Professor Lisa Austin and Mr. Daniel Carens-Nedelsky prepared the following report specifically addressing the context of Universities engaging in the extra-national outsourcing of eCommunications. The implications of their findings extend well beyond Universities, to any Canadian organization, and to any type of extra-national digital outsourcing: to any use of Software as a Service (SaaS), Platform as a Service (PaaS) or Infrastructure as a Service (IaaS) where data containing the personal information of Canadians is stored and/or processed outside of Canada.

Why Jurisdiction Still Matters

Lisa M. Austin

Daniel Carens-Nedelsky

May 31, 2015

1. Introduction

Our research shows that Universities, when making the decision to outsource eCommunications extra-nationally, have relied upon federal and provincial Privacy Commissioner decisions that conclude: "the risk of personal information being disclosed to government authorities is not a risk unique to U.S. organizations. In the national security and anti-terrorism context, Canadian organizations are subject to similar types of orders to disclose personal information held in Canada to Canadian authorities."[1] In this report we call this position the "similar risk" analysis and we argue that it is wrong. Given the information now available due to the Snowden revelations and subsequent government disclosures, Universities should reassess this

[1] *Bank's notification to customers triggers PATRIOT Act concerns* (19th October 2005), 2005-313, online: OPC <https://www.priv.gc.ca/cf-dc/2005/313_20051019_e.asp> [*PIPEDA 313*].

Lisa M. Austin and Daniel Carens-Nedelsky, "Why Jurisdiction Still Matters," May 31, 2015. This legal analysis was prepared as part of a research project funded by the Office of the Privacy Commissioner of Canada's 2014-2015 Contributions program "Assessing the Privacy Risks of Extra-National Outsourcing of eCommunications" and forms Appendix B of the final report. The complete project findings and recommendations are available at http://ecommoutsourcing.ischool.utoronto.ca/. This project has been funded by the Office of the Privacy Commissioner of Canada (OPC); the views expressed herein are those of the author(s) and do not necessarily reflect those of the OPC.

understanding of the privacy implications of extra-national outsourcing, particularly of eCommunications.

What is missing when institutions adopt the "similar risk" analysis?

1. The Constitutional Question

The "similar risk" analysis looks at whether state authorities can get access to information. What it does not ask is: access on what standards and with what mechanisms of accountability and oversight? Debates about the sufficiency of such standards, as well as accountability and oversight mechanisms, are what animate constitutional discourse regarding privacy and so we call this the constitutional question. The "similar risk" analysis does not ask this question about Canadian constitutional norms regarding privacy or note the relevant ways in which Canadian constitutional privacy norms are more robust than US constitutional privacy norms.

2. We Are Non-US Persons

The "similar risk" analysis is not sensitive to the fact that non-US persons receive significantly less protection under a number of US laws than US persons. It is also not sensitive to the fact that when non-US persons store their data in the US but otherwise remain outside of the US, then US constitutional norms do not apply to them – which is why US statutes can discriminate between US and non-US persons.

3. It's Not Just the USA Patriot Act

The "similar risk" analysis does not look at the US *Foreign Intelligence Surveillance Act* (FISA). Section 702 of FISA allows US authorities to access communications data (both content and metadata) without a warrant. The "similar risk" analysis also does not look at the US *Electronic Communications Privacy Act*, which allows US authorities to access stored emails and other electronic information without a warrant in a number of circumstances.

This report is focused on the privacy risks associated with extra-national outsourcing, as that is the current context of the University outsourcing decisions that we looked at. We do not look in detail at the potential extra-territorial reach of US law *within* Canada, such as the circumstances under which a Canadian organization operating within Canada (whether a Canadian subsidiary of a US company or otherwise) could be subject to US orders for the disclosure of information. This latter type of extra-territorial claim can be in conflict with Canadian sovereignty, especially where a US order conflicts with Canadian law. We discuss this issue briefly, along with the "blocking statutes" that respond to these concerns, in Appendix C of this report. The question of the extra-territorial reach of US law is also currently garnering international attention in relation to the Microsoft Ireland case, which we discuss in s. 5.3 of this report. While this issue is not the focus of this report, our comparative constitutional analysis does reveal the way in which several US laws are deeply inconsistent with Canadian constitutional doctrine, and is thus highly relevant to the question of the extra-territorial application of US laws.

