Freedom House

Canada

	2013	2014
Internet Freedom Status	**N/A**	**Free**
Obstacles to Access (0-25)	n/a	3
Limits on Content (0-35)	n/a	3
Violations of User Rights (0-40)	n/a	9
TOTAL* (0-100)	**N/A**	**15**

* 0=most free, 100=least free

Population:	35.3 million
Internet Penetration 2013:	86 percent
Social Media/ICT Apps Blocked:	No
Political/Social Content Blocked:	No
Bloggers/ICT Users Arrested:	No
Press Freedom 2014 Status:	Free

Key Developments: May 2013 – May 2014

- In October 2013, parliament introduced Bill C-13, which was intended to remedy concerns over cyberbullying but which also contains troubling provisions regarding warrantless disclosure of user data (see **Violations of User Rights**).
- Bill S-4, also known as the Digital Privacy Act, was introduced by parliament in April 2014 and includes requirements for organizations to disclose security breaches that put Canadians at risk. However, this bill could also reduce court oversight in cases related to copyright infringement (see **Violations of User Rights**).
- A Federal Court of Appeals ruling on January 31, 2014 found that section 13 of the Canadian Human Rights Act (CHRA), the legislation that provides for hate speech penalties, does not violate the constitutional right to freedom of expression. However, prior to this decision, parliament voted to repeal section 13 in June 2013; the repeal officially took effect in June 2014. Currently, hate speech can still be regulated under section 320.1 of the criminal code (see **Violations of User Rights**).

Introduction

Internet access in Canada is reliable and affordable for a majority of the population and is generally free of government restrictions. Canadians enjoy strong protections for freedom of expression, in addition to a well-developed set of rules regulating intermediary liability in cases of copyright infringement. Canada's communications regulator has avoided regulating "new media" entities, which encompasses a broad range of internet-based companies offering video and other content services. Further, Canada's privacy commissioner has aggressively focused on internet-related concerns, particularly those involving search functions and social media.

Despite these strengths, there remains considerable unease among many Canadians with respect to online rights. Proposed legislative reforms, including the Digital Privacy Act (Bill S-4) and the Protecting Canadians from Online Crime Act (Bill C-13, also known as the "cyberbullying" bill), have generated concern among many Canadians with regard to potentially negative provisions included within the bills, such as plans to expand the scope of voluntary disclosures of personal information without court oversight. Additionally, Canada's role in global surveillance activities was revealed over the past year through the NSA documents leaked by Edward Snowden, causing many to question the sufficiency of surveillance oversight in Canada.

The vertically integrated telecommunications market, in which a handful of companies dominate broadcast, telecom, wireless, and internet access, has also raised considerable fears about the state of competition within Canada and the potential for those companies to use their privileged position to violate net neutrality, increase access costs, or engage in uncompetitive behavior. The Canadian Radio-television and Telecommunications Commission has developed vertical-integration policies, but their effectiveness is open to question.

Obstacles to Access

According to the International Telecommunication Union (ITU), Canada had an internet penetration rate of nearly 86 percent in 2013, compared to 83 percent in 2012 and 77 percent in 2008.[1] Similarly, Statistics Canada reported in 2013 that 83 percent of Canadians use the internet.[2] DSL broadband internet access service is available in all provinces and territories. By the end of 2010, 85 percent of households were located within the DSL broadband footprint, and 15 percent of households were served by either fiber-to-the-node or fiber-to-the-home connections.[3]

Broadband internet access through cable modems is available in all provinces and territories except the northernmost territory of Nunavut, and by the end of 2013, approximately 33 percent of the

1 International Telecommunication Union (ITU), "Percentage of individuals using the Internet," 2013, 2012, 2008, accessed August 1, 2014, http://www.itu.int/en/ITU-D/Statistics/Pages/default.aspx.

2 Statistics Canada, Table 358-0152: Canadian Internet use survey, Internet use, by age group and household income for Canada, *provinces and census metropolitan areas (CMAs), Occasional (percent)*, CANSIM, accessed September 17, 2014, http://www5.statcan.gc.ca/cansim/a26?lang=eng&retrLang=eng&id=3580152&pattern=358-0152..358-0158&tabMode=dataTable&srchLan=-1&p1=-1&p2=31 (hereafter cited as *Table 358-0152*).

