of the US Digital Millennium Copyright Act (17 U.S.C. § 512) or the EU E-Commerce Directive (Dir. 2000/31/EC), certain intermediaries receive immunity with respect to third-party content as long as they meet certain criteria and follow certain requirements. Requirements can vary, but generally involve the

intermediary maintaining a relatively passive role with respect to the creation or selection of the content, and often include a requirement that service providers take some action when notified of unlawful content on their services. 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.

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. Conditions are designed in part to prevent safe harbors from being readily available to clear "bad actors" that are actively and knowingly aiding or conspiring in unlawful activity. 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, however – 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.

The main categories of service provider identified in the ECD and DMCA safe harbor regimes are as follows:

- "Mere conduits" that transmit information;
- "Caching" services that provide temporary storage for the sole purpose of making onward transmission more efficient;
- "Hosting" services for user-submitted content; and
- "Information location tools," such as search engines, that link to third-party content. (While the ECD 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.)

Strict Liability/No Protection. Some countries broadly impose liability on intermediaries in order to restrict expression. 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. In Thailand, Internet intermediaries that transmit or host third-party content face serious liability risks under the 2007 Computer Crimes Act (CCA). 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. These indirect methods of control can be just as dangerous for free expression as direct government censorship.

Intermediary Liability Inhibits Economic Activity, Innovation, and Free Expression

The problem with making intermediaries liable for content created by others is that, for several reasons, such policies are likely to lead to the curtailment of legitimate speech. First, holding intermediaries liable for user content greatly inhibits their willingness to host any content created by others. Indeed, liability may make it impossible for certain services to exist at all. Many user-

generated content platforms could not exist if they had to pre-screen everything before it was uploaded.

Second, intermediary liability creates an incentive to over-block content. The safest course will always be to reject the content. If a government official or a private litigant demands that a company take something down, intermediaries commonly comply with the request rather than challenging the request and risking legal consequences. This incentive is especially strong where definitions of illegal content are vague and overbroad, or where it is not easy to determine whether the disputed content is unlawful. Because intermediaries have little incentive to challenge a removal request, intermediary liability also leaves room for abuse on the part of the government or private litigant seeking to take down content for unscrupulous reasons.

Finally, intermediary liability also creates disincentives for innovation in ICTs. Without protection from liability, companies are less likely to develop new ICT products and services that offer platforms for user-generated content. The threat of liability may thereby further entrench existing companies, who will be less driven to innovate or improve upon existing business models.

Gatekeeping Obligations Likewise Affect Innovation and Users' Fundamental Rights

In addition to the question of liability for third-party content, some governments have sought to affirmatively require intermediaries to restrict or police user activity in specified ways. Example obligations include website blocking, domain name seizure, media licensing and content regulation, and proposals to deputize intermediaries to warn or punish users who appear to be engaged in illegal activity. Proponents of these approaches argue that intermediaries are well-positioned to prevent unlawful or harmful content, and that this is preferable to assessing liability after the fact. 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 law enforcement.

Imposing gatekeeping obligations on Internet intermediaries, however, can also have a profound and negative impact on innovation and fundamental rights. Burdensome obligations can discourage investment in innovative services that empower free expression and access to information, and many technical measures can have an overbroad impact on lawful content. Moreover, obligations that require content monitoring can also raise serious privacy concerns, particularly when imposed on access providers. Lastly, direct content regulation and broadcast-style licensing or registration requirements necessarily limit opportunities online and undermine the Internet's role as an open medium for speakers of all kinds.

Systems focused on warning subscribers about risky or illegal behavior 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.

Alternatives for Addressing Unlawful Content

Protecting intermediaries from liability and stifling gatekeeping obligations is critical for preserving the Internet as a space for free expression, access to information, and innovation. As governments all around the world struggle with how to best address a range of policy challenges – from child

protection to national security and copyright enforcement – increased and sustained advocacy is needed by human rights groups, Internet policy advocates, and industry actors alike, in support of policies that protect intermediaries as critical actors in promoting innovation, creativity, and human development. If liability concerns force intermediaries to close down or tightly restrict these forums, then the expressive and economic potential of the Internet and Internet-based platforms will be diminished.

It is possible, however, for governments to take steps to address harmful and unlawful online activity while minimizing any undue impact on lawful expression and innovation. Possible alternatives include:

User empowerment. Governments can encourage the use of a broad array of available tools that can help users block content they deem undesirable or harmful, including pornography, hate speech, or materials promoting illegal activity. The key feature of this approach is *user* control: empowering users to select and tailor technological tools according to their own needs and preferences. Government-mandated technology may ultimately be less effective, intrude on individual autonomy, and raise concerns around transparency and politically motivated content restrictions.

Education. Governments and intermediaries can play a role in educating the public and individual users about risks and legal obligations users face online. Done right, educational efforts, including systems under which access providers forward warning notices to certain subscribers, have the potential to play a positive role in shaping public understanding, expectations, and norms to discourage illegal and harmful online activity. Such systems must, however, follow fair processes and present balanced information. 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 overaggressive warnings could discourage recipients from engaging in legitimate activities.

Coordination and resources for law enforcement. Liability protections for online content should be limited to *intermediaries* and should not impede action against those responsible for illegal content in accordance with due process and rule-of-law protections. Coordinating cross-border enforcement can pose challenges, but they are not insurmountable.

Voluntary enforcement by intermediaries. Governments may seek to encourage Internet intermediaries to take *voluntary* action to control harmful or unlawful online content. Indeed, the US's "Section 230," which arguably offers the most expansive protection for intermediaries, contains a separate provision that shields service providers when they take good-faith steps to remove objectionable content. Private arrangements allow greater flexibility and thus may be preferable to 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. Nonetheless, voluntary measures can pose risks to users' rights. Voluntary actions that impose concrete sanctions on individuals, entities, or websites, for example, effectively put private parties into a quasi-judicial role, making strong safeguards essential.

Industry-wide approaches may offer an opportunity to develop sound best practices that are less ad-hoc, more fair, and more broadly understood and accepted. Adopting 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. And 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. At a minimum, 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.

"Follow the money." Governments may call for action by *financial* intermediaries, such as payment processors and ad networks. Targeting enforcement at entities with business relationships that enable sites to profit from unlawful activity is generally preferable to focusing on communications intermediaries – but it carries significant risks as well. If applied too broadly, money-focused measures could undermine freedom of expression by imperiling lawful sites. The threat of financial cutoff can also discourage investment in new services or lead to self-censorship. At a minimum, there need to be procedural protections 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.

In short, while there is no single solution to the policy challenges posed by harmful and unlawful online content, there are a number of potential tools and approaches that do not require burdening Internet intermediaries with liability or gatekeeping obligations for third-party content. In the interest of promoting economic growth, technology innovation, and free expression, governments around the world should establish legal frameworks that hold Internet users responsible for their own online behavior – but not the technological intermediaries that facilitate users' communications.

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