UNITED STATES DEPARTMENT OF COMMERCE
NATIONAL TELECOMMUNICATIONS
AND INFORMATION ADMINISTRATION

In the Matter of

Global Free Flow of Information On the Internet **Docket No. 100921457-0457-01**

COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY ENDORSED BY THE ASSOCIATION OF RESEARCH LIBRARIES AND THE AMERICAN LIBRARY ASSOCIATION

December 6, 2010

The Center for Democracy & Technology ("CDT") respectfully submits these comments in response to the Commerce Department's Notice of Inquiry regarding the free flow of information on the Internet. CDT is a nonprofit public interest organization dedicated to preserving and promoting openness, innovation, and freedom on the global Internet. The Association of Research Libraries and the American Library Association endorse these comments.[1]

Restrictions on the free flow of information on the Internet take a number of forms. Government policies assigning liability to online intermediaries for the content their users post serve as one of the most significant barriers to the free flow of information online. In Part I of these comments, we highlight the importance of liability protections for online intermediaries and the way these protections serve to maintain the Internet as a robust platform both for the free flow of information and for trade. In Part II, we discuss additional restrictions while addressing many of the specific questions outlined in the Notice.

Part I – The Importance of Intermediary Liability Protections to the Free Flow of Information and Trade on the Internet

The American Internet and online services industries remain the most vibrant and innovative in the world. American technology companies also benefit from the strongest domestic protection from liability for third party content, providing legal certainty and freeing U.S. business to innovate and grow. It is precisely these protections that have enabled American technology companies to become globally dominant players in their respective sectors.

---

[1] The Association of Research Libraries (ARL) is a nonprofit organization of 125 research libraries in North America. ARL influences the changing environment of scholarly communication and the public policies that affect research libraries and the diverse communities they serve. The American Library Association (ALA) is a nonprofit professional organization of more than 61,000 librarians, library trustees, and other friends of libraries dedicated to providing and improving library services and promoting the public interest in a free and open information society.

1. Intermediary liability protections are vital to the free flow of information in the U.S. and around the world.

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.[2] Internet intermediaries – the technological entities that provide the platforms and conduits for digital communications – play critical roles in getting information and ideas from one corner of the online world to another.[3]

The Internet has developed and flourished in this fashion because of an early U.S. (and to a lesser extent, European) policy framework based on competition, openness, innovation, and trust.[4] 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).

While users should remain responsible for their unlawful online activities, policies protecting intermediaries from liability for content posted by third parties promote free flow of information and innovation and better advance the Internet as a platform for a wide range of beneficial activities. If, in contrast, private intermediaries were to be held liable for the content created by others, they would strive to reduce their liability risk. In doing so, they would be likely to overcompensate, blocking even lawful content. In this way, intermediary liability would chill the free flow of information and transform 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 the free flow of information and user rights as direct government censorship.

2. Intermediary liability protections are likewise integral to maintaining the Internet as a platform for innovation and growth.

The global Internet has also become a vibrant and essential platform for economic and educational activity, enabled by the same intermediary liability protections that have supported its development as an unprecedented medium for the free flow of information. When intermediaries are protected from liability for their users' content,

---

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

[3] These intermediaries, which include Internet service providers (ISPs), telecommunications carriers, web-hosting companies, websites, online services, and a range of other technological 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.

[4] Two separate laws provide protections for Internet intermediaries under U.S. law: Section 512 of the Copyright Act, 17 U.S.C. 512 (for copyright infringement), and Section 230 of the Communications Act, 47 U.S.C. 230 (for a range of other kinds of claims). The EU provides similar but less comprehensive protections for intermediaries in the E-Commerce Directive, 2000/31/EC.

they are freer to innovate new products and services, which often serve as additional platforms for small innovators and individual speakers to offer content, services, or applications. The Internet has unleashed a wave of innovation driven by small inventors and entrepreneurs, generating an enormous amount of economic value. Moreover, libraries and educational institutions are prolific providers of content, services, and applications via the Internet and rely on the Internet to collaborate and to obtain and provide services to students, researchers, and members of the public. Multi-billion dollar companies, entirely new categories of products and services, and e-commerce of all kinds have arisen virtually from scratch. Greater competition has been introduced into many sectors as Internet-based endeavors challenge traditional business models.

Protections for intermediaries are essential to this innovation and growth. Intermediary liability and uncertainty over legal risk 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.

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. A range of intermediaries directly contributes to economic growth:[5] 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 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.[6] Inhibiting ICT development or adoption will limit many of these broader economic benefits.[7]

---

[5] *See* OECD, *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.

[6] 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).

[7] Internet-curtailing nations can 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)),

3. U.S. economic interests are severely harmed by uncertainty surrounding intermediary liability protections in international and domestic markets.

The history of the Internet to date demonstrates that the policy framework protecting intermediaries from liability for the acts of their users is necessary to support the free flow of information online. The U.S. online industry is the most dominant in the world precisely because of the protections afforded intermediaries by Section 230 and the DMCA. This policy framework, however, is under pressure internationally, as other countries shift toward holding intermediaries liable for third-party content, and domestically, as legislators and law enforcement seek to change the roles that intermediaries play.

In recent years, Internet policy 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. These trends have created an environment of increasing legal uncertainty in many parts of the world.

Some governments see Internet intermediaries as a convenient point of control. Because the Internet enables relatively anonymous or pseudonymous activity online, it is often difficult to identify the actual author of offensive content. Even if identifiable, the wrongdoer may be out of a government's jurisdictional reach. Accordingly, some governments turn to ISPs and other intermediaries: By holding intermediaries liable for illegal content if they do not block or remove it, governments can compel intermediaries to more actively monitor and police user content.[8] While entities like ISPs may have some role to play in achieving legitimate policy objectives, some of these new developments threaten to undermine the original policy framework – largely originating in the U.S. – that enabled American industry to flourish and succeed globally. The disparate treatment of intermediaries in the U.S. and around the world creates significant uncertainty for businesses looking to expand from the U.S. to the global marketplace.

Beyond disparate legal regimes between states, businesses also face uncertainty over how intermediaries are treated within the same legal system in some markets. For example, the EU Electronic Commerce Directive ("ECD") provides a range of Internet intermediaries with significant protection from liability for content posted or transmitted by others, so long as these intermediaries meet certain conditions. It also prohibits imposing on intermediaries a general obligation to monitor content on their services or a general duty to investigate possible unlawful activity. EU policymakers considered these

---

http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+20080219+ITEMS+DOC+XML+V0//EN&language=EN#sdocta18.

[8] The strategy of using intermediary liability to enforce speech restrictions is not limited to authoritarian regimes or emerging markets, however. In recent years, even some Western democracies have proposed laws that would force Internet intermediaries to assume greater content gatekeeping functions. *See* CDT, *Intermediary Liability: Protecting Internet Platforms for Expression and Innovation*, April 2010, www.cdt.org/files/pdfs/CDT-Intermediary%20Liability_(2010).pdf, at 11–12.

provisions indispensable for protecting free information flows and encouraging ICT development.

