Canada

Key Developments: June 2014 – May 2015

- In January 2015, the Canadian Radio-television and Telecommunications Commission (CRTC) issued a ruling grounded in the principles of net neutrality which stated that telecommunication companies cannot set rules or prices that favor their streaming services over those of competitors (see Media, Diversity, and Content Manipulation).

- In June 2014, a court in British Columbia issued a decision, which was subsequently upheld by an appeals court, requiring Google to remove search results for a copyright-infringing company on all of its domains, not just Google.ca (see Content Removal).

- The government passed two laws, the Digital Privacy Act (Bill S-4) and the Protecting Canadians from Online Crime Act (Bill C-13), which have significant implications for Canadian internet users’ right to privacy (see Surveillance, Privacy, and Anonymity).
Canada

Editor’s Note

The following chapter covers developments in Canada through May 31, 2015. In June 2015, the Canadian parliament passed Bill C-51, also known as the “Anti-terrorism Act, 2015.” This law caused significant controversy due to its vague wording and provisions that could have a negative impact on freedom of expression and the right to privacy. However, since the law was passed outside of this report’s coverage period, it did not have an impact on this year’s scores.

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, as well as a well-developed set of rules regulating intermediary liability in cases of copyright infringement.

Despite these strengths, there remains considerable unease among many Canadians with respect to online rights. Legislative reforms involving privacy protections and surveillance have generated some controversy, with many Canadians concerned about plans to expand the scope for companies to make voluntary disclosures of personal user information without court oversight. While the Canadian Radio-television and Telecommunications Commission (CRTC) issued a positive decision with regard to protecting net neutrality, the Canadian courts have issued several rulings that could increase intermediary liability and restrict access to information.

Obstacles to Access

There are very few infrastructural or regulatory obstacles to internet access in Canada. The internet and mobile phone penetration rates continue to grow, although there are still some barriers related to the affordability of internet access.

Availability and Ease of Access

According to the International Telecommunication Union, the internet penetration rate in Canada reached 87 percent in 2014, compared to 86 percent in 2013 and 80 percent in 2009. Canada had a mobile phone penetration rate of over 83 percent in 2014. Mobile carriers have deployed a number of newer technologies to provide mobile broadband service, including HSPA+ and LTE.

The government and the Canadian Radio-television and Telecommunications Commission (CRTC), an independent public regulator for the telecommunications sector, have different broadband targets. The CRTC’s 2015-2016 Priorities and Planning Report seeks to provide 100 percent of the population broadband access at speeds of 5 Mbps download or higher by the end of 2015, while, the government has set relatively low speed goals and a longer time frame in a plan that would still leave three-quarters of a million Canadians without access. Industry Minister James Moore promoted the

---

government’s commitment to broadband access in the summer of 2014 with “Connecting Canadians,” a program to bring internet access to 280,000 Canadians who currently do not have access or who have access at speeds considered to be too slow. According to a government release, by 2017 the $305 million investment would extend access at 5 Mbps to 98 percent of Canadian households. However, according to Industry Canada’s recently released 2015-2016 Report on Priorities and Planning, the target date for providing the 280,000 Canadians with new or faster access is now March 2019.

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 is closer to 63 percent. 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. Additionally, there is a wide range of content available in both of Canada’s official languages (English and French) as well as many other languages.

Restrictions on Connectivity

There are no government restrictions on bandwidth, although access providers frequently offer services with caps on bandwidth that result in increased fees for users who exceed the limit. 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 in theory could facilitate greater control of content and the implementation of surveillance technologies.

ICT Market

To operate as a Canadian telecommunications carrier, a company must meet the requirements in section 16 of the Telecommunications Act. In 2013, Canadian telecommunications revenues amounted to $44.8 billion. The five largest telecommunications companies, five largest cable companies, and five largest independent resellers captured 97 percent of total industry revenues.

Canadians have a choice of wireless internet providers, all of which are privately owned. There are at least three providers to choose from 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, three companies dominate the market: 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 continued to emphasize the need for more competition in this market, using a spring 2015 spectrum auction to provide new entrants with advantages in the acquisition of new spectrum.

