United States and Canada Overview

The Internet in the United States and Canada is highly regulated, supported by a complex set of legally binding and privately mediated mechanisms. Technical filtering plays a minor role in this regulation. The first wave of regulatory actions in the 1990s in the United States came about in response to the profusion of sexually explicit material on the Internet within easy reach of minors. Since that time, several legislative attempts at creating a mandatory system of content controls in the United States have failed to produce a comprehensive solution for those pushing for tighter controls. At the same time, the legislative attempts to control the distribution of socially objectionable material on the Internet in the United States have given rise to a robust system that limits liability over content for Internet intermediaries such as Internet service providers (ISPs) and content hosting companies. Proponents of protecting intellectual property online in the United States have been much more successful, producing a system to remove infringing materials that many feel errs on the side of inhibiting legally protected speech. National security concerns have spurred on efforts to expand surveillance of digital communications and fueled proposals for making Internet communication more traceable.

After a decade and half of ongoing contentious debate over content regulation in the United States, the country is still very far from reaching political consensus on the acceptable limits of free speech and the best means of protecting minors and policing

illegal activity on the Internet. Gambling, cyber security, and dangers to children who frequent social networking sites—real and perceived—are important ongoing debates.

Canadian legislators have been less aggressive than their U.S. counterparts in proposing specific legislative remedies for problems arising from Internet use. Canadians have been more inclined to employ existing regimes developed for regulating offline speech and less apt to propose broad solutions. Canadians do not currently pursue copyright infringement online with the same zeal as their U.S. counterparts. Neither does Canadian law provide the same formal protection for intermediaries. Unlike the United States, publishing of hate speech is restricted in Canada. Under section 320.1 of the Canadian Criminal Code, a judge can issue a warrant authorizing the deletion of (publicly available) online hate propaganda from computer systems located within the jurisdiction of the court.

Public dialogue, legislative debate, and judicial review have produced filtering strategies in the United States and Canada that are different from those described elsewhere in this volume. In the United States, many government-mandated attempts to regulate content have been barred on First Amendment grounds, often after lengthy legal battles.[1] However, the United States 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 much of the world, where ISPs are subject to state mandates, most content regulation in the United States and Canada occurs at the private level.

The United States and Canada both have relatively high Internet penetration rates. In each country, nearly three-quarters of the population has access to the Internet.[3] Despite such high Internet penetration rates, the two countries have relatively low broadband subscription rates, with the United States at 23 percent and Canada at 28 percent. Internet subscription rates on the whole are only slightly higher: the United States has a 24 percent subscription rate, while Canada's rests at 31 percent.[4] The broadband stimulus push of President Barack Obama's administration in early 2009 may improve these rates in the United States.

These high rates of Internet usage increase the ability of citizens to publish and widely distribute dissenting points of view. At the same time, Internet users engage in a large number of other online activities, such as accessing pornography, that test a society's dedication to free expression and privacy.

Regulating Obscene and Explicit Content

The United States Congress passed the Communications Decency Act (CDA) as part of the Telecommunications Act of 1996. Signed into law by President Bill Clinton in

February 1996, the CDA was designed to criminalize the transmission of ''indecent'' material to persons under 18 and the display to minors of ''patently offensive'' content and communications.[5] The CDA took aim not only at the authors of ''indecent'' material but also at their Internet service providers, although it offered them each safe harbor if they imposed technical barriers to minors' access.[6]

Prior to taking 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 sufficiently vague such that enforcement of either prohibition would violate the First Amendment.[7] ''As the most participatory form of mass speech yet developed,'' Judge Stewart Dalzell wrote in a concurring opinion, ''the Internet deserves the highest protection from governmental intrusion.''[8] The U.S. Supreme Court affirmed this holding in 1997, invalidating the CDA's ''indecency'' and ''patently offensive'' content prohibitions.[9] 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.[10] Other sections of the CDA continue to remain in force, including Section 230, which provides immunity to ISPs for content that third-party users place online.[11] Section 230 has had an undeniably powerful impact in promoting free speech in the United States. A growing body of case law suggests that it is being used by ISPs to settle or quickly dismiss claims that are brought against them.[12] Many question whether the sweeping protections offered by Section 230 offer in fact too much protection for online speech and excessively limit the ability of victims and the state to suppress harmful speech.[13]

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 U.S. Congress directed its regulation at commercial distributors of materials ''harmful to minors.''[14] The slightly narrower focus of COPA did not solve the constitutional problems that doomed the CDA. The district court enjoined COPA on First Amendment grounds.[15] After a few trips to the Supreme Court and back for fact-finding, the district court issued its ruling in March 2007, finding COPA 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. The Third U.S. Circuit Court of Appeals later affirmed this decision, and, in January 2009, the Supreme Court put the legislation to rest—at least for now—by refusing to hear the case.

