Canadian Cross-Border Data:

Your Data May Be Heading South Even When You Are Not

By Jacqueline Orr

Canadian data: what goes where?

Canada is fast becoming a technology powerhouse with cities across the country such as Waterloo, Calgary, Toronto, Montreal, and Edmonton transforming into tech hubs. They promise that their research centers and internet companies are going to light the way for Canada's innovation economy.

But the state of Canada's internet is increasingly becoming an oxymoron. While Canada's internet economy might be self-sustaining, the Canadian internet itself is not. Issues of territoriality are fluid and unbound. This is because Canada's network infrastructure relies on American networks to transfer and store data. But, when Canadian data enters the United States, it becomes foreign data and is not protected by the same privacy rights as those accorded to U.S. domestic data and its owners.

CIRA, the Canadian Internet Registration Authority, states that three-quarters of the Canadian population spends three to four hours a day online.[1] CIRA also reports 64 percent of Canadians are concerned about the security of their personal information when it is routed through the United States. Are these concerns justified? This Canada Institute briefing explores key questions about cross-border data travel to better understand the risks and opportunities facing Canadians in an increasingly inter-connected world. There is a glossary at the end of the document.

Is it legal for the U.S. government to collect data from Canadians?

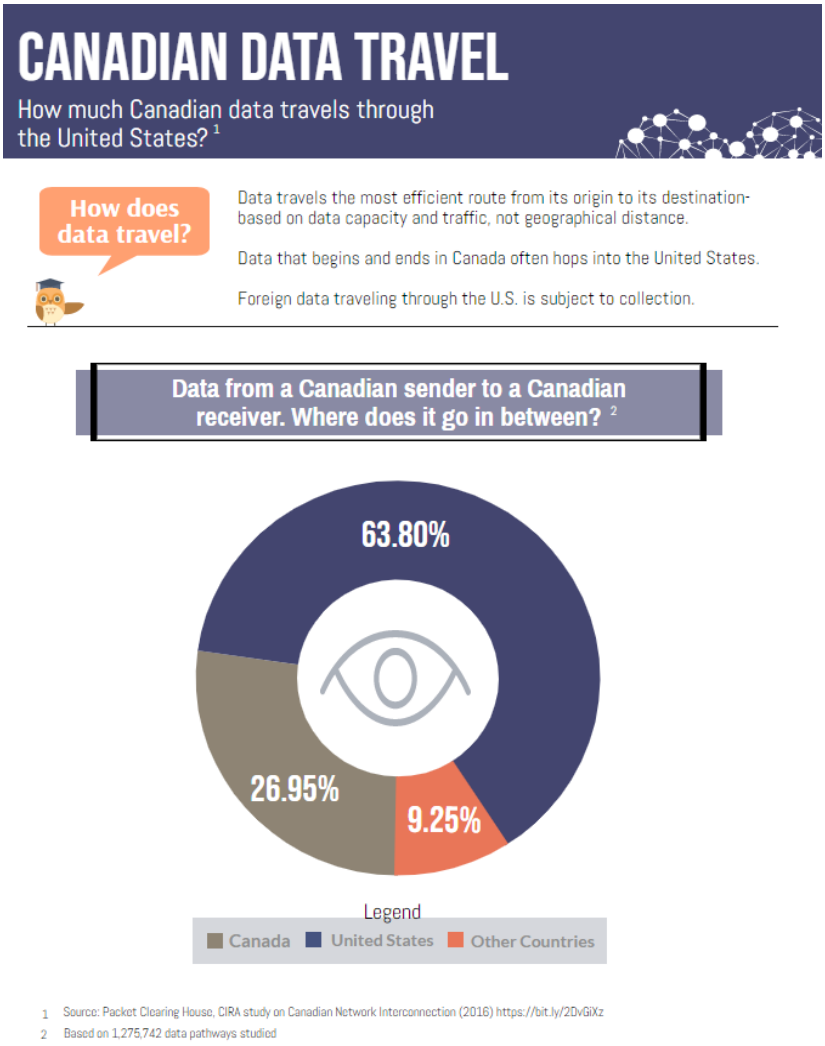
Yes. U.S. government agencies may collect any foreign data that crosses into U.S. territory under the *Foreign Intelligence Surveillance Act of 1978*.[2] Under Section 702, government agencies like the Central Intelligence Agency (CIA) and the Federal Bureau of Investigation (FBI), although primarily the National Security Agency (NSA), are allowed to collect, use, and disseminate electronic communications stored by U.S. Internet Service Providers (ISPs) such as Google, AT&T, Facebook, and Microsoft, including any content that is in transit through the United States.[3]