Regulatory Bodies

The Canadian Radio-television and Telecommunications Commission (CRTC), the regulatory body that oversees the communications industry, operates largely independently from the government. The government appoints the CRTC chair and commissioners. 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 2011.5

Limits on Content

The Canadian government does not generally block websites or filter online content. Illegal content may be removed by legal action taken through the court system.6 YouTube, Facebook, Twitter, and international blog-hosting services are freely available. However, there have been several court cases in recent years that have had negative impacts on intermediary liability, which could have the effect of increasing censorship.

Blocking and Filtering

The government does not generally block or filter online content, and 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).7 Accessing child pornography is illegal in Canada under section 163.1(4.1) of the criminal code.8 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, the national tipline for reporting exploitation of children, which will assess the site and, if necessary, obtain an independent, binding judgment from the National Child Exploitation Coordination Centre.9 An appeals process has also been put into place for cases in which content providers believe that their content has been wrongly blocked, although the list of blocked sites is not public since it would essentially provide a directory of child pornography.10 The project blocks approximately 1,000 child pornography images each year.

In April 2015, the government of Quebec announced plans in its budget to require ISPs to block access to online gambling sites. The list of blocked sites will be developed by Loto-Québec, a gov-

8 Criminal Code, RSC 1985 c C-46 s 163.1(4.1).
9 OpenNet Initiative, “United States and Canada Overview.”
ernment agency. This is expected to act as a revenue-enhancing measure for the government by direct-
gamblers to the state government’s own Loto-Québec-run online gaming site, Espacejeux. A Novem-
ber 2014 report found that Espacejeux was not meeting revenue targets, due to the popular-
ity of other sites. The government believes that the website blocking will increase revenues by $13.5 million in 2016-17 and $27 million per year thereafter. The plan is likely to face a legal challenge, both on free speech and jurisdictional grounds, since the federal government has exclusive jurisdic-
tion over telecommunications regulation.

The federal government’s tough anti-spam law, which regulates commercial electronic messages,
took effect on July 1, 2014. The law prescribes certain content requirements in electronic messages (such as unsubscribe mechanisms and location information) and restricts sending such messages without appropriate consent. There have been several enforcement actions involving the law. The first CRTC case involved Compu-Finder, a Quebec-based corporate training company that sent commercial emails without consent and without a proper unsubscribe mechanisms. Their email practices accounted for a quarter of the complaints in the sector received by the CRTC. In response, the company was hit with a $1.1 million penalty in March 2015.

The CRTC concluded its second case later the same month, this time targeting Plenty of Fish, the popular online dating site. The Commission received complaints that the company was sending commercial emails without a clear and working unsubscribe mechanism. One of the key require-
ments in the law is that each commercial email contain an unsubscribe mechanism to allow recipi-
ents to opt-out at any time. Plenty of Fish agreed to settle the case by paying a $48,000 penalty and developing a compliance program to address its email practices.

Content Removal

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. 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, and it is incumbent upon the person who uploaded the infringing content to remove it following a legal decision. 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 no-
tice-and-notice requirements.

The notice-and-notice requirements took effect on January 2, 2015. Despite the good intentions, the notice-and-notice system has been subject to some misuse. At least one U.S.-based anti-piracy firm, Rightscorp, has used the system to send notifications to subscribers that misstate Canadian law, citing U.S. damage awards and the possibility that their internet access will be terminated, in order to sow fear among Canadians so that they pay a settlement fee.

In June 2015, the British Columbia Court of Appeal upheld an earlier decision by the Supreme Court

---

of British Columbia in *Equustek Solutions Inc. v. Jack*, a closely-watched case involving a court order requiring Google to remove websites that infringed on the plaintiffs’ trademark from its global index. Rather than ordering the company to remove certain links from the search results available through Google.ca, the court’s decision intentionally targeted the entire database, requiring the company to ensure that no one, anywhere in the world, could see the search results. The decision is expected to be appealed to the Supreme Court of Canada.