However, the ECD was passed before the Web 2.0 era and the development of the user-generated content (UGC) services that exist today. Recently, cases have begun to filter through the European national courts applying liability protection provisions to UGC sites and the results have been mixed: Some courts have treated UGC sites as hosts eligible for immunity under the ECD, but they have also imputed knowledge of unlawful activity to the host (for example, because of knowledge of prior copyright infringement) thereby removing immunity. In other cases, UGC sites have been held liable as publishers (and thus not eligible for immunity), because they embed UGC into related content, provide an overall structure, or profit from advertising.[9]

Some European courts have also imposed monitoring duties on intermediaries in ways that undermine the policy choice laid out in the ECD. For example, a Belgian court held that requiring an ISP to filter certain copyrighted content did not violate the monitoring prohibition because the company was not being ordered to do so "generally."[10] German courts have also required monitoring to prevent future unlawful activity after a finding of prior infringement on the company's service.[11] One court has emphasized that "no unreasonable duties to monitor are to be entailed on [an online intermediary], which would challenge his whole business model," but at the same time admitted it is "difficult to predict what Courts would hold to be 'reasonable.'"[12] Results vary both within a member state and among member states.[13]

These still-evolving rules create a great deal of uncertainty around the legal responsibilities of Internet intermediaries, pose difficult compliance challenges to companies seeking to offer Internet services in the EU, and can stifle innovation. These uncertainties 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: 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.[14]

---

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

[10] Stephen W. Workman, "INTERNET LAW - Developments in ISP Liability in Europe," Internet Business Law Services, August 24, 2008 (also criticizing the Court for failing to apply Article 12 conduit immunity), *available at* http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=2126.

[11] Henning Krieg, Bird & Bird, "Online intermediaries may have an obligation to monitor content posted by users" (June 4, 2007), *available at* http://www.twobirds.com/English/NEWS/ARTICLES/Pages/Online_intermediaries_obligation_monitor_user-posted_content.aspx.

[12] *Id.*

[13] A Dutch study noted the uneven application of ISP liability in the monitoring context occurs, in part, because of the differing types of law under which these cases can be decided. Ministry of Economic Affairs, "Liability of ISPs in the Netherlands," p. 7, (November 5, 2008), *available at* http://ec.europa.eu/internal_market/e-commerce/docs/expert/20070220-dti_en.pdf.

[14] 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.

The U.S. must be careful not to tread down the same path that some European courts have taken, away from established policy that protects intermediaries and promotes innovation, and toward decisions and legislation that assign liability or encourage gatekeeping. Recent legislative proposals such as the Combating Online Infringement and Counterfeits Act (COICA) envision a role for Internet intermediaries that represents a drastic deviation from current U.S. policy and which threatens the free flow of information online.[15] Targeting the technical intermediaries that administer the domain name system (as in COICA, discussed in more detail below) or other elements of the Internet's architecture as a point of control for law enforcement is at odds with U.S. intermediary protection policy and places the free flow of information online in jeopardy.

The U.S. and other 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. Exporting such policies to weak rule-of-law states can have unintended consequences and 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 political dissent that repressive regimes deem to be "unlawful."

Maintaining the U.S.'s broad protections for intermediaries against liability, and encouraging adoption of similar liability protections globally, is vital to promoting information flows and continued technical and economic innovation on the Internet.

Recommendation: The U.S. government must maintain a united policy front toward protecting Internet intermediaries from liability for third party content. U.S. businesses enjoy a dominant position in the Internet industry – particularly in areas like search and social networking that depend on user-generated content – due to the liability protections they receive under Section 230 and the DMCA. To support the free flow of information and trade, both domestically and internationally, the U.S. must maintain its strong intermediary liability protections and resist efforts to convert intermediaries into gatekeepers and content police.

Recommendation: Through its role in trade negotiations and participation in inter-governmental fora, the Department of Commerce should work with its counterparts in other countries to emphasize the importance of intermediary liability protections in global commerce and the free flow of information, and to promote similar policies abroad.

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.

[15] For further analysis of S. 3804, see CDT, "Dangers of S. 3804: Domain Name Seizure and Blocking Pose Threats to Free Expression, Global Internet Freedom, and the Internet's Open Architecture," September 28, 2010, http://www.cdt.org/files/pdfs/Leahy_bill_memo.pdf.

Part II – Responses to Specific Questions in the Notice

1. Types of Restrictions on the Free Flow of Information on the Internet

Governmental controls on information are increasingly widespread and sophisticated

Governmental controls on the free flow of information have become much more sophisticated and widespread. More than forty countries now block access to content or services on the Internet to some degree.[16]

Building on filtering and blocking, a set of second-generation controls has become more established practice. Such controls include:

- Local licensing and registration requirements for service and content providers, which gives governments greater ability to exert control over content available domestically.
- Expanded use of defamation laws (especially criminal defamation) to restrict certain kinds of information.
- Selective and intermittent blocking of content or entire services during times of unrest or political sensitivity.
- Use of intermediary liability to encourage private censorship by companies who provide the platforms for expression.

Finally, a third generation of controls is now beginning to emerge. These controls include:

- A push towards pervasive, often covert surveillance of networks, which encourages self-censorship by users.
- Pressure on a range of service providers to build in technical capacity to enable government surveillance in new forms of online communications, including encrypted communications.
- Restrictions on anonymous or pseudonymous use of online services and mobile phones.

To implement these controls, many countries are now adopting new laws targeted at online information flows. For example, the Turkish government enacted the Internet Law of Turkey in 2007, known as Law No. 5651, in response to concerns about unlawful YouTube videos, as well as the availability of pornography and other online materials deemed harmful to children.[17] Although Law No. 5651 does not create new Internet speech crimes, it imposes new obligations on content providers, ISPs, and website hosts, and grants authority to an agency to issue administrative orders to block websites (for content hosted outside Turkey), under a very low standard of proof.[18] This agency

---

[16] Jillian C. York, "More than half a billion users are being filtered worldwide," *OpenNet Initiative Blog*, January 19, 2010, http://opennet.net/blog/2010/01/more-half-a-billion-internet-users-are-being-filtered-worldwide.

[17] 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) ("Internet Law of Turkey").

[18] Internet Law of Turkey, Art. 8. The law provides for some judicial oversight and a process for appealing blocking orders. However, the standard the agency must meet to get a blocking order approved in the first place is low, requiring only "sufficient suspicion" of criminal activity. For a fuller analysis, *see* Yaman 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.

may also issue orders to take down eight specific kinds of unlawful content, including obscenity, child abuse images, encouragement of or incitement to suicide, crimes against Atatürk, and the provision of substances dangerous to health.[19] Indeed, the Turkish government has used this law to block access to YouTube in Turkey for several years.