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 the threat of criminal liability, while writers and publishers would feel compelled to self-censor.

Stymied at restricting the publication of explicit material, congressional leaders changed their focus to regulating what someone might hear, rather than what they say. 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.''[16] 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.[17] In response, some libraries and schools have rejected E-Rate funding,[18] but most have felt financially compelled to install the filters.

In the aftermath of CDA, COPA, and CIPA, Internet filtering in the United States is carried out largely by private manufacturers. These companies compete for market share in a lucrative business area. Schools, businesses, parents, and other parties wishing to block access to certain content have a broad range of software packages available to them.[19] While some programs filter heavily, permitting access only to a ''white list'' of preapproved sites (for example, those appropriate for young children), others generate blacklists of blocked sites through a combination of automated screenings of the Web, staff members who ''rate'' sites on appropriateness, and user complaints.

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 rather 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,''[20] 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.[21]

Attempts to filter Internet content in the United States have also reached the state level. In 2004, Pennsylvania authorized the state attorney general's office to force ISPs to block Pennsylvania residents' access to sites that the attorney general's office identified as child pornography.[22] A district court struck down this regulation as unconstitutional where this state law in effect was regulating activity occurring

wholly outside the state's borders, but did not strike down the act due to overbreadth.[23] The court noted that "there is an abundance of evidence that implementation of the Act has resulted in massive suppression of speech protected by the First Amendment."[24]

The complexities of government-led efforts to restrict online speech have given rise to quasi-voluntary initiatives supported by the force of law. Since possession and distribution of child pornography are criminal acts in the United States, service providers respond to removal requests and report any requests to the National Center for Missing and Exploited Children. In June 2008, the New York state attorney general signed an agreement with Comcast, AT&T, Inc., AOL, Verizon Communications, Inc., Time Warner Cable, and Sprint to purge their servers of child pornography identified by the National Center for Missing and Exploited Children.[25] The agreement attempts to curtail access to child pornography by implementing a new system to rapidly identify child pornography images as well as responding to user complaints about child pornography. In addition, several ISPs agreed to stop supporting access to Usenet newsgroups, identified by the attorney general's office as a source of child pornography.

The desire to protect children from harm online continues to drive efforts at content-based restrictions on the Internet. Law enforcement agencies use pressure to convince private companies to take on voluntary Internet regulatory initiatives. Concerns over child safety online have focused attention on the potential risks associated with time spent on social network sites such as Facebook and MySpace, where children may come into contact with sexual predators and be subject to cyberbullying by their peers. Law enforcement officials in the United States have been vocal in promoting age and identity verification systems in order to better police online sites frequented by minors.[26] The Internet Safety Technical Task Force, a group of technology companies, Internet businesses, nongovernmental organizations, and academics, was brought together by agreement with 49 U.S. state attorneys general to study the use of technologies by industry and end users to promote Internet safety for minors. The task force report of January 2009 recommended a model of collaboration among industry groups, law enforcement, and others rather than implementation of a series of mandatory technical controls to protect children online.

Another U.S. legislative attempt to control online speech, the Megan Meier Cyberbullying Prevention Act, would criminalize "severe, repeated and hostile" speech online.[27] This proposed legislation, named after a girl who committed suicide thought to be induced by online harassment, has been harshly criticized as unnecessary, given the existing off-line remedies for harassment, and for its potential impact on protected online speech, as it could be applied to many incidents of online speech far beyond the cyberbullying targeted by the legislation.[28] Seventeen of the 50 states have passed laws against cyberbullying.[29]

While legislators in the United States have pursued broader definitions of offenses and mandates on Internet filtering, Canada has tended to act conservatively in response to online obscenity. In its response to online sexually explicit material, Canada has made only de minimis amendments to preexisting law.[30] Legislators have simply revised existing obscenity provisions to encompass online offenses. For example, the passage of the Criminal Law Amendment Act of 2001 established online acts of distributing and accessing child pornography and luring a child as crimes.[31] 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.[32] If a judge determines that the material in question is illegal, ISPs may be required to take it down and help the court identify and locate the person who posted it.[33]

There have been instances in Canada of ISPs attempting 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.[34] This unilateral action by Telus deviated from the general practice of Canadian ISPs to pass on any and all information without regard for content in exchange for immunity from liability over content.[35] 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.''[36] Telus's blocking also affected the customers of other ISPs that connect via Telus.[37] The matter was resolved when 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 (the site was hosted in the United States).[38]

In August 2006, 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.[39] The CRTC denied the application, but the decision recognized that although the CRTC cannot require Canadian ISPs to block content, it could authorize them to do so. However, the CRTC noted that the ''scope of this power has yet to be explored.''[40] In a 2009 decision by an Ontario court, Richard Warman was successful at getting an order for a Web site to disclose the identities of eight of its anonymous contributors.[41] The decision has been appealed by the defendants.[42] The rules that the court relied on were general duty of disclosure rules in Ontario civil procedure that were not written with the intent of applying to this situation. The state of court involvement in online speech therefore remains uncertain.

