Internet Filtering in the **United States and Canada**

Introduction

Though neither the United States nor Canada practices widespread technical Internet filtering at the state level, the Internet is far from "unregulated" in either state.[1] Internet content restrictions take the form of extensive legal regulation, as well as technical regulation of content in specific contexts, such as libraries and schools in the United States. The pressure to regulate specific content online has been expressed in concerns related to four problems: child-protection and morality, national security, intellectual property, and computer security. In the name of "protecting the children," the United States has moved to step up enforcement of child pornography legislation and to pass new legislation that would restrict children's access to material deemed "harmful." Legislators invoke national security in calls to make Internet connections more traceable and easier to tap. Copyright holders have had the most success in this regard by pressing their claims that Internet intermediaries should bear more responsibility—and more liability—than they have in the past. Those concerned about computer security issues, such as badware and spam, have also prompted certain regulations of the flow of Internet content. In addition, in Canada, although not in the United States, publishing of hate speech is restricted.

Debate on each of these restrictions is heated. Public dialogue, legislative debate, and judicial review have resulted in different filtering strategies in the United States and Canada than those described elsewhere in this volume. In the United States, many government-mandated attempts to regulate content have been barred on First Amendment grounds. In the wake of these restrictions, though, fertile ground has been left for private-sector initiatives. The government has been able to exert pressure indirectly where it cannot directly censor. In Canada, the focus has been on government-facilitated industry self-regulation. With the exception of child pornography, Canadian and U.S. content restrictions tend to rely more on the removal of content than blocking; most often these controls rely upon the involvement of private parties, backed by state encouragement or the threat of legal

action.[2] In contrast to those regimes where the state mandates Internet service provider (ISP) action through legal or technical control, most content-regulatory urges in both the United States and Canada are directed through private action.

With only 5.1 percent of the world's population, the United States and Canada are home to 21.1 percent of the world's Internet users. Together their Internet penetration rate is 69.4 percent.[3] Canada and the United States, however, have not kept pace with many other countries in expanding broadband access, slipping in the global ranking of Internet broadband penetration rates to 11th and 16th, respectively, in 2006.[4] These high rates of Internet usage bring with them the ability of citizens to express dissenting points of view, as well as to engage in a large number of other activities (such as accessing pornography) that test a society's dedication to free expression and privacy. Like the states that actively filter the Internet through technical means, Canada and the United States are not immune from the ongoing challenges that these tests pose.

Regulating and filtering obscene and explicit content

It is a truism (i.e., repeated without necessarily being true) that pornographers are the first to embrace every new technology. The first sustained battle over content filtering in the United States broke out over sexually explicit material, particularly because of the perception that it is easily accessible and the fear that it can do harm to minors who access it online.

Canada has tended to act conservatively in response to online obscenity, while legislators in the United States have pursued broader definitions of offenses and mandates on Internet filtering. In its response to online sexually explicit material, Canada has made only *de minimis* amendments to pre-existing law.[5] Legislators have simply revised existing obscenity provisions to encompass online offenses. For example, the passage of the Criminal Law Amendment Act of 2001[6] established online acts of distributing and accessing child pornography and luring a child as crimes.[7] The Criminal Code mandates a system for judicial review of material (including online material) alleged to be child pornography. It does not, however, require ISPs to judge the legality of content posted on their servers or to take corrective action prior to a judicial determination.[8] If a judge determines that the material in question is illegal, ISPs may be required to take it down and to give information to the court to help in the identification and location of the person who posted it.[9]