Thailand's 2007 Computer Crimes Act (CCA) is another example of a law specifically targeting Internet-related offences that has consequences for the free flow of information.[20] The CCA defines new computer crimes and sources of civil liability, and provides broad electronic search and seizure authority to government officials. The CCA, which implicates both intermediaries that transmit or host third-party content and the authors of the content themselves, punishes the online publication or knowing dissemination of "forged" or "false computer data" that is likely to cause injury to another person, the public, or to national security, as well as making "obscene computer data" accessible to the public.[21] However, the law leaves many of these terms undefined, and the breadth of the language makes it difficult to assess what speech might be judged unlawful. The CCA does not make specific reference to Thailand's *lèse majesté* law, which criminalizes criticism or defamation of the royal family.[22] However, because government officials have interpreted *lèse majesté* broadly to amount to harm to national security, the mechanisms created by the CCA have been used to penalize political dissent or criticism of the government online.[23]

Applying existing laws to online content can also impede information flows

In some cases, governments simply apply existing laws to online content. For example, under its hate speech laws, France prohibits the sale of Nazi memorabilia. A French court penalized Yahoo! in 2000 for providing access to such material online, arguing that existing French law applies to Internet speech.[24] In Turkey, it is a crime to insult the founder of the Turkish Republic, Mustafa Kemal Atatürk, or to "disparage Turkishness", and authorities have applied this law to videos hosted on YouTube.[25]

---

[19] Although Turkish lawmakers initially decided to limit the scope of the crimes covered by the Law, there is already pressure to expand this list. *See* Yaman Akdeniz & Kerem Altiparmak, *Internet: Restricted Access, A Critical Assessment of Internet Content Regulation and Censorship in Turkey* (2008), http://privacy.cyber-rights.org.tr/?page_id=256.

[20] Computer Crimes Act BE 2550 (2007), English translation available at http://advocacy.globalvoicesonline.org/wp-content/plugins/download-monitor/download.php?id=2 ("Computer Crimes Act").

[21] Computer Crimes Act, Section 14. Section 16 also specifically penalizes the public online dissemination of digital photographs meant to hurt the reputation of others or expose another person to public hatred or shame.

[22] *See* OpenNet Initiative, Thailand Country Profile (2007), http://opennet.net/research/profiles/thailand.

[23] *See* Reporters Without Borders, "Countries Under Surveillance – Thailand", Internet Enemies Report (2009), http://en.rsf.org/surveillance-thailand,36673.html, and United States State Department, 2009 Human Rights Report: Thailand (March 2010), http://www.state.gov/g/drl/rls/hrrpt/2009/eap/136010.htm.

[24] *UEJF et Licra v. Yahoo! Inc. et Yahoo France*, Tribunal de Grande Instance de Paris (May 2000), *translation available at* http://www.juriscom.net/txt/jurisfr/cti/yauctions20000522.htm. Yahoo! successfully sought a declaratory judgment in U.S. district court that the French judgment was unenforceable under the First Amendment to the Constitution. However, the Ninth Circuit reversed the lower court's decision on jurisdictional grounds. *Yahoo! Inc. v. LICRA and UEJF*, 433 F.3d 1199 (9th Cir. 2006), http://cases.justia.com/us-court-of-appeals/F3/433/1199/546158/.

[25] Yaman Akdeniz & Kerem Altiparmak, *Internet: Restricted Access, A Critical Assessment of Internet Content Regulation and Censorship in Turkey* (2008), http://privacy.cyber-rights.org.tr/?page_id=256.

However, applying offline rules to the Internet poses special problems and may yield rules with harsh consequences. For example, the UK has applied its "multiple publication rule" in deciding online defamation cases. Stemming from longstanding common law, the rule provides that each individual sale or distribution of defamatory content can be considered a separate publication of that content, and can thus give rise to a separate cause of action. However, applying this rule to online content raises serious problems, particularly because content can be widely disseminated almost instantaneously and content is often mirrored, archived, and made available years after initial publication. UK courts have applied this rule to online content, treating "each viewing of a defamatory posting" as a new publication that can give rise to damages.[26] This theory leaves open the possibility that a litigious plaintiff could bring an endless string of lawsuits for a single piece of content as it is archived, mirrored and redistributed online. The enormous threat of liability this would pose to media organizations and other content authors online can have a grave chilling effect on the free flow of information.[27] The UK's approach takes on particular salience when we consider the rising use of defamation suits aimed at user-written criticism posted on popular consumer review websites.[28]

In applying offline rules to the Internet, the question arises of what is the appropriate subset of offline rules to use. Some countries are extending to the Internet rules developed for traditional broadcast media (radio and television), even though these rules are not particularly well suited to the unique attributes of the Internet as an abundant, borderless, user-controlled medium. For example, the EU Audiovisual Media Services Directive (AVMS), which once only regulated European broadcast television, has been recently revised to apply to content available through "on-demand" audiovisual media services. This includes Internet content that consists of commercial

---

The provision on "Turkishness" was amended in 2008 to limit its application and lower penalties. *See also* Sabrina Tavernise, "Turkey to Alter Speech Law," N.Y. Times, Jan. 25, 2008, http://www.nytimes.com/2008/01/25/world/europe/25turkey.html. Nevertheless, concerns remain about its application, including in the Internet context. *See* Jeffrey Rosen, "Google's Gatekeepers", New York Times, 28 Nov. 2008, http://www.nytimes.com/2008/11/30/magazine/30google-t.html (discussing struggle between Google and Turkey over YouTube videos). In addition, Turkey has also passed a law specifically dealing with regulation of expression on the Internet. *See* Yaman 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.

[26] Clifford Davidson, "U.K. Internet Publication Rule Upheld; Internet Viewings Constitute Republication", Proskauer Privacy Law Blog, March 13, 2009, http://privacylaw.proskauer.com/2009/03/articles/international/uk-Internet-publication-rule-upheld-Internet-viewings-constitute-republication/. The UK rule was upheld by the European Court of Human Rights. Afua Hirsch, "Times fails to overturn 'Internet publication rule' in court case", The Guardian, March 10, 2009, http://www.guardian.co.uk/media/2009/mar/10/times-european-court-single-publication.

[27] In contrast, the US applies a single publication rule, where any one edition of a newspaper or any one radio broadcast is considered a single publication, and only one action can be brought by a plaintiff for that publication. U.S. courts have upheld the single publication rule for online content. For further background, see Itai Maytal, "Libel Lessons from Across the Pond: What British Courts Can Learn from the United States' Chilling Experience with the 'Multiple Publication Rule' in Traditional Media and the Internet," 3 J. of Int'l Media & Entertainment L. 121 (2010), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1655046.