In November 2006, Canada's largest ISPs launched Project Cleanfeed Canada in partnership with 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."[43] Acting on complaints from Canadians about images found online, 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 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.[44]

Since Project 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.[45] Beside the significant public outcry that would most likely occur, overblocking itself may be illegal under the Telecommunications Act mentioned previously.

Under Section 163 of the Canadian Criminal Code, accessing child pornography—as well as making it accessible—is unlawful.[46] Therefore, the filtering of such content does not infringe on rights of access or speech afforded by the Canadian Charter of Rights and Freedoms within Canada's constitution. 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, Project Cleanfeed has not yet sought or received authorization from the CRTC. Second, the blacklist maintained by Cybertip.ca remains secret, 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.[47] A content owner or ISP customer may complain to the ISP or directly to 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 a potential for abuse of that individual's rights by the ISP or perhaps even by authorities.

Canada's response to online obscenity and its voluntary filtering initiative are minimal in contrast to the more vigorous regulatory efforts of the United States.

Regulation of Online Gambling

In 2006, the United States House of Representatives passed legislation designed to limit online gambling by prohibiting the transfer of funds to gambling sites. The Unlawful

Internet Gambling and Enforcement Act (UIGEA), which was slipped into the SAFE Port Act,[48] banned gambling, prohibited online poker sites and other betting companies from ''knowingly accepting'' money from United States–based customers, and encouraged financial institutions to deny Internet gambling transactions. Since the act's inception, its legality has been in question.[49]

Two states in the United States have attempted to further limit gambling online. In October 2008, a circuit court judge in the state of Kentucky granted a request by the governor to have 141 Web sites used by online gaming operations transferred to state control.[50] In January 2009, following a petition filed by members of the Center for Democracy and Technology, the Electronic Frontier Foundation, and the American Civil Liberties Union of Kentucky,[51] a Kentucky appeals court overturned the judge's request.[52] In May 2009, John Willems, director of the Alcohol and Gambling Enforcement Division (AGED) of Minnesota's Department of Public Safety (DPS), filed an order requiring that 11 ISPs, including Comcast, Charter, and Verizon Wireless, prevent state residents from reaching approximately 200 gambling sites.[53] iMEGA (Interactive Media, Entertainment, and Gaming Association) had filed a lawsuit against Willems seeking an injunction to block implementation of the AGED order,[54] which was later dropped when the Minnesota DPS reached a settlement with iMEGA. ISPs are no longer required to block state residents' access to gambling sites.[55]

In 2008, Representative Barney Frank (Democrat, Massachusetts) again announced plans to introduce legislation aimed at overturning the UIGEA.[56] He had failed a previous attempt in 2007 in the form of an act entitled the Internet Gambling Regulation and Enforcement Act.[57]

The legality of online gambling in Canada is unclear, as few gaming cases exist to provide guidelines, although persons running online gaming operations can be subject to criminal liability.[58] As a result, offshore gambling sites are currently legal to use in Canada.[59] Advertising of such services is generally held to be illegal in Canada.

Defamation

As in other countries, the potential for legal liability for 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 constitute state action, even when the lawsuits and threats are brought by private individuals or entities.

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 many of their users' actions including defamation (copyright and criminal activity is excluded): ''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.''[60] Moreover, the First Amendment shields speakers from liability for much speech about public figures.[61]

Canada has no statutory equivalent to the statutory protection for ISPs under CDA 230. However, Canadian case law suggests that ISPs are entitled to a certain degree of immunity: in June 2004, the Supreme Court of Canada unanimously held that ISPs cannot be held liable for violations of Canadian copyright law committed by their subscribers.[62] The decision ruled that the act of caching content by an ISP would not make it liable and that an ISP's knowledge of potential infringements by subscribers is not necessarily sufficient to create liability either.[63] In Canada, ISPs are therefore able to escape liability if they prove that they are merely acting as ''conduits.''[64] They may, however, face liability as publishers if they exercise editorial control over material. This situation stands in contrast to the United States, where CDA 230 provides publisher immunity to ISPs, limited only where the provider or host has acted as an ''information content provider'' and actually created some or all of the content.[65] An important caveat to the U.S. immunity is that it does not apply to intellectual property law—while the Canadian situation exemplified in the case described earlier does provide immunity to ISPs regarding intellectual property matters such as copyright.[66] Overall, both Canadian and U.S. service providers receive legal protections that favor the protection of free speech online. Canadian ISPs, however, lack the clearly set out statutory protection that exists in the United States and may feel compelled to take down allegedly defamatory content (e.g., postings to message boards) when threatened with the possibility of costly lawsuits.