3 Canada, Canadian Radio-television and Telecommunications Commission. *Broadband Report November 2011*. [Ottawa], 2012. http://www.crtc.gc.ca/eng/publications/reports/broadband/bbreport1111.htm.

population had fixed broadband subscriptions.[4] Although satellite broadband internet access service is available throughout Canada, it is generally used to provide broadband internet service in the more rural and remote areas of the country. Wireless internet access is the fastest growing sector for internet service in Canada: over 48 percent of Canadians used wireless internet services in 2012, compared to about 26 percent in 2010.[5]

According to the ITU, Canada had a mobile phone penetration rate of over 78 percent in 2013.[6] Mobile carriers have deployed a number of newer technologies to provide mobile broadband service, including HSPA+ and LTE.

While internet access is widely available in Canada, there is a gap in access related to income: the highest income bracket has a penetration rate of nearly 95 percent, while the penetration rate within the lowest income bracket has an internet penetration rate closer to 63 percent.[7] Use of public access points such as libraries is declining but is still an important resource, particularly for younger Canadians or those with lower household incomes.

There is a wide range of content available in both of Canada's official languages (English and French) as well as many other languages. All major media organizations feature extensive websites with articles, audio, and video. The public broadcaster maintains a very comprehensive website that includes news articles and streamed video programming. Paywalls have become increasingly popular among newspaper organizations, but there remains considerable choice (including alternate, independent media) that is freely available.

There are no government restrictions on bandwidth, although access providers frequently offer services with caps on bandwidth that result in increased fees. The government has not centralized the telecommunications infrastructure in Canada. However, given the vertical integration of the Canadian marketplace, the telecom infrastructure is controlled by a small number of companies, which could facilitate greater control of content and the use of surveillance technologies.

To operate as a Canadian telecommunications carrier, a company must meet the requirements in section 16 of the Telecommunications Act. In 2012, Canadian telecommunications revenues amounted to $43.9 billion. Ten companies and their affiliates accounted for 93 percent of this total revenue, with the remaining smaller companies earning combined revenues of less than $2.9 billion. Each company's revenue falls within the 10 percent maximum of total Canadian telecommunications revenues, as required by subsection 16(6) of the Telecommunications Act.[8]

Canadians have a choice of wireless internet providers, virtually of which are privately owned (the notable exception being SaskTel, a government-owned provider in the Province of Saskatchewan).

4 International Telecommunication Union (ITU), "Fixed (-wired) broadband subscriptions," 2013, accessed August 1, 2014, http://www.itu.int/en/ITU-D/Statistics/Pages/default.aspx.

5 Statistics Canada, Table 358-0219: *Canadian Internet use survey, Internet use, by location and frequency of use, Occasional (percent),* CANSIM, accessed September 17, 2014, http://www5.statcan.gc.ca/cansim/a26?lang=eng&retrLang=eng&id=3580219&paSer=&pattern=&stByVal=1&p1=1&p2=31&tabMode=dataTable&csid.

6 International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions per 100 inhabitants," 2013, accessed August 1, 2014, http://www.itu.int/en/ITU-D/Statistics/Pages/default.aspx.

7 Statistics Canada, Table 358-0152: *Canadian Internet use by age group and household income for Canada, provinces, and metropolitan areas,* CANSIM, accessed September 17, 2014, http://www5.statcan.gc.ca/cansim/a05?lang=eng&id=3580152.

8 Statistics Canada, Table 358-0152.

There are at least three providers in all markets. Restrictions on foreign investment establish some controls, though Canada has seen some foreign companies enter the marketplace in recent years. The provision of access services is subject to regulation with rules on tower sharing, domestic roaming agreements, and a consumer regulator to address consumer concerns.

For wireless services, the market is dominated by three companies: Bell, Telus, and Rogers. Those same companies are leaders in the provision of internet services, along with Shaw, Cogeco, and Videotron. The government's Minister of Industry, James Moore, has emphasized the need for more competition in this market.

The Canadian Radio-television and Telecommunications Commission (CRTC), the regulatory body that oversees the communications industry, operates largely independently from the government. In 1976, the federal government created the CRTC by consolidating multiple federal regulatory bodies that had jurisdiction over electronic communication media. The CRTC's authority is derived from two federal acts: the Broadcasting Act and the Telecommunications Act. Section 7 of the Telecommunications Act outlines the broad policy objectives pursued by the Act and, by extension, the CRTC, in the field of telecommunications. Section 7 enumerates nine specific objectives that feature two key themes: consumer telecom services and a strong domestic telecom industry. Regulation is intended to be limited and focused on instances where the market is patently unable to achieve the intentions and goals of the Act.