[28] *See, e.g.*, Susan Stellin, *Hoteliers Look to Shield Themselves from Dishonest Reviews*, N.Y. Times, Oct. 25, 2010, at B7, *available at* http://www.nytimes.com/2010/10/26/business/26hotels.html (discussing a potential class action to be brought by Kwikchex on behalf of American and British hotels against the website TripAdvisor and individuals who posted negative reviews online).

mass media that is "television-like" and whose function is to "inform, entertain and educate the general public."[29] The EU Member States will ultimately interpret and apply these terms—and determine whether they will cover novel online video services, including those that support user-generated content. But the mere fact that Internet-based services are being subsumed at all under the AVMS is troubling, because broadcast media were traditionally subject to more restrictions than other kinds of media.

Applying traditional broadcast media laws to online platforms would cripple the innovation, growth, and diversity of information that the Internet has enabled. Broadcast regulatory models have been the most restrictive in the scope of content it proscribes. Licensing requirements for content or websites would create a severe bottleneck, reducing the current abundance of UGC to amounts comparable to that which we find on television; licensing costs would meanwhile destroy the Internet as a low-barrier-to-entry medium. License requirements would additionally provide governments with one more lever of control over content. This is a lesson already apparent by China's Internet users; China only allows local ISPs to deliver licensed websites and uses the license approval and renewal process as a means of censoring content and enforcing requirements that websites engage in self-censorship.[30]

Laws with legitimate policy objectives can still restrict information flows

The policy goals animating these governmental regulations range from the legitimate to the repressive. Often-cited concerns include child pornography, national security, cybercrime, copyright infringement, and potentially harmful content such as violence or sexual material. The legitimacy of these various motivating concerns notwithstanding, in all cases care must be taken to consider not just the ends at issue, but also the

---

[29] Directive 2010/13/EU of the European Parliament and of the Council on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (codified version), Recitals 22 and 24, March 10, 2010 (stating that "television-like" means "they compete for the same audience as television broadcasts, and the nature and the means of access to the service would lead the user reasonably to expect regulatory protection within the scope of this Directive"), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:095:0001:0024:EN:PDF.

[30] Websites hosted on Chinese servers are required to navigate multiple layers of bureaucracy and, sometimes, political as well as legal roadblocks to obtain what is known as an Internet Content Provider (ICP) license. John Bishop and Chris Myrack, "FOCUS: Google License Issue Seized by China to Make Political Statement," AFX News Limited, Feb. 23, 2006, http://www.forbes.com/feeds/afx/2006/02/23/afx2547661.html. Once the license is granted, the grantee is responsible for monitoring site content and engaging in self-censorship: the national telecommunications law prohibits Web sites from hosting or facilitating distribution of a wide range of content, including material that "harms the national interest" or "undermines social stability."
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. Those who fail to comply with the self-censorship requirements risk losing their ICP license, their website, and their business license. *China's Information Control Practices and the Implications for the United States*, *Testimony Before the U.S.-China Econ. & Sec. Review Comm'n* (June 30, 2010) (testimony of Rebecca MacKinnon, Visiting Fellow, Ctr. for Info. Tech. Policy, Princeton Univ.), http://www.uscc.gov/hearings/2010hearings/written_testimonies/ 10_06_30_wrt/10_06_30_mackinnon_statement.php. Most famously, Google battled to maintain its ICP license after it redirected all users who visited its google.cn website to its uncensored Hong Kong site, google.hk. David Drummond, "An Update on China," Google Blog, June 28, 2010, http://googleblog.blogspot.com/2010/06/update-on-china.html. *See generally,* Rebecca MacKinnon, "Studying Chinese Blog Censorship," RConversation, Nov. 29, 2008, http://rconversation.blogs.com/rconversation/2008/11/studying-chines.html.

means used to achieve them and any collateral impact on legitimate uses of online tools.

Many tactics come at significant cost to free flow of information and innovation. For example, few would question the legitimacy of a goal to eliminate child pornography. But intermediary filtering, a tactic used in many countries to stop its online distribution, can lead to serious overblocking concerns, affecting vast amounts of protected content.[31] Similarly, efforts to address national security risks online may adversely impact Internet users' privacy. And efforts to prevent and to punish copyright infringement, even in democratic rule-of-law countries, can significantly impact people's legitimate use of the Internet and the free flow of information.

For example, the recently proposed "Combating Online Infringement and Counterfeits Act" (COICA) in the U.S. contemplates the use of DNS blocking to obstruct access to websites dedicated to infringing activity. However, use of DNS blocking would have a significant harmful impact on the global free flow of information in several ways.[32] It would threaten legitimate online expression, primarily because it would inevitably block some lawful speech in addition to whatever material was being targeted. Single domains can "house" thousands of distinct pages at the subdomain level, and a domain registry or registrar taking blocking action against a domain would necessarily affect all subdomains – even sites unaffiliated with the site that gave rise to the blocking order.[33] In the U.S., such overblocking would run afoul of the First Amendment, which requires that an order against speech "be precise and narrowly tailored to achieve the pin-pointed objective of the needs of the case."[34]

Policymakers must also remain aware that more repressive governments will increasingly invoke widely accepted goals such as national security, cybercrime, or the protection of children to justify measures for repression and restriction on information flow. Consider the Green Dam incident: The Chinese government recently tried to require computer manufacturers to install a filtering program on computers sold in China as a child-protection measure. However, as it was revealed later, this filtering program blocked far more than just pornography, sweeping in politically sensitive content as well, and also created privacy and security risks.[35] Governments have also selectively blocked services like Twitter, YouTube, and Facebook during times of political sensitivity or civil unrest, citing national security concerns.[36] But it is these tools that activists in closed societies often use in order to reach the outside world, especially where traditional media is tightly controlled. While China is often viewed as extreme in

---

[31] *See*, e.g. *CDT v. Pappert*, 337 F.Supp.2d 606 (E.D. Penn. 2004) at 640 (citing evidence that IP filtering and DNS blocking led to the blocking of more than a million innocent web pages).

[32] For further analysis of S. 3804, see CDT, "Dangers of S. 3804: Domain Name Seizure and Blocking Pose Threats to Free Expression, Global Internet Freedom, and the Internet's Open Architecture," September 28, 2010, http://www.cdt.org/files/pdfs/Leahy_bill_memo.pdf.

[33] *See supra* n. 31 and accompanying text.

[34] Tory v. Cochran, 544 U.S. 734, 736 (2005) (internal quotes omitted).

[35] OpenNet Initiative Bulletin, "China's Green Dam: The Implications of Government Control Encroaching on the Home PC," OpenNet Initiative, July 27, 2009, http://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc.

[36] "Chinese curbs before anniversary," BBC News, June 2, 2009, http://news.bbc.co.uk/2/hi/asia-pacific/8078538.stm.

its enthusiasm for information control, many more moderate states are looking to China for successful strategies and tactics.