---

1 *CIRA*, "Canada's Internet Factbook 2018," (April 2019).
2 *Center for Democracy & Technology*, "Section 702: What It Is & How It Works," (February 2017).
3 Laura Donohue, "The Case for Reforming Section 702 of U.S. Foreign Intelligence Surveillance Law," *Council on Foreign Relations* (June 2017).

An NSA program called Downstream (formerly PRISM) collects and analyzes data that is stored on ISPs.[4] Data is duplicated and saved as it travels across the internet as a best-practice measure to increase data transfer speed and security. Devices are routinely attached to internet infrastructure to save data directly onto NSA computers and databases.[5]

The NSA's counterpart program to Downstream is Upstream, which collects data in transit through the Internet Backbone (i.e. cables, towers, and other infrastructure).[6] Thus, any foreign data in the United States is fair game for collection by U.S. federal agencies, even data that begins and ends its journey in Canada.



4 Donohue, (2017).
5 Jonathan A. Obar and Andrew Clement, "Internet Surveillance and Boomerang Routing: A Call for Canadian Network Sovereignty," *TEM JOURNAL 2013* (July 2016), 3.
6 Donohue, (2017).

How does Canadian data find its way into the United States?

Data sent by one user in Country A to another user in Country A, may hop into Country B during transit without either the sender or receiver knowing it.[7] This is called data boomeranging. Some countries have data localization laws that prohibit data from moving outside the country, but, with a few exceptions (such as banking), Canada does not have data localization requirements. Moreover, the USMCA[8] (specifically chapter 19 and chapter 17) has language to discourage mandatory data localization.

Data boomeranging is a practical solution because Canada does not have a lot of internet infrastructure compared to the United States.[9] There is less data storage space and fewer routes and nodes for data to hop along while transiting from place to place. Canadian websites are also routinely hosted, serviced, or have data stored by U.S. organizations. Those organizations' data networks will customarily use a data travel structure called hub-and-spoke that optimizes network infrastructure by connecting data through a central hub.[10] If the organization is based in the United States, the central hub will most likely be located there too. Canadian data frequently stops over in New York City, Chicago, and Washington, D.C., cities that are home to some of the largest data network hubs in North America.[11]

Canadian data also makes its way into the United States when Canadians travel to or through the United States. Foreigners in the United States who connect to U.S. networks are subject to data collection.[12] Even when Canadians remain in Canada, surfing the web is one of the most common ways that Canadian data migrates. A joint study by CIRA and Packet Clearing House found that about 70 percent of the 250 most popular websites in Canada[13] are hosted in the United States and website visitor data will likely be stored on a server in the United States.[14] (See the myths section and infographic for a closer look at this study.)

---

7 Andrew Clement, "Canadian Network Sovereignty: A Strategy for Twenty-First-Century National Infrastructure Building," *Centre for International Governance Innovation* (March 2018).

8 *Office of the United States Trade Representative,* Agreement between the United States of America, the United Mexican States, and Canada Text: Chapter 17: Financial Services and Chapter 19," (2018).

9 Bill Woodcock, "Results of the 2016 PCH / CIRA Study on Canadian Network Interconnection," *Packet Clearing House* and *CIRA* (November 2016).