The chair and commissioners of the CRTC are appointed by the government, and there is no public consultation on the appointment. The government also has, in some cases, provided guidance on their policy expectations regarding telecommunication regulations. Moreover, CRTC decisions can be appealed to the courts, or a government review can be requested. The government has (on rare occasions) overturned CRTC decisions and directed it to reconsider the issue. For example, the government required the CRTC to reconsider its approach to usage-based billing for internet services in 2011.[9]

Limits on Content

The Canadian government does not generally block websites or filter online content. Illegal content may be removed by private legal action taken through the court system.[10] YouTube, Facebook, Twitter, and international blog-hosting services are freely available.

There are few legal mechanisms that may lead to the blocking or removal of online content in Canada. Canada's largest ISPs participate in Project Cleanfeed Canada, an initiative that allows ISPs to block access to child pornography images that are hosted outside of Canada (as opposed to content hosted within Canada, which is subject to removal).[11] Accessing child pornography is illegal in Cana-

9 Steven Chase, "CRTC will rescind 'unlimited use' Internet decision - or Ottawa will overturn it," *The Globe and Mail*, February 2, 2011, http://www.theglobeandmail.com/technology/tech-news/crtc-will-rescind-unlimited-use-internet-decision---or-ottawa-will-overturn-it/article565223/#dashboard/follows/.

10 "Regional Overviews United States and Canada," OpenNet Initiative, accessed September 19, 2014, https://opennet.net/sites/opennet.net/files/ONI_UnitedStatesandCanada_2010.pdf (hereafter cited as OpenNet initiative).

11 "Canadian Center for Child Protection Inc.," Cleanfeed Canada, accessed September 19, 2014, 370, https://www.cybertip.ca/app/en/projects-cleanfeed#projects-cleanfeed.

da under section 163.1(4.1) of the criminal code.[12] The initiative is targeted at international sites that the Canadian government does not have the jurisdiction to shut down.

Under Project Cleanfeed Canada, an individual may issue complaints about content to the ISP or directly to Cybertip.ca, which will assess the site and, if necessary, obtain an independent, binding judgment from the National Child Exploitation Coordination Centre.[13] An appeals process has also been put into place for cases in which content providers believe that their content has been wrongly blocked (though the list of blocked sites is not public since it would essentially provide a directory of child pornography).[14] The project blocks approximately 1,000 child pornography images each year.

With respect to removal of content due to copyright infringement, in 2004 the Supreme Court of Canada ruled that ISPs are not liable for violations committed by their subscribers.[15] Canadian copyright law features a notice-and-notice provision, which, unlike a notice-and-takedown system, does not make intermediaries legally liable for removing content upon notification by the copyright owner. Rather, copyright owners are permitted to send notifications alleging infringement to ISPs. The providers are then required to forward the notifications to the implicated subscriber. Any further legal action is the responsibility of the copyright owner. No content is removed from the internet without a court order, and the internet provider does not disclose subscriber information without court approval. ISPs qualify for a legal safe harbor if they comply with the notice-and-notice requirements.

Defamation claims may also result in the removal of content, as providers fear potential liability as a publisher of the defamatory content. Unlike legal protections against liability for copyright infringement by its users, providers may face liability for alleged defamation once alerted to the publication. A court may also order the removal of the content.

With the exception of the topics discussed above (child pornography, hate speech, copyright) there does not appear to be widespread self-censorship in Canadian online publications. There is no evidence of government manipulation of online content. Some sites are affiliated with a particular partisan interest, but there are representative sites from all sides of the political spectrum available online.

To date, economic constraints such as net neutrality concerns have not been a significant factor in the success or failure of online media outlets and platforms in Canada, though the debate over net neutrality continues. The Canadian Radio-Television and Telecommunications Commission (CRTC) oversees the regulation and provision of internet services, and section 36 of the Telecommunications Act states that "a Canadian carrier shall not control the content or influence the meaning or purpose of telecommunications carried by it for the public," unless otherwise approved by the CRTC. Complaints can be filed with the CRTC for alleged violations. The provision is relevant in the net neutrality context since the CRTC has ruled that section 36 could be raised to counter an ISP controlling the content that it carries. The provision forms part of the net neutrality safeguards in Canada, which are called Internet Traffic Management Practices, or ITMPs. The CRTC has used the ITMPs to stop ISPs

12 *Criminal Code,* RSC 1985 c C-46 s 163.1(4.1).