This trend illustrates how non-democratic or weak rule-of-law countries have begun to adopt the rhetoric of democratic, rule-of-law countries to deflect criticism of certain restrictive policies. In pursuing the goal of a free and innovative Internet, therefore, it is crucial that the U.S. lead by example. Congress and the Administration must reject policies and practices that limit Internet freedom here at home, and policymakers must be aware how their proposals, however well motivated, are perceived abroad. When we seek to expand our surveillance infrastructure or interfere with core Internet architecture, we implicitly endorse the actions of regimes that do the same in an effort to exercise political control. Issues of current debate inside the U.S. that have global implications for the free flow of information online include identity management and authentication, filtering and other child protection measures, intermediary liability, standards for government surveillance, intellectual property protection, and cybersecurity (including cooperation between U.S. companies and the intelligence agencies). Policy debates around these legitimate concerns must also assess the impact of policy proposals on the free flow of information and online innovation.

Recommendations: Role of the Department of Commerce

Make Internet freedom a condition of aid and trade negotiations. Require that trade agreements explicitly acknowledge the importance of the free flow of information online to businesses and consumers. Assert that blocking of U.S. content and services is a trade barrier. Reject proposals that would increase restrictions on information and use the negotiating process to raise objections to existing restrictions.

Promote protections for Internet intermediaries. Advocate for laws that protect Internet intermediaries from liability for user-generated content. Intermediaries are key enablers of the free flow of information online because they provide the conduits and platforms for a robust variety of content. Laws that impose liability on intermediaries for the third-party content they host or transmit will force intermediaries to scrutinize and limit the use of their services by all users.

Reach out to other democratic countries to collaborate on these efforts. Use the DOC's participation in national and regional fora to advocate a broader understanding of the free flow of information as a trade concern encourage adoption of less-restrictive policies by partner nations. Work with allies to press other nations to reform policies that restrict the free flow of information.

Strengthen interagency coordination to ensure various policies do not work at cross-purposes. The Department of State and the Department of Commerce have both declared a U.S. interest in promoting information flows on the one global Internet.[37] In pursuing the goal of a free and innovative Internet, the U.S. must lead by example. Congress and the Administration must reject policies and practices that limit information flows here at home, and policymakers must be aware how their proposals, however well motivated, are perceived abroad. The Department of Commerce should work with

[37] US Secretary of State Hillary Rodham Clinton, "Remarks on Internet Freedom," Washington, DC, January 21, 2010, http://www.state.gov/secretary/rm/2010/01/135519.htm.

policy counterparts across the U.S. government to ensure greater policy coherence in promoting information flows online while addressing other pressing policy concerns, domestically and abroad.

2. Identifying Best Practices

• How effective are local restrictions given the global nature of the Internet and the possibility of individual users circumventing government regulations?

The effectiveness of any proposed Internet-focused regulation is an essential consideration for policymakers. Policies should not be implemented simply based on a belief that *something* needs to be done to address a particular concern. Lawmakers must conduct a sober and realistic assessment of the benefits offered. In many cases, those benefits may be so limited that they do not outweigh the significant costs to information flows and innovation discussed elsewhere in these comments.

ISP-level filtering stands out as an example of such a policy. Countries increasingly turn to filtering as a means to address unwanted content, but there are strong reasons for skepticism that filtering will be effective in the long term. Implementing ISP-level filtering would almost certainly provoke an ongoing and ultimately futile arms race between filtering proponents and those seeking to avoid the filters. Increased sophistication of filters would be met with increased ingenuity in efforts to avoid them.[38] The prospect of such escalation raises serious questions as to whether automated filtering indeed offers the potential benefits its proponents suggest.

The domain-name blocking contemplated in COICA offers another example. This bill, recently reported out of the Senate Judiciary Committee, would empower the Attorney General to seek court orders forcing domain-name registries and registrars to lock domain names connected to sites "dedicated to infringing activity," or forcing ISPs to filter and block resolution of DNS requests for these domains. The Department of Homeland Security is currently pursuing a similar approach, seizing the domain names of websites that enable users to download infringing and counterfeit material. [39]

As in the case of automated content filtering, the effectiveness of this approach would likely prove fleeting at best. DNS blocking is easily circumvented in multiple ways. First, third-party public DNS servers are widely available, and if blocking is implemented domestically, more would inevitably spring up outside the United States to avoid being subject to blocking orders. For Internet users, pointing DNS requests to these unfiltered servers would be simply a matter of updating a single parameter in their operating systems' Internet settings.[40] Users who want to engage in infringement will thus easily

---

[38] *See* Peter Biddle et. al., *The Darknet and the Future of Content Distribution*, Microsoft Corp., 2002, http://msl1.mit.edu/ESD10/docs/darknet5.pdf.

[39] Immigration and Customs Enforcement Press Release, "ICE seizes 82 website domains involved in selling counterfeit goods as part of Cyber Monday crackdown," November 29, 2010. http://www.ice.gov/news/releases/1011/101129washington.htm.

[40] Indeed, when Comcast experienced a DNS outage in early December 2010 that affected many of its East Coast customers, instructions for users on how to point their DNS requests to alternate servers appeared in technology-focused and mainstream news outlets. *See* Andrew McDiarmid, "Comcast Outage Reveals DNS-blocking's Achilles' Heel," *CDT PolicyBeta Blog*, December 2, 2010, http://cdt.org/blogs/andrew-mcdiarmid/comcast-outage-reveals-dns-blocking%E2%80%99s-achilles%E2%80%99-heel

be able to route their traffic around DNS providers that enforce any blacklist. Second, users could enter IP addresses manually into their browsers and bookmark those addresses, bypassing the DNS system entirely. Third, since most operating systems come with DNS server functionality built in, users could set up local DNS servers on their own computers, thus avoiding any DNS servers that have been ordered to block. Finally, operators of blacklisted websites could distribute a small browser plug-in or other piece of software to allow users to retrieve the IP addresses of the operators' servers. Any combination of these circumvention techniques would dramatically limit DNS blocking's effectiveness at restricting access to online information.

• Are there alternatives to government-mandated restrictions on the flow of information on the Internet that can realize legitimate policy objectives?

For some policy objectives, effective alternatives exist to government-mandated restrictions on the free flow of information. For example, governments can take steps to address offensive (though lawful) expression – while minimizing any collateral impact on lawful expression and innovation – by empowering users to control what content reaches their screens. In the U.S., courts have consistently held that user-based solutions for restricting minors' access to inappropriate content online are preferable, both from an efficacy standpoint and a constitutional one, to government restrictions on speech.[41] The market has produced a broad array of user empowerment tools.[42] Such 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,[43] intrude on individual autonomy, and raise concerns around transparency and politically motivated content restrictions.[44]

---

[41] *See* Reno v. ACLU, 521 U.S. 544 (1997); Ashcroft v. ACLU, 542 U.S. 656, 666-67 (2004).

[42] 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/.

[43] 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.

[44] 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/; 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.