Many Canadian ISPs, however, have begun to filter content hosted outside of Canada despite regulatory uncertainty in the area. For three days in July 2005, the Canadian ISP Telus blocked access to a Web site run by members of the Telecommunication Workers Union during a labor dispute containing what Telus argued was proprietary information and photographs that threatened the security and privacy of its employees.[10] This unilateral action by Telus broke the "cardinal rule" of Canadian ISPs—that they pass on any and all information without regard for content in exchange for immunity from liability over content. This action also conflicted with Section 36 of the Canadian Telecommunications Act, which states that, without the approval of the Canadian Radio-Television and Telecommunications Commission (CRTC), a "Canadian carrier shall not control the content or influence the meaning or purpose of telecommunications carried by it for the public."[11] Telus, however, argued that content filtering is permitted in the contract it holds with its subscribers, although, to the detriment of their argument, the blocking affected the customers of other ISPs that connect via Telus. The matter was resolved when, though the site was hosted in the United States,[12] Telus was able to obtain court orders from Alberta and British Columbia requiring the Web site operator, who

lives and works in Canada, to remove the offending materials.[13]

In August 2006 the Canadian human rights lawyer Richard Warman filed an application with the CRTC to authorize Canadian ISPs to block access to two hate speech sites hosted outside of Canada.[14] The CRTC denied the application, but the decision recognized that, although the CRTC cannot *require* Canadian ISP's to block content it, can *authorize* them to do. However, the CRTC noted that the "scope of this power has yet to be explored."[15]

In November 2006 Canada's largest ISPs launched Project Cleanfeed Canada in partnership with www.cybertip.ca, the nation's child sexual exploitation tipline. The project, modeled after a similar initiative in the United Kingdom, is intended to protect ISP customers "from inadvertently visiting foreign web sites that contain images of children being sexually abused and that are beyond the jurisdiction of Canadian legal authorities."[16] Acting on complaints from Canadians about images found online, www.cybertip.ca analysts assess the reported information and forward potentially illegal material to the appropriate foreign jurisdiction. If a URL is approved for blocking by two analysts, it may be added to the Cleanfeed Canada distribution list. Each of the participating ISPs voluntarily blocks this list without knowledge of the sites it contains, precluding ISP involvement in the evaluation of URLs. Blocked sites fail to load, but attempts to access them are not monitored and users are not tracked.[17]

Since Cleanfeed Canada is a voluntary program, the blocking mechanism is up to the discretion of the ISPs. Sasktel, Bell Canada, and Telus all claim to block only specific URLs, not IP addresses, in an attempt to avoid overblocking.[18] Besides the significant public outcry that would most likely result, overblocking may itself be illegal under the Telecommunications Act mentioned above.

Because accessing child pornography—as well as making it accessible—is unlawful in Canada, the filtering of such content does not infringe on rights of access or speech afforded by the Canadian Charter of Rights and Freedoms. Moreover, because ISP participation in Project Cleanfeed is voluntary, the blocking of sites through the project cannot be said to be state sponsored. However, the project remains controversial for other reasons. First, Cleanfeed Canada has not yet sought or received authorization from the CRTC. Second, the blacklist maintained by www.cybertip.ca remains secret, though necessarily, as publishing a "directory" of child pornography would itself be illegal. This lack of transparency inevitably generates distrust of the list and the process by which it is compiled. Third, the procedure for appealing the blocking of a site may have implications for anonymity.[19] A content owner or ISP customer may complain to the ISP or directly to www.cybertip.ca, which will reassess the site and, if necessary, obtain an independent and binding judgment from the National Child Exploitation Coordination Centre. It is unclear whether this process might expose the complainant's identity and create the potential for abuse of that individual's rights by the ISP or perhaps even by authorities.

Canada's response to online obscenity and its collaborative filtering initiative look restrained by contrast to the more vigorous regulatory efforts of the United States.

The United States Congress passed the Communications Decency Act (CDA) as part of the Telecommunications Act of 1996. Signed into law by President Clinton in February 1996, the CDA criminalized the transmission of "indecent" material to persons under eighteen and the display to minors of "patently offensive" content and communications.[20] The CDA took aim at both the speakers and service providers of indecent material, although it offered them each safe

harbor if they imposed technical barriers to minors' access.