Defamation claims may also result in the removal of content, as content hosts fear potential liability as a publisher of the defamatory content. Unlike legal protections against liability for copyright infringement by its users, platforms may face liability for alleged defamation once alerted to the publication. A court may also order the removal of the content. A recent Ontario case, *Baglow v. Smith*, involved allegedly defamatory comments posted by a blogger on a political website. Although the Ontario Superior Court decided in favor of the defendants, the court also held that message board operators are not neutral parties to whatever content is exchanged on their platforms. They may, therefore, find themselves liable for defamation if an anonymous individual uses their message board to post a defamatory comment against another individual. Finding otherwise, the court held, would leave plaintiffs without redress when the defamatory comment is made by someone anonymous.

**Media, Diversity, and Content Manipulation**

The online environment in Canada is relatively diverse, and internet users have access to a wide range of news, content, and opinions. There does not appear to be widespread self-censorship in Canadian online publications, and 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. 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.

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. In January 2015, the CRTC issuing a landmark decision on the net neutrality and “zero-rating” concerns associated with mobile television services offered by Bell and Vidéotron. The CRTC found that, by setting prices that favor their streaming services over others, Bell and Videotron had violated the rules that prohibit carriers from granting themselves an undue preference or creating an unreasonable disadvantage for competitors. It noted that the services “may end up inhibiting the introduction and growth of other mobile TV services accessed over the internet, which reduces innovation and consumer choice.” The decision was clearly grounded in net neutrality principles.

CRTC Chair Jean-Pierre Blais, speaking prior to the release of the decision, stated that there would be “no fast and slow lanes,” adding that “at its core, this decision isn’t so much about Bell or Vidéotron. It’s about all of us and our ability to access content equally and fairly, in an open market that favors innovation and choice.”

---

13 Baglow v Smith, [2015] ONSC 1175 (CanLII), [http://canlii.ca/t/ggf1t](http://canlii.ca/t/ggf1t).
14 Baglow v Smith.
Digital Activism

Social media and communication applications have been widely used in Canada for the mobilization of political and social movements. The most recent example involved the widespread protests over Bill C-51, the Anti-Terrorism bill, introduced in January 2015. The bill, among other things, introduced criminal penalties for sharing content deemed “terrorist propaganda” or for encouraging others to engage in terrorist acts, and sparked significant online and offline protests, including protests in cities across Canada. Hundreds of thousands of people signed online petitions and raised concerns through digital means. Moreover, the most influential commentary on the bill came through the efforts of Professors Craig Forcese and Kent Roach, who used open access publishing to release hundreds of pages of analysis. The accessibility of Forcese and Roach’s work raised public awareness and ultimately led to several important reforms to the bill.

Violations of User Rights

Despite having a generally positive record for freedom of expression, Canada has taken some regressive steps in recent years, 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 information requests.

Legal Environment

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. Under the Charter, one’s freedom of expression is “subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society.” These laws and protections apply to all forms of speech, whether online or offline.

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. 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, 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.

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 state-
ment could also be construed as a violation of the provisions that protect a number of enumerated
groups.

Libel tourism, or the practice of taking up a libel case in a jurisdiction considered to be more fa-
vorable 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 indicat-
ed 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.

Prosecutions and Detentions for Online Activities

Citizens can be subject to legal sanction for possessing, accessing or even distributing child pornog-
raphy if they post images of it on the internet. This also extends to text messages, for example in
the January 2014 case of a teenager who sent texts containing explicit images of another teenager
and was convicted of possession of child porn. Generally, writers, commentators, and bloggers are
not subject to legal sanction for content that they post on the internet.

Surveillance, Privacy, and Anonymity

The past year was a significant one for legislation and court cases involving surveillance and privacy.
The Canadian government passed three new laws with privacy implications. In June 2015 the gov-
ernment passed Bill S-4, the Digital Privacy Act, which expanded the scope for companies to make
voluntary warrantless disclosures of personal information by allowing for such disclosures to any
organization, not just law enforcement. The bill also established new mandatory security breach dis-
closure requirements and enhanced the meaning of consent within the law.