Recommendation:

Promote voluntary user empowerment tools as an effective solution to concerns about inappropriate content online. In negotiations and discussions with its foreign counterparts, the DOC can advocate for the role of voluntary user empowerment tools in achieving public policy goals related to online content. Particularly in the area of online child safety, concerns about sexual and violent content motivate many policy initiatives. User empowerment tools remain the most effective, and least restrictive, way to allow parents to decide what content is and is not appropriate for their own children.

3. Impact of Restricted Internet Information Flows on Innovation, Trade and Commerce

• How are traditional notions of jurisdiction, venue and choice of law evolving as services are offered on a global basis and data storage varies based on efficiency, rather than only legal, considerations?

As governments seek to regulate the flow of information online, questions of jurisdiction, of whether and to what extent they can regulate Internet content, are becoming increasingly prevalent. While a country's jurisdiction over the people, business, and activities that take place offline and within its borders is well settled, the Internet supports complicated multi-jurisdictional scenarios that have yet to be resolved. Some governments take a broad view of Internet jurisdiction and find that online material is subject to their jurisdiction if material is merely accessible in the country.[45] Multi-jurisdictional issues can arise even when all of the services (and thus all of the data) are in a single jurisdiction, especially if the service provider has business, marketing, or other offices in other jurisdictions.[46]

This jurisdictional uncertainty creates questions in the minds of users about which country's laws will govern their speech and the privacy of their data, and may discourage businesses from extending their services to or establishing physical operations in foreign countries. It also gives rise to issues such as "libel tourism," where a defamation plaintiff files suit in a country unrelated to the defamation claim, such as the UK, where it is relatively easy for a defamation plaintiff to prevail and where the courts are willing to exert jurisdiction over foreign defendants, as long as the material was obtainable in the UK.[47] In the Internet age, when content created in one jurisdiction

---

[45] One of the earliest examples of this view arose in Australia, where Australia's High Court held that the Dow Jones company was subject to the jurisdiction of Australian courts (and to the standards of Australian law) for allegedly defamatory material that appeared in an online version of one of its publications, despite the fact that the web site was produced and hosted in the U.S. and that it was available through a subscription service to only a handful of subscribers in Australia. Kurt Wimmer & Eve R. Pogoriler, "International Jurisdiction and the Internet" at 1, *available at* http://euro.ecom.cmu.edu/program/law/08-732/Jurisdiction/InternationalJurisdiction.pdf

[46] In one example, Belgium has sought to compel Yahoo! to disclose information located in U.S. servers, relying solely on Belgium law and ignoring the U.S.-Belgium treaty that governs cross-border law enforcement data requests. For more information on this specific case, *see* Cynthia Wong, *Yahoo! protects user privacy – and gets fined?,* PolicyBeta Blog, July 11, 2009, *available at* http://www.cdt.org/blogs/cynthia-wong/yahoo-protects-user-privacy-and-gets-fined.

[47] For example, in 2004, Rachel Ehrenfeld, the American author of the book *Funding Evil: How Terrorism is Financed – and How to Stop It* was sued for defamation in a UK court by a man she named as a possible financier of terrorism, Khalid Salim Bin Mahfouz. Even though the book had not yet been

is accessible in virtually any other, libel tourism can be a "mechanism for enforcing global censorship".[48] (In a positive development, the new UK government has pledged to review the country's famously plaintiff-friendly libel laws.[49]) In order to protect U.S. speakers from the threat of libel tourism, Congress recently passed the Securing the Protection of our Enduring and Established Constitutional Heritage (SPEECH) Act, which clarifies that U.S. courts can only enforce foreign defamation judgments when those adjudications provided at least as much protection for due process rights and the freedom of speech and the press as afforded by the U.S. Constitution.[50] The SPEECH Act further reinforces U.S. policy toward intermediaries, guaranteeing that a foreign judgment may only be enforced against intermediaries to the extent that it is consistent with Section 230.[51]

While this type of response, ensuring that U.S. standards of justice and policy are enforced by U.S. courts within U.S. jurisdictions, is perfectly appropriate, governments must be exceedingly careful when determining whether and how to assert jurisdiction over Internet content or portions of the Internet architecture. A key international issue over the past ten years has been "Internet governance," with many countries of the world concerned about what they perceive as undue U.S. control over the Internet, particularly because the U.S. continues to have some direct involvement in the management of the Domain Name System (DNS). An important aspect of American foreign policy under both Republican and Democratic administrations has been to reassure the global community that the United States would not abuse its position of oversight over the DNS. The alternative – sought by countries such as China, Brazil, and others – would have oversight of the DNS wrested from the U.S.-created ICANN and given to the International Telecommunications Union (ITU), which is controlled by the world's governments.

Proposals by U.S. policymakers, including COICA, that assert broad jurisdiction over domain names will significantly aggravate the situation, suggesting to the world that the U.S. does intend to use the historic nature of the DNS (with American companies

---

published in the UK, the court determined it had jurisdiction to hear the case because twenty-three copies of the book had been purchased online in the UK and because a portion of the book was also available on the web. This was not the first, nor the last, time that UK courts claimed jurisdiction because the alleged offending material was available online. *See* Todd W. Moore, Untying Our Hands: The Case for Uniform Jurisdiction Over "Libel Tourists," 77 Fordham L. Rev. 3243 (2009), law.fordham.edu/assets/LawReview/500flspub18464.pdf. *See also* Ron Chepesiuk, "Libel tourism", Global Journalist, 1 July 2004, http://www.globaljournalist.org/stories/2004/07/01/libel-tourism/.

[48] Christopher Walker, "Libel Tourism: The Globalization of Censorship", The International Herald Tribune, 16 March 2009, http://www.freedomhouse.org/template.cfm?page=72&release=788. See also IFEX, "Capsule Report: 'Libel Tourism' a growing threat to free speech, say ARTICLE 19 and Freedom House", 22 May 2008, http://www.ifex.org/united_kingdom/2008/05/22/capsule_report_libel_tourism_a/. Moreover, the effects of these adverse decisions are magnified by the UK's Internet publication rule, mentioned in Section I. Though UK libel laws may be the most infamous, Brazilian law also provides remedies for questionable affronts. Committee to Protect Journalists, "U.S. Reporter faces 'insult' suit in Brazil air crash aftermath", 29 Sept. 2009, http://cpj.org/2009/09/us-reporter-faces-insult-suit-in-brazil-air-crash.php.

[49] HM Government, "The Coalition: Our Programme for Government" at 11 (May 2010), http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_187876.pdf. *See also* Dinah Greek, "Changes to UK libel laws proposed", ComputerActive, 24 June 2010, http://www.computeractive.co.uk/computeractive/news/2264200/bill-proposes-changes-uk-libel.

[50] 28 U.S.C. 4102.

[51] 28 U.S.C. 1402(c).

administering ".com" and other leading top-level domains) to impose American law on the global Internet. Under COICA, the U.S. asserts that it can take down websites created and operated anywhere in the world, simply based on the fact that the websites use the most popular global top-level domain (.com). This type of assertion of global control is the kind of U.S. exercise of power about which other countries of the world have worried – and about which U.S. foreign policy has sought to reassure the world.