10 Woodcock, (2016).

11 Ibid.

12 Donohue, (2017).

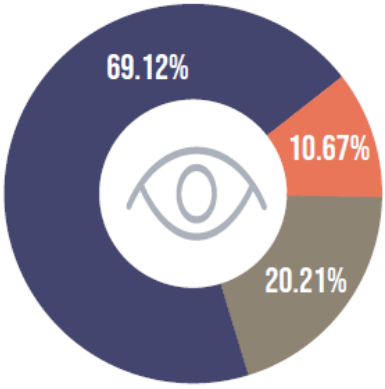
13 Alexa Internet, Inc., "Top Sites in Canada," (April 2019).

14 Woodcock, (2016).

CANADIAN DATA TRAVEL

How much Canadian Data Travels through the United States?

The top 250 most popular internet sites in Canada Where are they hosted? [3]

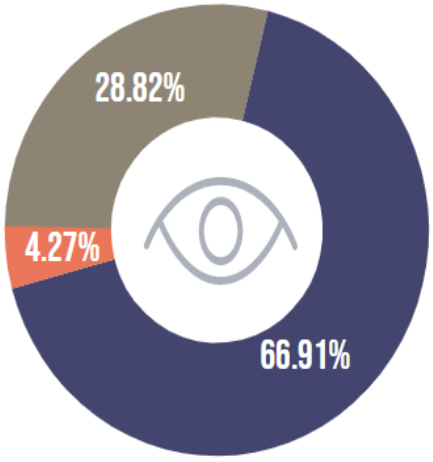


Even among popular Canadian websites hosted in Canada, more than

40%

of data pathways that originated in Canada hopped through the U.S.[4]

What about Canadian government websites? Where are they hosted? [5]



And, believe it or not, even when Canadians access Canadian government websites, their data hops through the U.S.

53%

of the time.[6]

3 Based on 47,906 data pathways studied

4 Based on 9,681 data pathways studied

5 Based on 961 Canadian government websites and 45,291 data pathways studied

6 Based on 13,053 data pathways studied

Created by Mariana Sánchez Ramírez, The Wilson Center, Canada Institute

Why does data not stay in Canada?

Companies have little incentive to avoid boomeranging because adding local internet infrastructure is so expensive. Also, the Canadian network system is smaller, therefore slower, less secure, and more prone to crashes.[15] In order to try to decrease barriers to entry and encourage more competition in the internet services market, the Canadian government has, at times, mandated data-infrastructure sharing, but these mandates have discouraged investment in new infrastructure because they leave one company with a large bill while other companies free ride on faster networks.[16]

When Canadian networks decide to build more infrastructure, they have shown an inclination for bolstering cross-border routes as opposed to adding domestic ones, so cross border routes perform better.[17]

Why don't Canadian internet companies team up?

One way for companies to avoid high latency (i.e. long connection delays) without having to build infrastructure or boomerang is to peer with another network.[18] This kind of agreement, usually costless for both companies, links the two networks' infrastructure together into one larger and more intricate network. Peering increases internet capacity and is especially useful when networks have fluctuating inflows of users. Peering also increases security since data has more than one path to travel along if the main path is compromised.

However, in the current ecosystem of Canadian internet companies vying for an oligopoly seat, a peering network in Canada is rare because smaller companies are perceived to be free riders on larger companies with larger networks.[19] Even though peering is an inexpensive and effective way to upgrade a network, evidence suggests that larger companies are disinclined to peer with smaller companies, potentially helping them grow to become competitors.

Admittedly, larger Canadian internet companies do sometimes peer with smaller Canadian companies, but there's often a catch. Peering networks are linked together by creating or using an exchange point (i.e. an internet bridge that allows data to pass through two or more networks), and larger Canadian networks wanting to increase costs for their peering partner will require that the exchange point is located outside of Canada.[20] To peer with these larger networks, smaller networks lacking cross-border

---

15 Woodcock, (2016).
16 *CBC News*, "Bell challenges cellphone roaming, tower-sharing rules in court," (September 2013).
17 Woodcock, (2016).
18 Ibid.
19 Ibid.
20 Byron Holland, "New study from Packet Clearing House and CIRA looks at Canadian Internet traffic patterns," *The Canadian Internet Registration Authority* ("CIRA") (November 2016).

network infrastructure have to spend a lot of money to send data across the border. So in the competitive Canadian internet environment, Canadian internet companies do team up, it's just normally done outside of Canada, leading to less internet infrastructure investment in Canada and more data boomeranging across the border.