Copyright

U.S. copyright law has evolved more quickly than Canadian law both in addressing the issue of ISP 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,[67] gives service providers a ''safe harbor'' from liability for their users' copyright infringement provided they implement copyright policies and provides the legal basis for 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 liability so long as it promptly removes or blocks access to the material upon notice of a claimed infringement.[68] Section 512 (c) of the DMCA[69] provides that ''a service provider shall not be liable for monetary relief, . . . , for injunctive or other equitable relief, for infringement of copyright by reason

of the storage at the direction of a user of material that resides on a system or network . . . if the service provider

- does not have actual knowledge that the material or an activity using the material on the system or network is infringing;
- in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or
- upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;
- does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and
- upon notification, . . . responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.''

The notice-and-takedown provisions of the DMCA have been put to broad use and have proven to be an effective instrument for combating copyright infringement online. This has also 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 counternotice and have the content restored if the copyright owner does not file a claim in court, but such challenges are rare.[70] 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.[71] Major search engines such as Google comply with hundreds of removal requests a month, even though it is not even clear that provision of a hyperlink would incur copyright liability.[72]

When 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 retabled 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 followed, calling for balance between the rights of content creators and fair public use.[73] The ''Canadian DMCA'' has since been proposed, in the form of Bill C-61 in 2008, which appears to be even more restrictive that the U.S. DMCA.[74] The consensus on this bill is that it is unlikely to pass, although it continues to be a priority of the Conservative government.[75]

With no legislation yet enacted, Canadian ISPs have implemented a ''notice and notice'' policy for handling copyright infringement. This policy would be continued under Bill C-61.[76] ''Notice and notice'' was a concept 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.[77] Under this policy, copyright owners send notices to ISPs regarding possible copyright infringement by subscribers. Providers then forward these notices to their subscribers—instead of being obligated themselves to remove the content.[78] 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.[79]

Legal protections against defamation and copyright infringement afforded under U.S. and Canadian law are in tension with the rights of service providers and Internet users. This often gives 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,[80] and while they are indirect rather than direct state-mandated filtering, they constitute real censorship of online speech.[81]

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.

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.[82] 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 that originates in Canada.[83] The ''Anti-Spam Bill'' was finally tabled by the Canadian Government on April 24, 2009, as the Electronic Commerce Protection Act (Bill C-27) and is headed for committee review.[84] Government materials accompanying the release of Canada's ECPA point to plans to establish a Spam Reporting Centre similar to the U.S. FTC reporting mechanism.[85] 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 malicious software infecting

computers, though most of the efforts to filter information based upon content deemed to be computing security risks are carried out by private firms or individuals on a voluntary basis.[86] Calls are also being made to promote greater responsibility among ISPs for malicious software spread over their networks in order to contain the worst of ''zombie'' computers sending spam and distributing malware, 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.[87]

Network Neutrality

As a new Federal Communications Commission begins its work in the Obama Administration, network neutrality and the problem of bandwidth throttling are near the top of the list of issues it must tackle. One common mode of filtering Internet traffic is for ISPs to discriminate based upon the type or amount of data sent or requested through the network. Many people have had the experience of seeking to send an e-mail to a colleague with a large attachment, such as a photo or a video, only to have the e-mail bounce back with a note stating that an e-mail server along the way had rejected the message because of its size. Writ large, this same issue arises for ISPs and their users. Providers practice various forms of network management, where they decide to favor some data packets over others, often to combat network scourges like spam and malware. Some ISPs, for instance, allow users only a certain amount of bandwidth for certain activities. In August 2008, the FCC ruled that Comcast, a large ISP, had violated federal network neutrality rules when it practiced bandwidth throttling to prevent usage of the BitTorrent service.[88] The Comcast decision—a vote of 3–2 by the commission—marked the first such intervention by the FCC, but by no means resolved the issue of what kind of reasonable network management ISPs are permitted to practice. The new Obama administration FCC will likely be called upon to consider new legislation by Congress, new regulatory systems, and new allegations of infractions of the sort carried out by Comcast.