Even before it took effect, the CDA was challenged in federal court by a group of civil liberties and public interest organizations and publishers who argued their speech would be chilled by fear of the CDA's enforcement. The three-judge district court panel concluded that the terms "indecent" and "patently offensive" were so vague that enforcement of either prohibition would violate the First Amendment.[21] "As the most participatory form of mass speech yet developed," Judge Dalzell wrote in a concurring opinion, "the Internet deserves the highest protection from governmental intrusion."[22] The U.S. Supreme Court affirmed this holding in 1997, invalidating the CDA's "indecency" and "patently offensive" content prohibitions.[23] In the landmark case *Reno v. ACLU,* the Court held that CDA was not the "least restrictive alternative" by which to protect children from harm. Rather, parent-imposed filtering could effectively block children's access to indecent material without preventing adults from speaking and receiving this lawful speech.[24]

U.S. lawmakers responded to the Supreme Court's decision in *Reno v. ACLU* by enacting the Child Online Protection Act (COPA)—a second attempt at speaker-based content regulation. In COPA, the Congress directed its regulation at commercial distributors of materials "harmful to minors."[25] The slightly narrower focus of COPA, nicknamed "son of CDA," did not solve the Constitutional problems that doomed the CDA. The district court enjoined COPA on First Amendment grounds.[26] As this volume went to press, the district court had just struck down COPA, finding it void for vagueness and not narrowly tailored to the government's interest in protecting minors. Once again, the court held that criminal liability for speakers and service providers was not the "least restrictive means" to accomplish the government's purpose because the private use of filtering technologies could more effectively keep harmful materials from children.

Plaintiffs successfully argued that CDA and COPA would chill the provision and transmission of lawful Internet content in the United States. Faced with the impossible task of accurately identifying "indecent" material and preemptively blocking its diffusion, ISPs would have been prompted to filter arbitrarily and extensively in order to avoid threatened criminal liability, while writers and publishers felt compelled to self-censor.

Stymied at restricting the publication of explicit material, Congressional leaders changed their focus to the recipient end of the equation. The Children's Internet Protection Act (CIPA) of 2000 forced public schools and libraries to use Internet filtering technology as a condition of receiving federal E-Rate funding. A school or library seeking to receive or retain federal funds for Internet access must certify to the FCC that it has installed or will install technology that filters or blocks material deemed to be obscene, child pornography, or material "harmful to minors."[27] The Supreme Court rejected First Amendment challenges to CIPA, holding that speakers had no right of access to libraries and that patrons could request unblocking.[28] In response, some libraries and schools have rejected E-Rate funding, but most have felt financially compelled to install the filters.

The aftermath of CDA, COPA, and CIPA has left the business of Internet filtering largely to private manufacturers competing for market share. Schools, businesses, parents, and other parties wishing to (or compelled to) block access to certain content have a broad range of competing software packages available to them. Some programs permit access only to whitelists of preapproved sites, but most services generate blacklists of blocked sites through automated screenings of the Web and, in some cases, real-time monitoring. Whatever their configuration, these products and the content they permit and

restrict reflect different normative choices about the subjects targeted for filtering. Indeed, it is developers first, and users second, who determine what gets filtered when such software is implemented.

Although CIPA mandates the presence of filtering technology in schools and libraries receiving subsidized Internet access, it effectively delegates blocking discretion to the developers and operators of that technology. The criteria "obscene," "child pornography," and "harmful to minors" are defined by CIPA and other existing legislation, but strict adherence to these (vague) legal definitions is beyond the capacity of filters and inherently subject to the normative and technological choices made during the software design process. Moreover, while CIPA permits the disabling of filters for adults and, in some instances, minors "for bona fide research or other lawful purposes,"[29] it entrusts school and library administrators with deactivating the filters, giving them considerable power over access to online content. Once FCC certification requirements have been met, it is these individuals who shoulder the burden of ensuring access to constitutionally protected material.[30]

In the single known U.S. attempt to install filtering deeper into the network, the Commonwealth of Pennsylvania in 2004 authorized the state attorney general (AG)'s office to force ISPs to block Pennsylvania residents' access to sites the AG's office identified as child pornography. A district court struck this regulation down on First Amendment grounds of overbreadth because the filters' imprecision blocked substantial lawful speech unrelated to child pornography.[31] Since both possession and distribution of child pornography are criminal in the United States, service providers do respond to requests to remove it from their networks and report it to the National Center for Missing and Exploited Children when they encounter it.