Bill C-13, the lawful access and cyber-bullying bill, passed in the fall of 2014. The bill created a new
warrant that allows a judge to order the disclosure of transmission data where there are reasonable
grounds to suspect that an offense has been or will be committed, the identification of a device
or person involved in the transmission will assist in an investigation, or will help identify a person.
Although this bill preserves judicial oversight of access to metadata, the standard for releasing this
data is much lower than the “reasonable grounds to believe” standard, which many thought should

18 Kevin Bissett, “Douglas Hugh Stewart, New Brunswick Man, Gets 5 Years In Prison For Millions Of Child Porn Images,”
yy/1RTm8Ev.
have been adopted in the language of the bill. Critics argued that there is reason for concern, as there are significant implications in treating metadata as having a low privacy value. The government passed the bill in the House of Commons in October 2014.

Bill C-51, or the Anti-Terrorism Act, passed in June 2015 also has major privacy implications. The privacy-related concerns stem from Bill C-51’s Security of Canada Information Sharing Act (SCISA), a bill within the bill, which goes far further than allowing for the sharing of information related to terrorist activity. The bill permits information-sharing across government for an incredibly wide range of purposes, most of which have nothing to do with terrorism. The government tried to justify the provisions on the grounds that Canadians would support sharing information for national security purposes, but the bill allows sharing for reasons that would surprise and disturb most Canadians. The bill was opposed by all Canadian privacy commissioners, but ultimately passed and became law.

Privacy was also a major issue in the courts and in complaints to the privacy commissioner of Canada. The most notable case was the Supreme Court of Canada’s R. v. Spencer decision, released in June 2014. The Spencer decision, which examined the legality of voluntary warrantless disclosure of basic subscriber information to law enforcement, called into question longstanding practices and forced law enforcement and other agencies to re-examine their approach. In a unanimous decision written by Justice Thomas Cromwell, the court issued a strong endorsement of internet privacy, emphasizing the privacy importance of subscriber information, the right to anonymity, and the need for police to obtain a warrant for subscriber information except in exigent circumstances or under a reasonable law. This ruling also calls into question the legality of several privacy-related bills passed during the coverage period.

In December 2014, the Supreme Court of Canada issued its decision in R. v. Fearon, a case involving the legality of a warrantless cellphone search by police during an arrest. To the surprise of many, a divided court upheld the ability of police to search cellphones without a warrant incident to an arrest. The majority opinion established some limiting conditions, but ultimately ruled that it was possible navigate the privacy balance by establishing some safeguards with the practice. A strongly worded dissent noted the privacy implications inherent in warrantless access to cellphones and the need for judicial pre-authorization as the best method of addressing these implications.

The Office of the Privacy Commissioner provides an important oversight function related to privacy of Canadians’ information in the digital medium. The Privacy Commissioner of Canada is an officer of parliament who reports directly to the House of Commons and the Senate. Daniel Therrien was appointed Privacy Commissioner of Canada beginning June 5, 2014. The commissioner’s mandate includes overseeing compliance with the Privacy Act, which covers the personal information-handling practices of federal government departments and agencies, and the Personal Information Protection and Electronic Documents Act (PIPEDA), Canada’s private sector privacy law. In March 2015, the Privacy Commissioner of Canada issued an important finding on the legality of online behavioral advertising, ruling that a targeted advertising program run by Bell violated the law.

**Intimidation and Violence**

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

---

Technical Attacks

There have been several high profile cyberattacks and data breaches in Canada, including some that have involved the government. In July 2014, the Canadian government blamed Chinese hackers for a cyberattack on the Canadian National Research Council. Subsequently, in June 2015, another cyberattack crashed several government websites and e-mail services. The international group Anonymous claimed responsibility for this attack, citing it as a protest against the passage of the Bill C-51 Anti-terrorism Act. 22

---