Does the *Patriot Act* give the U.S. government the right to use the personal data of any Canadian who travels to or through the United States?

No, but the *Foreign Intelligence Surveillance Act* does. It gives the U.S. government the right to collect and analyze foreign data in the United States, including data coming from Canada. In 2017 President Trump strengthened this commitment with an executive order stipulating that that protections provided under the *Privacy Act of 1974* only apply to U.S. citizens and permanent residents.[21]

The 2001 *Patriot Act*, passed in the wake of 9/11, is a popular target for critics because it gave the U.S. government the right to expand surveillance to U.S. citizens by removing the requirement that it must be proven that data is foreign before it was collected and investigated. [22] The bill also unlocked previously restricted tools for investigators to "detect and prevent terrorism."[23]

Data does not travel with a state license plate attached. Even with an email or Internet Protocol (IP) address, it is hard to tell whether data is foreign or not without collecting it.[24] Thus, in the process of collecting foreign intelligence, U.S. agencies also have expanded opportunities for surveillance of U.S citizens.

The extent of mass surveillance of citizens was revealed by Edward Snowden in 2013, provoking a backlash from Americans.[25] Critics tried to limit the extent of government surveillance of Americans with the 2015 *USA Freedom Act*. The bill provided some safeguards against aspects of the *Patriot Act* deemed overly invasive but did not address legal loopholes that allow for similarly invasive measures.[26] The government still maintains largely unfettered access to the data of U.S. citizens.[27] The bill is up for re-authorization in 2019. In March, a bill was introduced to end government

---

21 Bill Zimmer, "PROTECTING CANADIANS' PRIVACY AT THE U.S. BORDER," *House of Commons Canada* (December 2017).
22 Donohue, (2017).
23 *The United States Department of Justice*, "The USA PATRIOT Act: Preserving Life and Liberty," (March 2019).
24 Asaf Lubin, "We Only Spy on Foreigners: The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance," *Chicago Journal of International Law*, Vol. 18, No. 2 Winter 2018 (July 2017), 539.
25 Glen Greenwald, "THE U.S. GOVERNMENT'S SECRET PLANS TO SPY FOR AMERICAN CORPORATIONS," *The Intercept*, (September 2014).
26 Emily Birnbaum, "Lawmakers introduce bipartisan bill to end NSA's mass phone data collection program," *The Hill* (March 2019).
27 Ibid.

surveillance on U.S. citizens' phone data.[28]

Who else is watching?

Another important organization in the world of cross-border data collection is the Five Eyes (FVEY), the surveillance co-operation organization that originated in World War II and includes the United States, Canada, New Zealand, Australia, and the U.K. These countries share intelligence data and technologies.[29] While their level of cooperation is believed to be robust, the extent and details of their data-sharing is not publicly known.

What about private companies using my data?

It is illegal for private companies to use your personal data without your consent. It is similar to a houseguest using personal information they find in the host's desk drawer. Both the United States and Canada have privacy laws that cover digital personal data. In Canada, private companies must comply with Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), a law that is similar to the European Union's General Data Protection Regulation (GDPR), which requires companies to be responsible for safeguarding personal data.[30] There is no central data privacy law in the United States, but data privacy is dealt with in various federal and state legislation.[31]

PIPEDA obligations include protecting data, limiting the use of data to necessary activities, safely destroying irrelevant data, and receiving "meaningful consent"[32] from data owners for how their data will be used.[33] Openness is one of PIPEDA's main principles and any form of consent obtained through deceit is deemed noncompliant with the law.[34]