Defamation

As in other national contexts, the potential for legal liability for other civil violations, including defamation and copyright, constrains the publishers of Internet content and certain service providers in the United States and Canada. These pressures can have a "chilling effect" on lawful online content and conduct and can threaten the anonymity of users. The content and court adjudication of such laws is "state action," even when the lawsuits and threats are brought by private individuals or entities.

At common law, one crucial factor in determining liability for defamation is the provider's relation to the content—whether the provider functioned as a carrier, distributor, or publisher of the defamatory content. In the United States the common law has been overridden by a federal statute, a holdover portion of the CDA, 47 U.S.C. 230. A key part of the CDA survived judicial scrutiny. Section 230 immunizes ISPs for their users' defamation: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[32] Moreover, the First Amendment shields speakers from liability for much speech about public figures. In Canada ISPs must still find their fit within the traditional categories, where they can escape liability if they are carriers or distributors, transmitting data without discrimination, preference, or regard for content, or may face liability as publishers if they exercise editorial control over material. Thus, while Canadian and U.S. service providers share the right to remove content voluntarily, those in Canada do not have the broad discretion or protection enjoyed by those in the United States, and may be compelled to take down allegedly defamatory content (e.g., postings to message boards) under threat of suit.

Copyright

U.S. copyright law has also evolved more quickly—perhaps even hastily—than Canadian law in

addressing the issue of service provider liability and in encouraging removal of infringing material. The "Online Copyright Limitations of Liability Act," a part of the Digital Millennium Copyright Act (DMCA) of 1998,[33] gives service providers a "safe harbor" from liability for their users' copyright infringements provided they implement copyright policies and a notice-and-takedown regime. Where a service provider unknowingly transmits, caches, retains, or furnishes a link to infringing material by means of an automatic technical process, it is protected from monetary liability so long as it promptly removes or blocks access to the material upon notice of a claimed infringement.[34] (The ISPs' CDA 230 immunity discussed above applies primarily in the context of defamation matters and explicitly excludes intellectual property offenses.)

The notice-and-takedown provision has been seen as giving copyright owners—potentially anyone who has fixed an "original work of authorship"—unwarranted leverage over service providers and their subscribers. When a provider is notified of an alleged infringement, risk aversion encourages it to remove or disable access to the specified material, probably without first informing the subscriber. The subscriber may file a counter-notice and have the content restored if the copyright owner does not file a claim in court,[35] but such challenges are rare. Subscribers, like the providers hosting their Web sites, are more likely to concede to takedown pressures, even when an infringement may not actually be occurring. If a subscriber is sued, his or her identity may be subpoenaed, as in cases of defamation, and with similarly little judicial scrutiny.[36] Major search engines such as Google comply with hundreds of removal requests a month, when it is not even clear that provision of a hyperlink would incur copyright liability.[37]

As Canada began to consider amending its copyright laws, it appeared to be following in the footsteps of the United States. In 2004, the House of Commons Standing Committee on Canadian Heritage re-tabled its *Interim Report on Copyright Reform,* which proposed a notice-and-takedown policy similar to that of the DMCA, under which Canadian service providers would be compelled to remove content immediately upon receiving notice of an alleged infringement from a professed copyright holder. The *Report* came under fire from the Canadian Internet Policy and Public Interest Clinic (CIPPIC), Digital Copyright Canada, and the Public Interest Advocacy Centre (PIAC); numerous petitions and critiques have followed, calling for balance between the rights of content creators and fair public use. The government seems to be responding to these inputs as it continues to consider changes to copyright legislation.[38]

