

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 AND RESPONSIBILITY PRIMER

December 2012

This paper provides a brief overview the impact on free expression, privacy, and online innovation of forcing Internet intermediaries to assume liability or gatekeeping obligations for third-party content. Full a full discussion of these issues, see URL.

Internet communications involve and rely upon a range of private intermediaries such as ISPs, social networks and other content hosts, and search engines. These conduits and platforms are not only the locus of tremendous investment and a source of economic growth; they are also essential to the exercise of fundamental rights online. The policy environment in which they operate is therefore critical to the continued growth of the Internet as a medium of commerce, innovation, and free expression.

A central tenet of sound Internet policy is that while users should bear legal responsibility for their activities, Internet intermediaries generally should not. Policies that protect intermediaries from liability for third-party content and from obligations to police such content encourage investment and expand the space for expression and innovation. In contrast, policies that force intermediaries to bear liability risks or high costs associated with monitoring or policing content discourage intermediaries from enabling users to post content in the first place, diminishing opportunities for expression and preventing the full benefits of the information society from being realized.

Models for Protecting Intermediaries

Broad immunity. In the US, Section 230 of the Communications Act protects all Internet intermediaries being treated as the speaker or publisher of third-party content. Thus, 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. Users – not the intermediaries they use – bear responsibility for their own online activities.

Conditional “safe harbor.” Under laws that follow the model of the US DCMA or Europe's E-Commerce Directive, 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 of the content, and often include a requirement that service providers take some action when notified of unlawful content on their service. To best protect online free expression, access to information, and innovation, conditional safe harbors systems should follow these principles:

- Protection must be broadly available to a range of intermediaries, including content hosts, search engines, and access providers.
- Conditions should not be so burdensome that they introduce unreasonable obstacles to offering the service in question. Conditions should scale with the volume and pace of Internet communication, and avoid requirements that intermediaries monitor all traffic.
- If action is required upon notice of unlawful content, intermediaries need clear guidance as to what constitutes a valid notice. Clarity and specificity are essential.

- Actions required must be narrowly tailored to specific unlawful content and proportionate to the harm such content generates, in order to prevent overbroad action and to safeguard users' rights.
- The removal of content upon private notice (as opposed to court orders) must be limited to contexts where illegality is straightforward.
- In any notice-and-action system, safeguards are necessary to mitigate risks of abuse. They should include appeal mechanisms, meaningful penalties for unjustified notices, and some degree of flexibility for intermediaries to ignore flawed notices.

Gatekeeping Obligations

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. Proponents argue that intermediaries are well-positioned to prevent unlawful or harmful content, and that this is preferable to assessing liability after the fact. Imposing gatekeeping obligations on intermediaries, however – whether through site-blocking mandates, seizures of domain names, media licensing requirements, systems by which intermediaries warn or punish users for their behavior, or other means – can threaten innovation and fundamental rights in much the same way as liability risk. Burdensome obligations can discourage investment in innovative services that empower free expression and access to information; many technical measures can have an overbroad impact on lawful content. Obligations that require content monitoring can also raise serious privacy concerns, particularly when imposed on access providers.

Alternatives to Intermediary Liability and Gatekeeping Obligations

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.

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.

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.

“Follow the money.” 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.

Voluntary enforcement by intermediaries. In addition to developing and enforcing their own terms of service, intermediaries may engage in private multiparty agreements to, for example, report or respond to unlawful content. Private arrangements allow greater flexibility and thus may be preferable to government mandates. Nonetheless they can pose risks to users' rights, particularly where punitive measures are contemplated or where an industry widely agrees to similar standards or practices, effectively limiting users' choice and access to alternatives.

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