As responsible parties, companies handling personal data have to ensure that third parties processing their data (e.g. companies handling data that is boomeranged into the United States) are not compromising their compliance with PIPEDA. U.S. private companies directly working in Canada are not exempt from compliance under PIPEDA.[35]

---

28 Ibid.
29 Lubin, (2017), 505.
30 Quebec, Alberta, British Columbia are not covered by PIPEDA but have similar laws to PIPEDA. *Government of Canada*, "Personal Information Protection and Electronic Documents Act," (March 2019).
31 *Global Legal Group*, "USA: Data Protection 2018," (December 2018).
32 *Office of the Privacy Commissioner of Canada*, "Guidelines for obtaining meaningful consent," (May 2018).
33 *Government of Canada*, (March 2019).
34 Ibid.
35 Ibid.

Could the United States government access foreign intellectual property or personal data and hand it over to private American corporations?

Yes, the U.S. government could theoretically hand over foreign intellectual property or data acquired during routine surveillance to private American companies, but it is unlikely. The U.S. government has been an outspoken critic of IP theft and has an Intellectual Property Task Force dedicated to confronting IP theft on a global scale.[36]

After the Snowden documents were released in 2013, Director of National Intelligence James Clapper defended against accusations that the United States would engage in economic espionage for profit:

> It is not a secret that the Intelligence Community collects information about economic and financial matters… what we do not do… is use our foreign intelligence capabilities to steal the trade secrets of foreign companies on behalf of—or give intelligence we collect to—U.S. companies to enhance their international competitiveness or increase their bottom line.[37]

Will 5G change the data path landscape?

Ironically, as much as Canadians are likely to complain about the public esthetics of 5G infrastructure and the security considerations of dealing with suppliers such as Huawei, 5G will likely help keep Canadian data in Canada and encourage network sharing among Canadian companies.

The 4G internet network is composed of a large number of tall internet towers dispersed across the country. While 5G systems will continue to incorporate 4G towers and other infrastructure, the 5G network will be much more decentralized, relying on backpack-sized (and smaller) internet small cells that can send data along short electromagnetic waves. These small cells cannot carry data very far, but they can carry a lot of it and very quickly.[38] An effective 5G network in Canada will require a proliferation of small cells on streetlamps, around malls, in sporting arenas, even in homes and cars. But, the upside of this profusion of small cells will be greatly increased internet capacity and decreased latency, particularly in densely populated regions.[39]

Because launching 5G will be so expensive and visible to the public,

---

36 A proven case of foreign IP theft by the U.S. government would hurt its current and future foreign relationship. See discussion by former senior CIA analyst Paul Pillar in Mark Hosenball's *article for Reuters*, "Obama halted NSA spying on IMF and World Bank headquarters," (October 2013).

37 James Clapper, "STATEMENT BY DIRECTOR OF NATIONAL INTELLIGENCE JAMES R. CLAPPER ON ALLEGATIONS OF ECONOMIC ESPIONAGE," *Office of the Director of National Intelligence* (September 2013).

38 Ferry Grijpink, Alexandre Ménard, Halldor Sigurdsson, and Nemanja Vucevic, "The road to 5G: The inevitable growth of infrastructure cost," *Mckinsey & Company* (February 2018).

39 Ibid.

Canadian companies will probably have to work together more than they do now. Cooperation in internet infrastructure and network sharing is working well in other countries – particularly in Europe.[40] McKinsey reports that operators benefit from a 30 percent drop in costs of ownership and more efficient networks when they participated in network sharing.[41]

Myth Busting

Myth – The internet is a cloud.

Reality – The internet is a massive network of interconnected machines, digital towers, and cables situated around the world (including in the depths of the oceans). Data hops along multiple nodes in the network before finding its way to the recipient.

Myth – Data travels the most geographically efficient route.

Reality – Data travels the most efficient route based on data-capacity and traffic – even if that means crossing international borders or travelling from City A to City A, via City B.[42]

Myth – Data has a natural owner. It is easy to target an individual's data and communications.