13 OpenNet Initiative.

14 Michael Geist, "Project Cleanfeed Canada," Michael Geist (blog), November 24, 2006, accessed September 19, 2014, http://www.michaelgeist.ca/content/view/1548/125/.

15 *Society of Composers, Authors and Music Publishers of Canada v Canadian Assn of Internet Providers,* 2004 SCC, 2 SCR 427.

from throttling internet traffic, and the policies are currently being considered in the context of mobile video services.

Social media and communication applications have been widely used in Canada for the mobilization of political and social movements. For example, a social media campaign in 2012 successfully stalled a government proposal that would have allowed for increased monitoring and tracking of Canadians' activities online. On February 13, 2012, then-Public Safety Minister Vic Toews infamously told the House of Commons that critics of his forthcoming lawful access bill could either stand with the government or "with the child pornographers."[16] Bill C-30 was introduced the following day, but within two weeks, a massive public outcry—much of it online—forced the government to quietly suspend the bill. A year later, the government openly acknowledged that the bill had been dropped.

The Twitter-based #tellviceverything campaign, invoking the idea that the government already has too much access to one's private communications data, provided a perfect illustration of how the internet can fuel awareness and action at remarkable speed.[17] Through thousands of tweets, Canadians used humor to send a strong message against Bill C-30. Alongside the Twitter activity were dedicated websites, hundreds of blog postings from commentators on the left and right of the political spectrum, thousands of calls and letters to MPs, and nearly 100,000 signatures on the Stop Spying petition hosted by the organization Open Media.

There are undoubtedly many factors that led to the successful fight against the bill. Toews' comments placed the government on the defensive from the outset, and the substance of the bill generated criticism from both sides of the political spectrum. Yet the bigger story was the emergence of the public voice on digital policy. Justice Minister Rob Nicholson's comments in announcing the defeat of Bill C-30 highlighted the impact of the public outcry:

> "We will not be proceeding with Bill C-30 and any attempts that we will continue to have to modernize the Criminal Code will not contain the measures contained in C-30, including the warrantless mandatory disclosure of basic subscriber information or the requirement for telecommunications service providers to build intercept capability within their systems. We've listened to the concerns of Canadians who have been very clear on this and responding to that."[18]

The emphasis on responding to public concern highlights the public campaign's effectiveness and the recognition of the need to incorporate broader perspectives into legislative and policy developments.

16 Postmedia News, "Vic Toews accuses online surveillance bill C-30 opponents of siding with 'child pornographers'," February 14, 2012, http://news.nationalpost.com/2012/02/14/online-surveillance-bill-critics-are-siding-with-child-pornographers-vic-toews/.

17 Laura Payton, "'Tell Vic Everything' tweets protest online surveillance" CBC News, February 16, 2012, http://www.cbc.ca/news/politics/tell-vic-everything-tweets-protest-online-surveillance-1.1187721

18 Laura Payton, "Government killing online surveillance bill," CBC News, February 11, 2013, http://www.cbc.ca/m/touch/news/story/1.1336384.

Violations of User Rights

Despite having a generally positive record for freedom of expression, Canada has, in recent years, taken some regressive steps, driven by court decisions that weakened confidentiality for journalists' sources, and the introduction of several bills that could have negative implications for the protection of internet users' data. Activists have also criticized Conservative Prime Minister Steven Harper's government for tightening access to information and its slow response time to requests. The country's 30-year-old Access to Information Act (ATIA) is also highlighted as an obstacle given the long delays and regular use of exceptions to redact large amounts of information from released documents.

The Canadian Constitution includes strong protections for freedom of speech and freedom of the press. Freedom of speech in Canada is protected as a "fundamental freedom" by section 2 of the Canadian Charter of Rights and Freedoms. Section 1 of the Charter allows the government to pass laws that limit free expression so long as the limits are reasonable and can be justified. These laws and protections apply to all forms of speech, whether online or offline.

Two 2010 court cases—Globe and Mail v. Canada[19] and R. v. National Post[20]—have dealt with journalistic privilege directly. While Canada's Supreme Court Justices have stopped short of offering blanket confidentiality, they have stressed that compelling journalists to reveal sources should be extraordinary and not the rule, recognizing that investigative reporting plays an important role in society. Instead, tests should be applied on a case by case basis. In addition, the court ruled that journalists have the right to publish confidential material from a source, even when the source has no right to divulge the information or has obtained it by illegal means.