In the midst of this period of copyright uncertainty, Canadian ISPs have implemented a notice-and-notice policy for handling copyright infringement. Originally proposed in the now-defunct Bill C-60, which was dropped from the legislative agenda in 2005 with the collapse of the Liberal government,[39] the policy allows copyright owners to send notices to ISPs regarding possible copyright infringement by subscribers. The ISPs then forward the notices to their subscribers requesting them to desist in their illegal activities.[40] Even though the notices do not mean that immediate legal action will follow if infringing activities do not cease, they have been successful in getting significant portions of infringing subscribers to remove their materials.[41]

At present, however, protections against defamation and copyright infringement afforded under U.S. and Canadian law remain in tension with the rights of service providers and Internet users, often giving rise to the censoring and self-censoring of material. Canadian service providers erring on the side of caution may remove content from subscribers' sites, as U.S. providers do when informed of alleged copyright violations. User material is therefore subject to censorship based on unsubstantiated claims. Moreover, because subpoenas offer plaintiffs an

avenue for ascertaining subscribers' identities without scrutiny, the potential for misuse of these subpoenas can instill a fear of improper discovery in subscribers that leads to self-censorship. These chilling effects have been well documented,[42] and while they are indirect rather than direct state-mandated filtering, they do constitute real censorship of online speech.[43]

National security, computer security

Security concerns drive many of the state-mandated limitations on the speech and privacy interests of citizens. These security concerns in the United States and Canada take two forms: national security and computer security.

Concerns related to national security have led more to online surveillance by the state than to content filtering. The Bush Administration's warrantless wiretaps are reported to have included taps on major Internet interconnect points and data-mining of Internet communications.[44] Tapping these interconnect points would give the government the ability to intercept all overseas and many domestic communications. At press time, the U.S. government has moved to dismiss lawsuits filed against it and against AT&T by asserting the state secrets privilege; district courts in California and Michigan have refused to dismiss the lawsuits. If the allegations prove to be true, they show that the United States maintains the world's most sophisticated Internet surveillance regime. The Bush Administration is pushing to expand the Communications Assistance to Law Enforcement Act (CALEA) to force providers to give law enforcement wiretap access to electronic communications networks. Attorney General Gonzales has called for data retention laws to force ISPs to keep and potentially produce data that could link Internet subscribers to their otherwise-anonymous communications.[45]

Canadian electronic surveillance, primarily undertaken by the National Defense's secretive Communications Security Establishment (CSE), operates in close cooperation with U.S. and other allied intelligence networks. Although bound by Canadian laws and prohibited from eavesdropping on solely domestic Canadian communications without explicit ministerial approval, the CSE's activities are highly secret and oversight is minimal.

Computer security has led to certain content restrictions in the United States and Canada. Concerns about unwanted messages reaching computers, in various flavors of spam, have prompted content-based restrictions such as the CAN-SPAM Act of 2003 in the United States. In Canada a National Task Force on Spam was convened in 2005 to study the spam problem. While some laws, such as the Personal Information Protection and Electronic Documents Act, were found to at least tangentially apply to spam, the Task Force found a need for legislation directly limiting spam, which has yet to be passed.[46] The U.S. Congress has considered a range of options for limiting the free flow of bits across the Internet to address the problem of bad applications infecting computers, though most of the efforts to filter information based upon content deemed to be a computing security risk are carried out by private firms or individuals on a voluntary basis.[47] Calls are also being made to consider ISP liability in order to contain the worst of "zombie" computers sending spam and distributing badware, in the interest of preserving network safety for other connected PCs. In sum, there is still an active, ongoing discussion about how and why regulation of the flow of obviously malicious code over the Internet might take place.[48]

Conclusion

Although the United States and Canadian Internet are often thought to be relatively free from technical Internet filtering, Internet activity is far from "unregulated." With respect to online surveillance, the United States may be among the most aggressive states in the world in terms of monitoring online conversations. Lawmakers in both countries have imposed Internet-specific

regulation that can limit their citizens' access and view of the Internet. In addition, they have empowered private individuals and companies to press Internet intermediaries for content removal or to carry out the filtering in the middle of the network. Although the laws are subject to legislative and judicial debate, these private actions may be less transparent. Governments in both countries, however, have experienced significant resistance to their content restriction policies and, as a result, the extreme measures found in some of the more repressive countries of the world have not gained ground in North America.