Reality – Even with an IP address or an email address, it is difficult to tell where data originates. Often, court orders are required to track internet users to identify an individual user.[43]

Myth – No U.S. government agency is allowed to monitor private communications in the United States because it violates U.S. citizens' rights to privacy.

Reality – The government is not supposed to target U.S. citizens without cause or use someone's data against them to find legal infractions, but the rules are somewhat different for foreigners (e.g. Canadians) whose data ends up transiting the United States, with or without their knowledge. Under Section 702 of the *Foreign Intelligence Surveillance Act*, government officials are allowed to keep in-transit and stored data in the United States, including U.S. citizens' data, as long as a main purpose for the surveillance relates to U.S. foreign affairs.[44] Every year, the Attorney General and the Director of National Intelligence receives approval to continue this activity from the United States Foreign Intelligence Surveillance Court.[45] Agencies

---

40 Ferry Grijpink, Alexandre Ménard, Halldor Sigurdsson, Nemanja Vucevic, "Network sharing and 5G: A turning point for lone riders," *Mckinsey & Company* (February 2018).
41 Ibid.
42 Lubin, (2017), 534.
43 Lubin, (2017), 539.
44 Donohue, (2017).
45 *Center for Democracy & Technology*, (February 2017).

are not required to delete irrelevant data.[46]

Myth – Data in the United States is considered domestic until proven foreign.

Reality – If the NSA is in doubt about whether data is foreign or domestic, the default option is to consider it foreign.[47] This includes data from abroad that has hopped into the United States from another country as well as U.S. data that has hopped across an international border and back into the United States.

Myth – Encrypted data can be collected but not hacked into.

Reality – Encryption, i.e. data twisted into a secret code requiring a personal password or proof of access to a personal device, is an effective way to keep data safe. But even encrypted data is not immune to being decoded once collected. The 2013 Snowden documents revealed that most encryption on the internet was no match for the NSA but, since then, internet users have been using more sophisticated technology to lock out prying eyes.[48] In response the NSA has tried to compel companies to write backdoors into encryptions but, at present, the encryptors still have the advantage. The future ability of the NSA to use personal data will depend on their own technological prowess and their ability to legally compel corporations to hand over their systems' data to or to let them in through back doors.[49]

Glossary

General Data Protection Regulation (GDPR): The European Union's data privacy policy that guarantees data subjects (i.e. internet users) ownership over their own data. Among many requirements, it obliges internet companies to receive meaningful and clear consent to use a data subject's data.[50] It also requires that data subjects can easily request and receive all data a company has on file about them and ask a company to "forget" them by asking them to delete their data file.[51]

Hop: Data does not travel through the air from a sender to a receiver like a carrier pigeon, instead it travels the most efficient route from one node to another until it reaches its final destination.[52] Data is said to hop along nodes.

---

46 Ibid.
47 Lubin, (2017), 515.
48 Sharon D. Nelson and John W. Simek, "How to Protect Data from Uncle Sam," American Bar Association, *Litigation* 41, no. 1 (2014): 11-12. Amanda Ziadeh, "To Break or Not Break Encryption: The Global Debate," *Government CIO Media & Research* (November 2018).
49 See for example Sinéad Baker, "These towering, windowless, bomb-proof buildings in major US cities are reportedly part of an under-the-radar partnership between AT&T and the NSA," *Business Insider* (June 2018).
50 *Intersoft Consulting*, "General Data Protection Regulation GDPR," (April 2019).
51 Ibid.
52 Lubin, (2017), 534.

Internet Exchange Point (IXP): When multiple ISPs will agree to share their internet infrastructure with each other and share operation costs, the place where those networks connect is called an Internet Exchange Point.[53] An IXP is beneficial for all parties because it generally means they have access to a very large internet network that is faster and more secure without having to pay the full cost on their own or contract with a large ISP for access to more infrastructure.[54] Joining an IXP means these ISPs only have to pay for a share of the IXP's operational costs.[55]

Internet Backbone: A term to describe the largest data traffic routes between large internet networks. Since the U.S. government invented the internet, the United States has a strong internet backbone, but there are internet backbones in other countries as well as between countries and continents.