Surveillance

Concerns related to national security in the United States have contributed to the development of an extensive and technologically sophisticated online surveillance system. The U.S. surveillance system was expanded significantly under the Bush administration following the attacks of September 11, 2001. Government wiretaps are reported to have included taps on major Internet interconnect points and data mining of Internet communications.[89] Tapping these interconnect points would give the government the ability to intercept every overseas communication and many

domestic ones. 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 also pushed to expand the Communications Assistance to Law Enforcement Act (CALEA) to force providers to give law enforcement wiretap access to electronic communications networks. The attorney general under the Bush administration, Alberto Gonzales, called for data retention laws to force ISPs to keep and potentially produce data that could link Internet subscribers to their otherwise anonymous communications.[90] During Barack Obama's election campaign, he criticized both the Bush administration's use of warrantless surveillance and its reliance on the state secrets privilege, yet in January 2009 defended congressional legislation immunizing telecommunications companies from lawsuits regarding their participation in the Bush administration's surveillance programs.[91]

The U.S. government is required to produce annual reports on the number of wiretaps it conducts under Title III of the Omnibus Safe Streets and Crime Control Act of 1968 (the ''Wiretap Act''), as well as communication interceptions conducted under the Foreign Intelligence Surveillance Act (FISA) and the Pen Register and Trap and Trace statute (Pen/Trap statute).[92] No reports have been provided under the Pen/Trap statute since 1998.[93]

In Canada, Part VI of the Criminal Code governs the powers of law enforcement to engage in electronic surveillance of private communications when conducting criminal investigations. The Criminal Code requires the production of annual reports on the details of the interceptions that occur.[94] Canadian electronic surveillance for foreign intelligence is primarily undertaken by the National Defense's secretive Communications Security Establishment (CSE), which operates in close cooperation with its U.S. counterpart and other allied intelligence networks. A commissioner is appointed to review the actions of the CSE and produce annual reports commenting on the adherence of the agency to its legislative mandate in the National Defense Act.[95] The commissioner's annual reports, while providing some oversight, provide little additional transparency, as no statistics on the number of communications interceptions are reported.

Conclusion

While there is little technical filtering in either country, the Internet is subject to substantial state regulation in the United States and Canada. With respect to surveillance, the United States is believed to be among the most aggressive countries in the world in terms of listening to online conversations.

Legislators in both countries have imposed Internet-specific regulation that limits their citizens' access to Internet content. In addition, lawmakers have empowered private entities to press Internet intermediaries, including ISPs, for content removal or to carry out filtering. 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 carried out in some of the more repressive countries of the world have not taken hold in North America.

Notes

1. Derek E. Bambauer, "Cybersieves," *Duke Law Journal*, vol. 59 (2009), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1143582&rec=1&srcabs=1026597#.

2. 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*, vol. 21 (2006): 31–65.

3. International Telecommunication Union (ITU), "Internet Indicators: Subscribers, Users, and Broadband Subscribers," 2007, http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/InformationTechnologyPublic&RP_intYear=2007&RP_intLanguageID=1.

4. Ibid.

5. 47 U.S.C.A. §§223(a), §223(d) (Supp. 1997).

6. Solveig Bernstein, "Beyond the Communications Decency Act: Constitutional Lessons of the Internet," Cato Institute, Cato Policy Analysis No. 262, November 4, 1996, http://www.cato.org/pubs/pas/pa-262.html.

7. *ACLU v. Reno*, 929 F. Supp. (E.D. Pa. 1996) at 854–865.

8. *ACLU v. Reno*, 929 F. Supp. (E.D. Pa. 1996) at 883.

9. *Reno v. ACLU*, 521 U.S. 844 (1997).

10. Ibid.

11. 47 U.S.C. §230.

12. Citizen Media Law Project, "Section 230 of the Communications Decency Act," http://www.citmedialaw.org/section-230.

13. Adam Thierer and John Palfrey, "Dialogue: The Future of Online Obscenity and Social Networks," *ArsTechnica*, March 5, 2009, http://arstechnica.com/tech-policy/news/2009/03/a-friendly-exchange-about-the-future-of-online-liability.ars.

14. 47 U.S.C. §231.

15. *ACLU v. Reno*, No. 98–5551 (February 1, 1999).

16. Federal Communications Commission, ''Children's Internet Protection Act,'' http://www.fcc.gov/cgb/consumerfacts/cipa.html.

17. *United States v. American Library Association*, 539 U.S. 194 (2003).

18. Federal Communications Commission, ''E-Rate,'' http://www.fcc.gov/learnnet/.

19. Electronic Frontiers Australia, ''Internet Content Filtering and Blocking: Reviews of Internet Filtering Software,'' http://www.efa.org.au/Issues/Censor/cens2.html#reviews.