Authors: Kevin O'Keefe, John Palfrey, Wendy Seltzer

NOTES

1. See Jack Goldsmith and Tim Wu, "How governments rule the Net," chapter 5, pp. 65–84, in *Who Controls the Internet: Illusions of a Borderless World,* New York: Oxford University Press, 2006.
2. See John Palfrey and Robert Rogoyski, "The Move to the Middle: The Enduring Threat of Harmful Speech to the End-to-End Principle," *Washington University Journal of Law and Policy* 21: 31–65, (2006).
3. Internet World Stats, "Internet usage statistics for the Americas," http://www.internetworldstats.com/stats2.htm.
4. International Telecommunication Union, *World Telecommunication Indicators 2006.*
5. This approach was first recommended in a 1997 study commissioned by Industry Canada. See Internet Content-Related Liability Study, "Conclusion," http://strategis.ic.gc.ca/epic/internet/insmt-gst.nsf/en/sf03316e.html.
6. Passed as Bill C-15a, 1st Session, 37th Parl., 2001.
7. R.S. 1985, c. C-46, §§163.1(3), 163.1(4.1), 172.1.
8. Project Cleanfeed Canada, Frequently Asked Questions, http://www.cybertip.ca/en/cybertip/cf_faq; R.S., 1985, c. C-46, §IV, http://laws.justice.gc.ca/en/showdoc/cs/C-46/bo-ga:l_V//en#anchorbo-ga:l_V.
9. R.S., 1985, c. C-46, §164.1, http://laws.justice.gc.ca/en/showdoc/cs/C-46/bo-ga:l_V//en#anchorbo-ga:l_V.
10. Michael Geist, "Telus breaks ISPs's cardinal rule," Toronto Star, August 1, 2005, http://www.michaelgeist.ca/index.php?option=content&task=view&id=919. OpenNet Initiative, "Telus Blocks Consumer Access to Labour Union Web Site and Filters an Additional 766 Unrelated Sites" http://opennet.net/bulletins/010/.
11. Telecommunications Act, R.S.C., ch. 38, §§27(2), 36, http://www.crtc.gc.ca/eng/LEGAL/TELECOM.HTM; see also Michael Geist, "Telus breaks ISPs's cardinal rule," *Toronto Star,* August 1, 2005, http://www.michaelgeist.ca/index.php?option=content&task=view&id=919.
12. OpenNet Initiative, "Telus Blocks Consumer Access to Labour Union Web Site and Filters an Additional 766 Unrelated Sites" http://opennet.net/bulletins/010/.
13. See "TELUS removes blocking from VFC website," July, 28, 2005, http://www.voices-for-change.ca/news/archive.asp?PagePosition=2.
14. http://www.crtc.gc.ca/PartVII/eng/2006/8646/p49_200610510.htm.
15. http://www.crtc.gc.ca/archive/ENG/Letters/2006/lt060824.htm.
16. See "ISPs and tipline set up battle against Internet child exploitation," November 24, 2006, http://www.cybertip.ca/en/cybertip/cleanfeed_canada.
17. See Project Cleanfeed Canada, Frequently Asked Questions, http://www.cybertip.ca/en/cybertip/cf_faq.
18. "Cleanfeed Canada: What would it accomplish?" http://yro.slashdot.org/article.pl?sid=06/12/15/1624215.
19. See Project Cleanfeed Canada, "Appeal process," http://www.cybertip.ca/en/cybertip/cf_appeal.
20. 47 U.S.C.A. §223(a), §223(d) (Supp. 1997).
21. *ACLU v. Reno,* 929 F. Supp. (E.D. Pa. 1996) at 854-865.
22. *ACLU v. Reno,* 929 F. Supp. (E.D. Pa. 1996) at 883.
23. *Reno v. ACLU,* 521 U.S. 844 (1997).
24. Ibid. "The Government may not 'reduce the adult population . . . to . . . only what is fit for children.' 'Regardless of the strength of the government's interest' in protecting children, 'the level of discourse reaching a mailbox simply cannot be limited to that which would be suitable for a sandbox.'"
25. 47 U.S.C. §231.
26. *ACLU v. Reno,* No. 98-5551 (E.D. Pa. 1999) Memorandum and Order granting preliminary injunction.
27. See Federal Communications Commission, What CIPA Requires, http://www.fcc.gov/cgb/consumerfacts/cipa.html.
28. *United States v. American Library Association,* 539 U.S. 194 (2003).
29. 20 U.S.C. §6777(c); 20 U.S.C. §9134(f)(3); 47 U.S.C. §254(h)(6)(D).
30. For examples of how libraries and schools have responded to CIPA, see Marjorie Heins, Christina Cho, and Ariel Feldman, Internet Filters: A Public Policy Report (2006), pp. 4–7, www.brennancenter.org/dynamic/subpages/download_file_36644.pdf.
31. *CDT v. Pappert,* 337 F.Supp.2d 606 (E.D. Penn. 2004). For an extensive analysis, see Jonathan Zittrain, "Internet points of control," 44 B.C. L. Rev. 653 (2003).