Internet Service Provider (ISP): A company that provides internet access to customers so they can transmit data and other communications including email, voice or video calls, or television services.[56]

Latency: The time it takes data to travel from one node to another. This includes the time it takes to access a webpage after clicking a web link, to send an email, or to download a file from the internet. When the internet connection is slow, latency is high.

Node: The point where data paths connect within a network. A node could be a phone, a router, a printer, a computer in a data center or any device that can send or receive information.

Upstream network: When an Internet Service Provider (ISP) finds its own internet infrastructure lacking, it will pay to connect to another ISP that has more internet infrastructure, forming an upstream network.[57] That larger ISP will in turn pay to connect to another ISP with an even larger network. This continues until you reach a massive ISP at the top of the network pyramid that has access to all the other ISPs' internet infrastructure without paying for this access.[58]

Sources

Alexa Internet, Inc. April 2019. "Top Sites in Canada." www.alexa.com/topsites/countries/CA.

Baker, Sinéad. June 2018. "These towering, windowless, bomb-proof buildings in major US cities are reportedly part of an under-the-radar partnership between AT&T and the NSA." *Business Insider*. www.businessinsider.com/att-buildings-around-us-reportedly-used-as-

53 *Techopedia*, "Internet Exchange Point (IXP)," (March 2019).
54 Ibid.
55 Ibid.
56 *Techopedia*, "Internet Service Provider (ISP)," (March 2019).
57 *Techopedia's* "*Internet Service Provider*," (March 2019).
58 Ibid.

part-of-nsa-spying-2018-6.

Birnbaum, Emily. March 2019. "Lawmakers introduce bipartisan bill to end NSA's mass phone data collection program." *The Hill*. thehill.com/policy/technology/436482-lawmakers-introduce-bill-to-end-nsas-mass-phone-data-collection-program.

CBC News. September 2013. "Bell challenges cellphone roaming, tower-sharing rules in court." www.cbc.ca/news/business/bell-challenges-cellphone-roaming-tower-sharing-rules-in-court-1.1706476.

Center for Democracy & Technology. February 2017. "Section 702: What It Is & How It Works." *CDT*. www.cdt.org/insight/section-702-what-it-is-how-it-works/.

CIRA. April 2019. "Canada's Internet Factbook 2018." https://cira.ca/factbook/canada%E2%80%99s-internet-factbook-2018.

Clapper, James. September 2013. "STATEMENT BY DIRECTOR OF NATIONAL INTELLIGENCE JAMES R. CLAPPER ON ALLEGATIONS OF ECONOMIC ESPIONAGE." Office of the Director of National Intelligence. www.dni.gov/index.php/newsroom/press-releases/press-releases-2013/item/926-statement-by-director-of-national-intelligence-james-r-clapper-on-allegations-of-economic-espionage.

Clement, Andrew. March 2018. "Canadian Network Sovereignty: A Strategy for Twenty-First-Century National Infrastructure Building." *University of Toronto - Faculty of Information*. www.cigionline.org/articles/canadian-network-sovereignty.

Donohue, Laura. June 2017. "The Case for Reforming Section 702 of U.S. Foreign Intelligence Surveillance Law." *Council on Foreign Relations*. https://www.cfr.org/report/case-reforming-section-702-us-foreign-intelligence-surveillance-law.

Global Legal Group. December 2018. "USA: Data Protection 2018." iclg.com/practice-areas/data-protection-laws-and-regulations/usa.

Government of Canada. March 2019. "Personal Information Protection and Electronic Documents Act." laws-lois.justice.gc.ca/eng/acts/P-8.6/page-11.html#h-26.