Historically, the United States has been the bulwark against censorship and government-imposed blocking of Internet content. If the United States sets the precedent that any country can seize or order the blocking of a domain name if some of the content on the domain (wherever located) violates the country's local laws, the effort to protect the rights of Internet users and the free flow of information will be critically harmed.

4. The Role of Internet Intermediaries

• To what extent do various governments' third party liability laws allow for immunity with exceptions for Internet intermediaries? How useful are such laws?

One of the most important issues facing the Internet is whether these technological intermediaries, such as ISPs or platforms for user-generated content (UGC), should be liable for the content created or transmitted by their users. In the U.S. and the EU, an early consensus emerged that intermediaries should not be liable for the content created by third parties and transmitted over the services of those intermediaries. This policy of protecting Internet intermediaries from liability fostered the growth and innovation that we enjoy today.[52]

However, this policy consensus appears to be fraying. Governments are increasingly turning technological intermediaries into online cops, seeking to force them to control the content created, posted, or transmitted by their users, or be held liable for it.[53] For a fuller discussion of these issues, see *supra* Section I.

• Are there specific principles or factors that governments should take into account when dealing with content restrictions and the intermediaries who might be in a good position to monitor postings and remove illegal or objectionable content?

Some countries require ISPs to implement a system to take down unlawful content when notified of it in order to qualify for immunity. Notice and takedown systems, however, are vulnerable to abuse in ways that can chill the free flow of information. 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

---

[52] In the U.S., 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 in U.S. law against liability also, importantly, insulates from challenge the efforts of intermediaries to identify, block and remove both child pornography and lawful but offensive content. These self-regulatory activities illustrate how a policy of protecting intermediaries from liability is compatible with – and can even help serve – other societal interests, such as protecting children.

[53] For more on the issue of intermediary liability in addressing unlawful behavior online, see Section I *supra* as well as CDT, *Intermediary Liability*, *supra* note 7.

factors related to the content at issue, including the effectiveness of user-controlled alternatives to address the harm and the 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 risk of abuse, since the host, facing the difficulty of assessing the copyright claim, may be inclined to cooperate with even spurious takedown requests.

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).[54] 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.[55]

• How might governments promote innovation in the provision of new intermediary services (e.g., by granting immunities), while at the same time encouraging responsible conduct by those same intermediaries?

The existing approach to intermediary liability under U.S. law has been remarkably successful at achieving the balance between promoting innovation and encouraging responsible conduct. In particular, Section 230 does so by not only shielding intermediaries from liability for content posted by others, but also from liability for actions taken to voluntarily remove objectionable content. The latter protection removes the disincentives to take down third-party content that would arise from fear of liability under tort, contract, or other claims. It also protects online service providers against the risk that any editorial decision might lead to liability for other objectionable content not

---

[54] 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).

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

taken down.[56] Thus, service providers are free to develop and enforce terms of service that allow market and normative forces, rather than mandates or liability fears, to dictate how they operate their services.

An alternative approach is to condition immunity on intermediaries' implementing notice-and-takedown policies under which objectionable content is removed upon notice from a third party. This is the approach taken by the DMCA, which has been in large part a successful in addressing copyrighted content. However, notice-and-takedown systems are not desirable in all cases. They are vulnerable to abuse by both governmental and private actors.[57] 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.[58] Intermediaries typically have little or no incentive to challenge a takedown request, even if they suspect the notice and takedown system is being abused.[59] Advocates have documented how these drawbacks can chill free expression.[60] Efforts to encourage more countries to impose liability on intermediaries in the name of copyright, especially when those countries do not have counterbalancing protections, thus raise concerns that intermediary liability frameworks could lead to increased monitoring by ISPs or other limitations on expression.[61]

These concerns are especially strong in the context of issues like defamation, where a server provider has no way to determine whether any particular content is in fact

---

[56] Indeed, Section 230 overturned an earlier court decision holding an ISP liable for content not removed based in part on its policy of filtering out some user content. See Stratton-Oakmont, Inc. v. Prodigy Services Co., 23 Media L. Rep. 1794 (NY Sup. Ct. May 26, 1995).

[57] 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. 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.

[58] 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), http://www.nartv.org/mirror/evasiontactics-indexoncensorship.pdf. US copyright law 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). But see also CDT, "Campaign Takedown Troubles: How Meritless Copyright Claims Threaten Online Political Speech," September 2010, http://www.cdt.org/files/pdfs/copyright_takedowns.pdf.

[59] 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.

[60] 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); Chilling Effects Clearinghouse, http://www.chillingeffects.org/index.cgi.

[61] Several countries (including the US 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 in the name of copyright protection. 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/.

defamatory. In the DMCA copyright context, the greatest problems have arisen with notice-and-takedown in the area of "fair use," which require a sometimes-difficult legal judgment to assess. Notice-and-takedown for defamation or other similar concerns would be even more problematic (because, for example, if a video alleges that "Mr. Smith had an affair" is defamatory, the service provider has no way to determine whether in fact the assert affair occurred, thereby making the content non-defamatory under U.S. law).

Chile and Brazil have sought to ameliorate some of these typical problems with notice-and-takedown regimes. Chile recently passed a bill limiting the liability of ISPs for copyright infringements by their customers that on its surface appears similar to the U.S.'s DMCA. However, unlike in the U.S., Chilean content hosts are not required to remove access to infringing material until notified by a court order.[62] In requiring a court order, rather than simply a privately issued notification, to initiate a takedown, Chile's law is designed to prevent the types of abuses that are possible under more traditional notice-and-takedown regimes. Meanwhile, as of writing, Brazil is debating a law that would provide general protections for intermediaries provided they comply with all court-issued takedown orders.[63]

6. International Cooperation

a. Complement voluntary, multi-stakeholder initiatives

Voluntary, multi-stakeholder initiatives can provide rich forums for problem solving and articulation of best practice. The Global Network Initiative (GNI) has become a key venue for ICT companies who want to chart an ethical path forward in an increasingly complicated global operating environment.[64] As we have outlined in the preceding sections, governments are increasingly turning to private technological intermediaries to enforce social policy. Companies are often asked to take actions that may harm the free flow of information online or undermine user trust by implicating user privacy. For example, in 2009, China asked computer manufacturers to pre-install the Green Dam filtering software on all computers sold in China in an attempt to further decentralize its

---

[62] Chapter III, Art. 85-L to 85-U, Ley N° 20435, Modifica La Ley N° 17.336 Sobre Propiedad Intelectual (4 May 2010), http://www.leychile.cl/Navegar?idNorma=1012827&idParte=&idVersion=2010-05-04. See also Vinod Sreeharsha, "No Safe Harbors in Argentina," NYTimes Bits Blog, Aug. 20, 2010, http://bits.blogs.nytimes.com/2010/08/20/no-safe-harbors-in-argentina/; "Chile Breaks New Ground in Regulating IP Liability," WIPO Magazine, June 2010, http://www.wipo.int/wipo_magazine/en/2010/03/article_0009.html. For a detailed legislative history of the law, from the perspective of intellectual property advocates, see International Intellectual Property Alliance, *Chile: International Intellectual Property Alliance 2010 Special 301 Report on Copyright Protection and Enforcement,* (Feb. 18, 2010), www.iipa.com/rbc/2010/2010SPEC301CHILE.pdf.