32. 47 U.S.C. §230(c)(1).
33. Pub. L. No. 105-304, 112 Stat. 2860 (1998).
34. 17 U.S.C. §§512(a)-(d).
35. 17 U.S.C. §512(g).
36. 17 U.S.C. §512(h).
37. See Chilling Effects, http://www.chillingeffects.org/dmca512/.
38. See Department of Canadian Heritage: Copyright Policy Branch, Government Statement on Proposals for Copyright Reform, http://pch.gc.ca/progs/ac-ca/progs/pda-cpb/reform/statement_e.cfm.
39. Online Rights Canada, "What are copyright reform and Bill C-60?" December 7, 2005, http://www.online-rights.ca/learn/what_is_c-60/.
40. Michael Geist, "The effectiveness of notice and notice," February 2007, http://www.michaelgeist.ca/content/view/1705/125/.
41. CBC News, "Email warnings deter Canadians from illegal file sharing," February 15, 2007, http://www.cbc.ca/consumer/story/2007/02/14/software-warnings.html.
42. See the work of Chilling Effects Clearinghouse, www.chillingeffects.org.
43. See Wendy Seltzer, "Unsafe harbors: Abusive DMCA subpoenas and takedown demands," http://www.eff.org/IP/P2P/20030926_unsafe_harbors.php#_edn3.
44. James Risen and Eric Lichtblau, "Spy agency mined vast data trove, officials report," *The New York Times,* December 24, 2005.
45. Declan McCullagh, "Gonzales pressures ISPs on data retention," May 2006, http://news.com.com/Gonzales+pressures+ISPs+on+data+retention/2100-1028_3-6077654.html.
46. Michael Geist, "Spam plans," March 15, 2007, http://www.michaelgeist.ca/content/view/1805/125/.
47. Consider, for instance, the interstitial pages that search giant Google places between search results and certain pages on the Internet deemed to host badware that might harm an end-user's computer. See http://stopbadware.org.
48. See, for example, Jonathan Zittrain, *The Future of the Internet and How to Stop It,* chapters 7 and 8 (forthcoming 2007), (discussing various methods for tempering the badware problem through code, law, and social reforms).

Country Summaries