20. 20 U.S.C. §6777(c); 20 U.S.C. §9134(f)(3); 47 U.S.C. §254(h)(6)(D).

21. Marjorie Heins, Christina Cho, and Ariel Feldman, ''Internet Filters: A Public Policy Report,'' Brennan Center for Justice at NYU Law School (2006), 4–7, http://www.brennancenter.org/dynamic/subpages/download_file_36644.pdf.

22. Jim Hu, ''Court Strikes Down Pennsylvania Porn Law,'' *CNet News*, September 10, 2004, http://news.cnet.com/Court-strikes-down-Pennsylvania-porn-law/2100-1028_3-5361999.html.

23. *Harvard Law Review*, ''The First Amendment Overbreadth Doctrine,'' vol. 83, no. 4 (1970): 844–927, http://www.jstor.org/pss/1339842; *Broadrick v. Oklahoma* 413 U.S. 601 (1973); *CDT v. Pappert*, 337 (E.D. Penn. 2004) http://www.cdt.org/speech/pennwebblock/20040910memorandum.pdf.

24. *CDT v. Pappert*, 337 F.Supp.2d 606 (E.D. Penn. 2004). For an extensive analysis, see Jonathan Zittrain, ''Internet Points of Control,'' *Boston College Law Review*, 44 (2003): 653.

25. David Kravets, ''Communications Decency Act Tipping under Cuomo Kid-Porn Accord,'' *Wired Threat Level*, June 10, 2008, http://www.wired.com/threatlevel/2008/06/analysis-commun/.

26. Brad Stone, ''Online Age Verification for Children Brings Privacy Worries,'' *New York Times*, November 15, 2008, http://www.nytimes.com/2008/11/16/business/16ping.html?scp=1&sq=protecting%20children%20online&st=cse.

27. See *Megan Meier Cyberbullying Prevention Act*, http://www.govtrack.us/congress/bill.xpd?bill=h111-1966.

28. Euguene Volokh, ''Federal Felony to Use Blogs, the Web, Etc. to Cause Substantial Emotional Distress through 'Severe, Repeated, and Hostile' Speech?'' April 30, 2009, http://volokh.com/posts/1241122059.shtml.

29. See the First Amendment Center's overview of state cyberbullying laws, at http://www.firstamendmentcenter.org/PDF/cyberbullying_policies.pdf.

30. This approach was first recommended in a 1997 study commissioned by Industry Canada.

31. Passed as Bill C-15a, 1st Session, 37th Parl., 2001; R.S. 1985, c. C-46, §§163.1(3), 163.1(4.1), 172.1.

32. Project Cleanfeed Canada, ''Frequently Asked Questions,'' http://www.cybertip.ca/en/cybertip/cf_faq; R.S., 1985, c. C-46, section IV, http://www.canlii.org/en/ca/laws/stat/rsc-1985-c-c-46/latest/rsc-1985-c-c-46.html.

33. 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....

34. Michael Geist, ''Telus Breaks ISPs' Cardinal Rule,'' *Toronto Star*, August 1, 2005, http://www.michaelgeist.ca/index.php?option=content&task=view&id=919.

35. Ibid.

36. Telecommunications Act, R.S.C., ch. 38, §§27(2), 36, http://www.crtc.gc.ca/eng/LEGAL/TELECOM.HTM.

37. OpenNet Initiative, ''Telus Blocks Consumer Access to Labour Union Web Site and Filters an Additional 766 Unrelated Sites,'' August 2, 2005, http://opennet.net/bulletins/010.

38. See ''TELUS Removes Blocking from VFC Website,'' July, 28, 2005, http://www.voices-for-change.ca/news/archive.asp?PagePosition=2 (accessed November 10, 2006).

39. Canadian Radio-Television and Telecommunications Commission, ''Papazian Heisey Myers for Richard Warman—Application for Interim Approval to Permit Canadian Carriers to Block the Content of Certain Hate Websites and Additional Follow-up Relief, '' August 22, 2006, http://www.crtc.gc.ca/PartVII/eng/2006/8646/p49_200610510.htm.

40. Ibid.

41. Michael Geist, ''Ontario Court Orders Website to Disclose Identity of Anonymous Posters,'' March 24, 2009, http://www.michaelgeist.ca/content/view/3777/125/.

42. SteynOnline, ''Anonymous Commenter Sues Anonymous Commenters,'' April 1, 2009, http://www.steynonline.com/content/view/1939/128/.