Greenwald, Glen. September 2014. "THE U.S. GOVERNMENT'S SECRET PLANS TO SPY FOR AMERICAN CORPORATIONS."*The Intercept*. theintercept.com/2014/09/05/us-governments-plans-use-economic-espionage-benefit-american-corporations/.

Grijpink, Ferry, Alexandre Ménard, Halldor Sigurdsson, and Nemanja Vucevic. February 2018. The road to 5G: The inevitable growth of infrastructure cost." *Mckinsey & Company*. www.mckinsey.com/industries/telecommunications/our-insights/the-road-to-5g-the-inevitable-growth-of-infrastructure-cost."

Grijpink, Ferry, Alexandre Ménard, Halldor Sigurdsson, and Nemanja Vucevic. February 2018. Network sharing and 5G: A turning point for lone riders." *Mckinsey & Company*. www.mckinsey.com/industries/telecommunications/our-insights/network-sharing-and-5g-a-turning-point-for-lone-riders."

Holland, Byron. November 2016. "New study from Packet Clearing House and CIRA looks at Canadian Internet traffic patterns." *Canadian Internet Registration Authority*. cira.ca/blog/state-internet/new-study-packet-clearing-house-and-cira-looks-canadian-internet-traffic.

Hosenball, Mark. October 2013. "Obama halted NSA spying on IMF and World Bank headquarters." *Reuters*. www.reuters.com/article/us-usa-security-imf/obama-halted-nsa-spying-on-imf-and-world-bank-headquarters-idUSBRE99U1EQ20131031.

Intersoft Consulting. April 2019. "General Data Protection Regulation GDPR." gdpr-info.eu/.

Lubin, Asaf. July 2017. "We Only Spy on Foreigners: The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance." *Chicago Journal of International Law*, Vol. 18, No. 2 (Winter 2018). papers.ssrn.com/sol3/papers.cfm?abstract_id=3008428.

Nelson, Sharon D., and John W. Simek. 2014. "How to Protect Data from Uncle Sam." *Litigation* 41, no. 1 (2014): 11-12. www.jstor.org/stable/44678116.

Obar, Jonathan A., and Andrew Clement. February 2014. "Internet Surveillance and Boomerang Routing: A Call for Canadian Network Sovereignty." *TEM JOURNAL 2013*. papers.ssrn.com/sol3/papers.cfm?abstract_id=2311792.

Office of the Privacy Commissioner of Canada. May 2018. "Guidelines for obtaining meaningful consent. www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/.

Office of the United States Trade Representative. 2018. "Agreement between the United States of America, the United Mexican States, and Canada Text: Chapter 17 Financial Services." ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/17_Financial_Services.pdf.

Office of the United States Trade Representative. 2018. "Agreement between the United States of America, the United Mexican States, and Canada Text: Chapter 19 Digital Trade." ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19_Digital_Trade.pdf.

Techopedia. March 2019. "Internet Exchange Point." www.techopedia.com/definition/27705/internet-exchange-point-ixp.

Techopedia. March 2019. "Internet Service Provider (ISP)." www.techopedia.com/definition/2510/internet-service-provider-isp.

The United States Justice Department. March 2019. "Intellectual Property Task Force." www.justice.gov/iptf.

The United States Department of Justice. March 2019. "The USA PATRIOT Act: Preserving Life and Liberty." www.justice.gov/archive/ll/highlights.htm.

Woodcock, Bill. November 2016. "Results of the 2016 PCH / CIRA Study on Canadian Network Interconnection." *Packet Clearing House* and *CIRA*. https://cira.ca/sites/default/files/public/Canadian%20Peering%202016.pdf.

Ziadeh, Amanda. November 2018. "To Break or Not Break Encryption: The Global Debate." *GovernmentCIO Media & Research*. governmentciomedia.com/break-or-not-break-encryption-global-debate.

Zimmer, Bill. December 2017. "PROTECTING CANADIANS' PRIVACY AT THE U.S. BORDER." *House of Commons Canada*. www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9264624/ethirp10/ethirp10-e.pdf.