Copyright legislation in Canada includes specific protections for non-commercial, user-generated content (UGC). The drafting of this legislation was particularly focused on online mashups and other forms of remix expression. The non-commercial UGC provision, which took effect in 2012, legalizes both the creation and distribution of user-generated content provided that the work meets four criteria, including that it is non-commercial, there is attribution where reasonable, the original work was not infringing copyright, and the new work does not have a substantial adverse effect on the original.

Hate speech is also regulated under the Canadian criminal code. According to section 320.1, a judge may order that publicly available hate propaganda be made unavailable.[21] In the past, the Canadian Human Rights Commission could investigate and settle complaints regarding online hate speech through section 13 of the Canadian Human Rights Act (CHRA), which prohibits the repeated communication of hate speech over the phone or internet. On June 26, 2013, the parliament passed legislation (Bill C-304) that repealed section 13 of the CHRA, slated to take effect in June 2014. However,

19 Globe and Mail v. Canada (Attorney General), [2010] 2 SCR 592, 2010 SCC 41 (CanLII), accessed September 19, 2014, http://www.canlii.org/en/ca/scc/doc/2010/2010scc41/2010scc41.html.

20 Supreme Court judgement, *R. v. National Post,* May 7, 2010, http://scc-csc.lexum.com/scc-csc/scc-csc/en/item/7856/index.do.

21 *Criminal Code,* RSC 1985 c C-46 s 320.1; OpenNet Initiative.

in January 2014, a Federal Court of Appeals ruling found section 13 to be constitutionally valid and not a violation of the right to freedom of expression.[22]

There are no specific online restrictions on sensitive topics. Anti-spam legislation, enacted in July 2014, requires opt-in consent to send commercial electronic messages. Critics of the legislation have argued that it is overly broad and seeks to overregulate commercial speech. The constitutionality of the law has not yet been tested.

Defamatory libel is punishable under the criminal code with imprisonment for a term not exceeding five years (s. 301 of the criminal code). Human rights complaints regarding any potentially defamatory statements could also be decided through the mechanisms provided by the Human Rights Code (Ontario) and the Canadian Human Rights Act, in situations where a potentially defamatory statement could also be construed as a violation of the provisions that protect a number of enumerated groups.

Judicial rulings related to freedom of expression and defamation online have varied. In 2011, an Ontario Supreme Court decision in the case of Baglow v. Smith established that the threshold for prosecuting defamatory content from political blogs should be higher than in traditional forms of media, since the blogosphere is "a place where readers expect to encounter disrespectful comments and visceral rejoinders."[23] This case was originally decided by a summary judgment, or expedited ruling, in September 2011, as the judge deemed it to be a relatively straightforward case; however, the summary judgment was overturned by appeal in June 2012, and the full trial began on March 24, 2014. As of May 2014, the trial was still ongoing.

Libel tourism, or the practice of taking up a libel case in a jurisdiction considered to be more favorable to the plaintiff, is not a significant problem in Canada, although recent court rulings have called into question whether there are adequate legal protections against such actions. In the case of Breeden v. Black in 2012, the Supreme Court issued a ruling confirming that defamation takes place where the content is published; however, as this pertains to the internet, the place where the content is published could mean anywhere the content can be accessed, not just the jurisdiction in which it was uploaded. The court recognized that this interpretation could lead to libel tourism, and indicated a willingness to consider applying the law according to where the most harm was done to the plaintiff's reputation, which in most cases would be the jurisdiction of their home country.

Citizens can be subject to legal sanction depending on the material that is being accessed. They can be found guilty of possessing, accessing or even distributing child pornography if they post images of it on the internet.[24] This also extends to text messages, such as in a January 2014 case of a teenager who had sent texts containing explicit images of another teenager and was convicted

22 Joseph Brean, "Court finds Internet hate speech law Section 13 to be constitutionally valid, doesn't violate freedom of expression," *National Post*, February 2, 2014, http://news.nationalpost.com/2014/02/02/court-finds-internet-hate-speech-law-section-13-to-be-constitutionally-valid-doesnt-violate-freedom-of-expression/.

23 Mark A.B. Donald, "Baglow v. Smith and online defamation in the blogosphere," Canadian Journalists for Free Expression, April 9, 2013, https://cjfe.org/resources/features/baglow-v-smith.