43. Project Cleanfeed Canada, ''ISPs and Tipline Set Up Battle against Internet Child Exploitation,'' November 24, 2006, http://www.cybertip.ca/en/cybertip/cleanfeed_canada (accessed November 10, 2006).

44. Project Cleanfeed Canada, ''Frequently Asked Questions,'' http://www.cybertip.ca/app/en/media_faq.

45. *Slashdot*, ''Cleanfeed Canada: What Would It Accomplish?'' December 15, 2006, http://yro.slashdot.org/article.pl?sid=06/12/15/1624215.

46. Criminal Code of Canada (R.S., 1985, c. C-46) §163.

47. Project Cleanfeed Canada, ''Appeal Process,'' http://www.cybertip.ca/app/en/cleanfeed_p1#anchor_menu.

48. SAFE Port Act, http://www.gpo.gov/fdsys/pkg/PLAW-109publ347/content-detail.html.

49. Bob Dart, ''Poker Players Push for a New Deal on Internet,'' *Denver Post*, October 25, 2007, http://www.denverpost.com/headlines/ci_7271902.

50. Brian Krebs, ''Kentucky Tests State's Reach against Online Gambling,'' *Washington Post*, October 8, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/10/08/AR2008100802870.html.

51. Grant Gross, ''Groups Ask Kentucky Court to Reverse Domain Seizures,'' *PC World*, November 14, 2008, http://www.pcworld.com/businesscenter/article/153930/groups_ask_kentucky_court_to_reverse_domain_seizures.html.

52. Jaikumar Vijayan, ''Domain Names Can't Be Appropriated, Court Says,'' *PC World*, January 22, 2009, http://www.pcworld.com/businesscenter/article/158169/domain_names_cant_be_appropriated_court_says.html.

53. Wendy Davis, ''Minnesota Faces Tough Odds in Limiting Online Gambling,'' *MediaPost*, May 4, 2009, http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=105194.

54. Pokerstrategy.com, ''IMEGA Files Lawsuit against Minnesota,'' May 9, 2009, http://www.pokerstrategy.com/news/world-of-poker/IMEGA-Files-Lawsuit-Against-Minnesota_19471.

55. iMEGA, ''Minnesota Drops 'Black List' Blocking Order in Settlement with iMEGA,'' June 8, 2009, http://www.imega.org/2009/06/09/minnesota-drops-black-list-blocking-order-in-settlement-with-imega/.

56. Eric Pfanner, ''A New Chance for Online Gambling in the U.S.,'' *New York Times*, April 26, 2009, http://www.nytimes.com/2009/04/27/technology/internet/27iht-gamble.html?_r=1&ref=globalhome.

57. Tom Somach, ''Gambling . . . Gold Rush?'' *San Francisco Chronicle*, June 2, 2007, http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2007/07/02/BUG5LQO5P11.DTL.

58. Javad Heydary, ''Advertising for Online Gambling—Is It Legal?'' *E-Commerce Times*, April 28, 2005, http://www.heydary.com/publications/online-gambling-laws.html.

59. Tim Naumetz, ''Senate Saves the Day for Online Gambling,'' *Law Times*, December 10, 2007, http://www.lawtimesnews.com/200712103704/Headline-News/Senate-saves-the-day-for-online-gambling.

60. 47 U.S.C. §230(c)(1).

61. *New York Times Co. v. Sullivan*, 376 U.S. 254 (1964).

62. *Society of Composers, Authors and Music Publishers of Canada v. Canadian Assn. of Internet Providers*, [2004] 2 S.C.R. 427 [hereinafter *CAIP v. SOCAN*]: http://scc.lexum.umontreal.ca/en/2004/2004scc45/2004scc45.html.

63. Javad Heydary, ''Guidelines Evolving on ISP Liability for Users' Misdeeds,'' *Tech News World*, August 12, 2004, http://www.technewsworld.com/story/35750.html.

64. Ibid.

65. 47 U.S.C. §230 .

66. 47 U.S.C. §230(e)(2).

67. Public Law No. 105–304, 112 Stat. 2860 (1998).

68. 17 U.S.C. §§512(a)–(d).

69. 17 U.S.C. §512(c) (2007).

70. 17 U.S.C. §512(g).

71. 17 U.S.C. §512(h).

72. See Chilling Effects, ''DMCA Safe Harbor,'' http://www.chillingeffects.org/dmca512/.

73. Department of Canadian Heritage: Copyright Policy Branch, http://www.pch.gc.ca/pc-ch/org/sectr/ac-ca/pda-cpb/index-eng.cfm.

74. Michael Geist, ''The Canadian DMCA: Check the Fine Print,'' June 12, 2008, http://www.michaelgeist.ca/content/view/3025/125; Bill C-61, http://www2.parl.gc.ca/HousePublications/Publication.aspx?Docid=3570473&file=4.