[63] *See* "New Draft Bill Proposition: Available for Download," Marco Civil da Internet, May 21, 2010, http://culturadigital.br/marcocivil/2010/05/21/new-draft-bill-proposition-available-for-download. The drafting process has been remarkable for its level of netizen input. *See "Sobre,"* Marco Civil da Internet, http://culturadigital.br/marcocivil/sobre/.

[64] For more on the GNI, we refer to the comments submitted by the GNI to this proceeding, Comments of the Global Network Initiative, In the matter of Global Free Flow of Information on the Internet, to the U.S. Department of Commerce, NTIA, Docket No. 100921457-0457-01, December 6, 2010.

censorship regime.[65] Many governments are increasingly building up surveillance and censorship capabilities using technologies developed in the west.[66]

The way in which companies respond to these complex human rights questions can have a substantial impact on the free flow of information online, as well as user trust in ICT and in American companies. The GNI provides a flexible framework for companies to systematically examine and mitigate the human rights risks their businesses face worldwide.

After extensive consultation, research, and benchmarking, the GNI produced a set of high-level Principles and detailed Implementation Guidelines that begin to develop a standard for corporate responsibility and human rights due diligence in the ICT sector. These Principles and Guidelines provide operational guidance for ethical company decision-making all around the world. GNI companies commit to implementing the Principles throughout their operations, conducting human rights risk assessments, and crafting strategies to mitigate risks presented – all with the help and support of human rights and technology policy experts, investors, and academics. The GNI also acts as a platform for collaboration on key issues of government policy and for collective action when emerging threats to the free flow of information or user privacy arise. Companies strengthen their hand when they work with other companies and non-company stakeholders to push back against government demands that impact human rights. In addition, the GNI is far more equipped to respond rapidly to unfolding events.

Companies who join the GNI not only benefit from this framework for engagement and collaboration, but also more credibly demonstrate their commitment to addressing human rights risk by engaging in a transparent and accountable way. The ultimate goal of the GNI's company assessment mechanism is to improve company processes and to enhance the Principles and Guidelines over time through a collaborative learning process. Increasing transparency around governmental restrictions and company practices, and promoting due process and the rule of law are at the core of the GNI's approach.

In our view, GNI offers the most promising path forward for companies to join with other key stakeholders to address the ethical challenges companies will face. While it may be possible for a company to find an alternative means of managing human rights risk, it is it is demonstrably clear that doing nothing is no longer an option. How companies respond to these risks will have a broad impact on the free flow of information online. Yet GNI will not achieve its full potential unless more companies join its effort. Currently, only Microsoft, Yahoo!, and Google have joined, though the GNI continues to reach out to a range of companies. [67]

---

[65] OpenNet Initiative Bulletin, "China's Green Dam: The Implications of Government Control Encroaching on the Home PC," OpenNet Initiative, July 27, 2009, http://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc.

[66] See, e.g., Helmi Noman, "Middle East Censors Use Western Technologies to Block Viruses and Free Speech," OpenNet Initiative Blog, http://opennet.net/blog/2009/07/middle-east-censors-use-western-technologies-block-viruses-and-free-speech; Naomi Klein, "China's All-Seeing Eye," Rolling Stone, May 29, 2008, http://www.rollingstone.com/politics/story/20797485/chinas_allseeing_eye/print.

[67] See also "Global Internet Freedom and the Rule of Law, Part II," Hearing of the Senate Judiciary Committee, Subcommittee on Human Rights and the Law, March 2, 2010, http://judiciary.senate.gov/hearings/hearing.cfm?id=4437; "Durbin Sends Letter to Technology Firms

Finally, we believe that governments could play a complementary role to the GNI in articulating a set of norms and expectations—shared by the U.S. and other democratic, rule-of-law states—for corporate human rights due diligence in the ICT sector. If appropriately structured to both promote due diligence while also nurturing innovation, such norms could provide greater legal certainty for responsible companies operating in the global market, while also promoting information flows

Recommendation: The Commerce Department could help U.S. companies navigate these difficult legal and ethical questions in several ways:

- Help U.S. companies develop, document, and promote best practices for responding to governmental requests to restrict information flows or assist in surveillance.
- Encourage companies to develop and implement tools for assessing risk to free flow of information that their business operations may pose.

b. Ensure policy coherence in U.S. positions at intergovernmental policy setting bodies

As the NOI notes, a number of different intergovernmental policy setting bodies have taken increasing interest in guiding the growth of the Internet, including the International Telecommunications Union (ITU), OECD, Council of Europe, and the Asia-Pacific Economic Cooperation (APEC) Forum. Many of these bodies are addressing specific areas of policy—for example, cybercrime, intermediary responsibility in advancing social policy, and child protection. As we have seen in many of the preceding examples, policies enacted to address these very legitimate concerns could also have an impact on the free flow of information.

In addition, policy norms articulated through these bodies could have wide influence on national policy, even if such norms take the form of non-binding recommendations. Yet these bodies have varying levels of formal civil society, consumer, or public interest involvement. (In the case of the ITU, civil society has no formal role at all.)

Recommendations: In light of these concerns, we urge the Task Force and the Department of Commerce to:

- Strengthen interagency collaboration to ensure various policies do not work at cross-purposes to promoting the free flow of information.

- Scrutinize positions taken in bilateral and multilateral treaties and within global policy bodies that may have an impact on the free flow of information.

- Seek public interest and civil society input in crafting U.S. government policy positions in all these venues.

* * * * *

Regarding Internet Freedom in China," February 2, 2010, http://durbin.senate.gov/showRelease.cfm?releaseId=322042.

We appreciate the Department's consideration of these comments, and we would welcome the opportunity work together to achieve our shared goals of promoting the free flow of information and commerce over the Internet.

Respectfully submitted,

John B. Morris, Jr.
Cynthia M. Wong
Emma J. Llanso
Andrew McDiarmid

Center for Democracy & Technology
1634 I Street, N.W., Suite 1100
Washington, D.C., 20001
202-637-9800

Endorsed by:

Association of Research Libraries
21 Dupont Circle, N.W., Suite 800
Washington, D.C. 20036
202-296-2296

American Library Association
1615 New Hampshire Ave, N.W., 1st Floor
Washington, D.C. 20009
202-628-8410

December 6, 2010