24 Kevin Bissett, "Douglas Hugh Stewart, New Brunswick Man, Gets 5 Years In Prison For Millions Of Child Porn Images," *Huffington Post*, November 14, 2011, accessed September 19, 2014, http://www.huffingtonpost.ca/2011/11/14/douglas-hugh-stewart-child-porn-sentence_n_1092964.html.

of possession of child porn.[25] Generally, writers, commentators, or bloggers are not subject to legal sanction because of what they post on the internet.

Website owners, bloggers, and internet users in general are not required to register with the government. However, identification is required in order to purchase a mobile phone through a telecommunications company. Pay-as-you-go phones can be purchased without ID, since no contract is required.

In a decision related to privacy protections for user's identifying information, the Divisional Court in 2010 overturned an order in the case Warman v. Fournier requiring the named defendants, who run an internet message board, to produce documents identifying several users who posted allegedly defamatory comments on the message board. The Divisional Court found that the case engaged both freedom of expression and privacy interests under the Charter, and that these interests should be balanced against the public interest. It held that courts should adopt a process that provides for a balancing of the interests at stake before identity information is disclosed by a party, noting that otherwise, a plaintiff with no legitimate claim could, for example, misuse the court rules by bringing a frivolous action against an ISP for the sole purpose of identifying an anonymous internet commentator.[26]

In the past year, the Canadian parliament proposed two pieces of legislation—Bill C-13 and Bill S-4—with implications for privacy and freedom of expression. Bill C-13, known as the Cyberbullying Bill, would make it illegal to circulate explicit images online without the subject's consent, but would also grant legal immunity to telecommunication service providers who voluntarily hand over user's information to the authorities.[27] Bill S-4, the Digital Privacy Act, contained certain provisions that could enhance users' privacy online, including making it mandatory to notify consumers when a company experiences a data protection breach. However, the bill could remove the court order requirements in cases of copyright infringement lawsuits, effectively moving to a notice-and-takedown system. Both pieces of legislation contain positive attempts to protect individual's privacy online; however, negative or vaguely worded provisions in the legislation require further consideration regarding their implications for individual's rights online. By May 2014, the end of this report's coverage period, both bills were still pending in parliament.

Users are allowed to use encryption software to protect their communications. Canadians are free to develop, import, and use whatever cryptography products they wish.[28] There are no laws in Canada that restrict the use of encryption or other security tools,[29] although Ottawa offices have told telecommunication companies that one of the conditions of obtaining a license to use wireless spectrum is to provide the government with the capability to bug the devices that use the spectrum. In

25 Dirk Messier, "Sexting B.C. teen found guilty of child pornography," CTV News Vancouver, January 10, 2014, http://bc.ctvnews.ca/sexting-b-c-teen-found-guilty-of-child-pornography-1.1633678 .

26 *Warman v Fournier*, 2010 ONSC 2126, 100 OR (3d) 648.

27 Evan Dyer, "Cyberbullying bill draws fire from diverse mix of critics," CBC News, October 2, 2014, http://www.cbc.ca/news/politics/cyberbullying-bill-draws-fire-from-diverse-mix-of-critics-1.2803637.

28 Industry Canada. Digital Policy Branch. *Summary of Canada's Policy on Cryptography*: [Ottawa], 2013. http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/gv00118.html.

29 Industry Canada. Digital Policy Branch. *Cryptography*, [Ottawa], 2013. http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/h_gv00085.html.

addition, as part of the requirements Ottawa has demanded companies to scramble encryption so that it can be accessed by Canada's law enforcement agencies.[30]

The June 2013 revelations about the online surveillance practices of the U.S. National Security Agency (NSA) had a significant impact on discussions surrounding the practices and policies of the Canadian government as well, particularly as Canada is a member of the Five Eyes alliance (along with the United States, the United Kingdom, Australia, and New Zealand). It is difficult to know precisely what occurs with respect to online monitoring. The Communications Security Establishment of Canada (CSEC) maintains that it does not monitor Canadians; however, leaked documents revealing that U.S. and British intelligence agencies may have been able access to their citizens' data through the Five Eyes alliance calls this statement into question.

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, though the information is aggregated and provides only limited insight into actual interception practices.