75. Michael Geist, ''Entertainment Software Association Lobbies for Reintroduction of C-61,'' http://www.michaelgeist.ca/content/view/3883/196/.

76. Michael Geist, ''Why Notice-and-Notice Should Be Part of the Canadian DMCA,'' June 6, 2008, http://www.michaelgeist.ca/content/view/3009/125/; see Bill C-61, s.41.26, http://www2.parl.gc.ca/HousePublications/Publication.aspx?Docid=3570473&file=4.

77. Online Rights Canada, ''What Are Copyright Reform and Bill C-60?'' December 7, 2005, http://www.onlinerights.ca/learn/what_is_c-60/.

78. Michael Geist, ''The Effectiveness of Notice and Notice,'' February 15, 2007, http://www.michaelgeist.ca/content/view/1705/125/.

79. *CBC News*, ''E-Mail Warnings Deter Canadians from Illegal File Sharing,'' February 15, 2007, http://www.cbc.ca/consumer/story/2007/02/14/software-warnings.html.

80. See the work of Chilling Effects Clearinghouse, www.chillingeffects.org.

81. The Electronic Frontier Foundation, ''Unsafe Harbors: Abusive DMCA Subpoenas and Take-down Demands,'' September 2003, http://www.eff.org/IP/P2P/20030926_unsafe_harbors.php#_edn3.

82. Industry Canada, ''Stopping Spam: Creating a Stronger, Safer Internet,'' May 2005, http://www.ic.gc.ca/epic/site/ecic-ceac.nsf/en/h_gv00317e.html.

83. Michael Geist, ''Spam Plans,'' March 15, 2007, http://www.michaelgeist.ca/content/view/1805/125/.

84. Michael Geist, ''Canada Introduces Electronic Commerce Protection Act,'' April 24, 2009, http://www.michaelgeist.ca/content/view/3891/125/; Bill C-27 itself: http://www2.parl.gc

.ca/HousePublications/Publication.aspx?DocId=3832885&Language=e&Mode=1; Michael Geist, ''Electronic Commerce Protection Act Headed to Committee Following Odd Debate,'' May 12, 2009, http://www.michaelgeist.ca/content/view/3956/125/.

85. Michael Geist, ''The Electronic Commerce Protection Act—The Enforcement Prohibitions,'' April 28, 2009, http://www.michaelgeist.ca/content/view/3902/125/.

86. Consider, for instance, the interstitial pages that search giant Google places between search results and certain pages on the Internet deemed to host malware that might harm an end user's computer. See StopBadware.org, http://stopbadware.org.

87. Jonathan Zittrain, *The Future of the Internet and How to Stop It* (New Haven, CT: Yale University Press, 2008), 153–199.

88. Declan McCullagh, ''FCC Formally Rules Comcast's Throttling of BitTorrent Was Illegal,'' *CNet News*, August 1, 2008, at http://news.cnet.com/8301-13578_3-10004508-38.html.

89. James Risen and Eric Lichtblau, ''Spy Agency Mined Vast Data Trove, Officials Report,'' *New York Times*, December 24, 2005, http://www.nytimes.com/2005/12/24/politics/24spy.html.

90. Declan McCullagh, ''Gonzales Pressures ISPs on Data Retention,'' *CNet News*, May 27, 2006, http://news.zdnet.com/2100-1009_22-148226.html.

91. David Kravets, ''Obama Sides with Bush in Spy Case,'' *Wired.com*, January 22, 2009, http://www.wired.com/threatlevel/2009/01/obama-sides-wit/.

92. Respectively: 18 U.S.C. §§ 2510–22; 50 U.S.C. §§1801–11; 18 U.S.C. §§3121–7.

93. Electronic Privacy Information Center, ''FBI Reporting Concerning Pen Register/Trap and Trace Statistics,'' April 29, 2009, http://epic.org/privacy/wiretap/ltr_pen_trap_leahy_final.pdf.

94. Criminal Code (R.S., 1985, c. C-46), s.195, http://laws.justice.gc.ca/en/C-46/; Public Safety Canada, *Annual Report on the use of Electronic Surveillance 2007*, 2008, http://www.publicsafety.gc.ca/abt/dpr/le/elecsur-07-eng.aspx.

95. Office of the Communications Security Establishment Commissioner, ''Annual Reports,'' http://ocsec-bccst.gc.ca/ann-rpt/index_e.php; *National Defense Act* (R.S., 1985, c. N-5) Part V.1, s.273.63, http://laws.justice.gc.ca/en/N-5/section-273.63.html.