Canadian electronic surveillance for foreign intelligence is primarily undertaken by the National Defense's secretive Communications Security Establishment (CSEC), 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 CSEC and produce annual reports commenting on the adherence of the agency to its legislative mandate in the National Defense Act of 1985. The commissioner's annual reports, while providing some oversight, offer little additional transparency, as no statistics on the number of communications interceptions are reported.

Canada's private sector privacy law (PIPEDA) requires consent for the collection, use, and disclosure of personal information along with appropriate disclosure of privacy practices. The law features a complaints mechanism that allows for individuals to direct complaints to the Privacy Commissioner of Canada, who is independent of the government. While this process provides some measure of oversight with respect to the collection, use, and disclosure of personal information by the private sector, the activities of law enforcement are less well known. The Supreme Court of Canada has ruled on the need for a court order or warrant for the disclosure of personal information by ISPs.

While oversight and review mechanisms exist regarding government surveillance, there are concerns about the sufficiency of the system. For example, past statements by the head of the CSEC indicate that the intelligence agency does not consider metadata to be subject to the same privacy protections accorded to content.[31] Canadian privacy commissioners have also highlighted the privacy implications of metadata and information that is not typically classified as "content." In May 2013, the Privacy Commissioner of Canada released a report on the privacy value of IP addresses, noting that one data point could lead to information on website habits that include sites on sexual preferences.[32]

30 Ron Deibert, "To protect Canadians' privacy, telcos must shut the 'back door'," *Globe and Mail*, September 16, 2013, http://www.theglobeandmail.com/globe-debate/to-protect-canadians-privacy-telcos-must-shut-the-backdoor/article14333544/ .

31 Canada. Parliament. Senate. Standing Senate Committee on National Security and Defence. *Minutes of Proceedings*. 1st sess., 39th Parliament, Meeting Nos. 26, 27, 2007, http://www.parl.gc.ca/Content/SEN/Committee/391/defe/15evbe.htm?comm_id=76&Language=E&Parl=39&Ses=1.

32 "What an IP address can reveal about you: a report prepared by the Technology Analysis Branch of the Office of the Privacy Commissioner of Canada," May 2013, https://www.priv.gc.ca/information/research-recherche/2013/ip_201305_e.asp.

In July 2013, Ontario Privacy Commissioner Ann Cavoukian issued a primer on metadata for consumers, asserting that such data may be more revealing than content.[33]

In a decision on the case R. v. Vu in November 2013, the Supreme Court ruled that authorities must obtain specific authorization to search computers or other electronic devices located on the premises outlined in a search warrant, noting that the "privacy interests implicated by computer searches are markedly different from those at stake in searches of receptacles such as cupboards and filing cabinets."[34]

There were no documented cases of violence or physical harassment of internet users in Canada for their online activities during the reported period.

There have been several high profile cyberattacks and data breaches in Canada, including some that have involved the government. In 2011, a cyberattack apparently launched from China targeted several government agencies, including Defence Research and Development Canada, the civilian branch of the Department of National Defence.[35] Canadian universities have also reported a rise in cyberattacks over the past year.[36] In May 2013, a study released by the U.K.-based International Cyber Security Protection Alliance stated that nearly 70 percent of Canadian businesses had experienced cyberattacks.[37]

33 Canada. Information and Privacy Commissioner. *A Primer on Metadata: Separating Fact from Fiction*. Ottawa, Ont., 2013. http://www.privacybydesign.ca/content/uploads/2013/07/Metadata.pdf.

34 Supreme Court of Canada, R. *v.* Vu, 2013 SCC 60, [2013] 3 S.C.R. 657, November 7, 2013, http://www.canlii.org/en/ca/scc/doc/2013/2013scc60/2013scc60.html?searchUrlHash=AAAAAQALMjAxMyBTQ0MgNjAAAAAAAQ.

35 Greg Weston, "Foreign hackers attack Canadian government," CBC News, February 16, 2011, http://www.cbc.ca/news/politics/foreign-hackers-attack-canadian-government-1.982618.

36 Eric Andrew-Gee, "Cyber attacks a growing problem for Canadian universities," *Toronto Star*, September 22, 2013, http://www.thestar.com/news/gta/2013/09/22/cyber_attacks_a_growing_problem_for_canadian_universities.html.

37 "Nearly 70 percent of Canadian businesses hit by cyber attacks, says year-long survey," CTV News, May 8, 2013, http://www.ctvnews.ca/sci-tech/nearly-70-of-canadian-businesses-hit-by-cyber-attacks-says-year-long-survey-1.1272687.