2. Summary of Argument

As we show in this report, if one supplements the 'similar risk' analysis with the three missing components (the constitutional question, US treatment of non-US persons, and the importance of statutes beyond the USA Patriot Act) the following becomes clear:

- US authorities can access Canadian persons communications data within US jurisdiction on statutory standards that are lower than those that apply within Canada and would be unconstitutional if applied within Canada.
- US constitutional law does not apply when US authorities access Canadian persons communications data within US jurisdiction as long as the Canadian person remains outside of the US.
- Even if US constitutional law did apply, Canadian constitutional law offers more privacy protection to communications data.

- Although Canadian authorities may share information with US authorities in some circumstances, both the collection of this information and its sharing is subject to Canadian law and Canadian constitutional standards.
- Mutual Legal Assistance Treaties ensure that the constitutional norms of the "assisting" country are applied. Therefore US authorities obtaining Canadian person information through the MLAT process are subject to stricter norms than US authorities obtaining Canadian person information within US jurisdiction.

3. The 'Similar Risk' Analysis

As stated above, the "similar risk' analysis argues that because both Canadian and American governments have legal mechanisms through which they can access Canadians' electronic information, Canadians' data is at a no greater risk of surveillance when stored in the US than in Canada.

This analysis was first articulated in a 2005 decision of the Office of the Privacy Commissioner of Canada (OPC) under the *Personal Information Protection and Electronic Documents Act* (PIPEDA). The case involved an investigation into a number of complaints made by CIBC costumers. They were concerned that their personal information was not adequately protected because a US-based company was processing it. Of particular concern to customers was the USA Patriot Act, legislation passed just after 9/11 that significantly expanded the powers of US authorities to access private information for intelligence gathering and law enforcement purposes. Further, it included provisions making it illegal for companies to inform costumers that US authorities had accessed their information. CIBC's customers argued that because American companies were subject to the USA Patriot Act, their private information could never be adequately protected by contractual agreements.[2]

The OPC report readily conceded this point, noting that "while customer personal information is in the hands of a foreign third-party service provider, it is subject to the laws of that country and no contract or contractual provision can override

[2] *PIPEDA 313 supra note* 1.

those laws."[3] As a result of this, the office concluded that "an organization with a presence in Canada that outsources the processing of personal information to a U.S. firm cannot prevent its customers' personal information from being lawfully accessed by U.S. authorities."[4]

However, the report proceeded to find that in the wake 9/11, Canadian authorities had been granted similar powers to access private information.[5] Thus the report concluded that the costumer's information was equally secure (or insecure) in both countries, making the relevant question whether CIBC had negotiated for sufficiently protective contractual provisions, notwithstanding that they could be rendered moot by the USA Patriot Act. In essence, the report argued that because similar privacy limiting legislation existed in both countries there was no substantial difference between CIBC outsourcing data to a company based in American or one operating entirely within Canada. To further buttress this finding the report noted that there are "longstanding formal bilateral agreements between the U.S. and Canadian government agencies that provide for mutual cooperation and for the exchange of relevant information,"[6] suggesting that regardless of where information is stored it can find its way to the governments of both countries.

Taken as a whole, this is what we refer to as the 'similar risk' analysis. This analysis has subsequently been widely (and uncritically) relied on by both governmental and private sector organizations.[7] It is worth noting that Heather Black, the Assistant Privacy Commissioner who resolved the 2005 complaint subsequently co-authored an editorial calling for a Canadian governmental response to the lack of

---

[3] *PIPEDA 313 supra note* 1.
[4] *Ibid.*
[5] *Ibid.*
[6] *PIPEDA 313 supra note* 1, at p. 3.
[7] See *Canadian-based company shares customer personal information with U.S. parent* (July 10 2006), 2006-333, online: OPC <https://www.priv.gc.ca/cf-dc/2006/333_20060511_e.asp>; *Responsibility of Canadian financial institutions in SWIFT's disclosure of personal information to US authorities considered* (2 April 2007), 2007-365, online: OPC < https://www.priv.gc.ca/cf-dc/2007/365_20070402_e.asp>; and *Outsourcing of canada.com e-mail services to U.S.-based firm raises questions for subscribers* (19 September 2009), 2008-394, online: OPC < https://www.priv.gc.ca/cf-dc/2008/394_20080807_e.asp*>; Reviewing the Licensing Automation System of the Ministry of Natural Resources: A Special Investigation Report* (27 June 2012), PC12-39, online: IPC < https://www.ipc.on.ca/images/Findings/2012-06-28-MNR_report.pdf>; Alberta Office of the Information and Privacy Commissioner *Public-sector Outsourcing and Risks to Privacy* (February 2006), online: OIPC < http://www.oipc.ab.ca/Content_Files/Files/Publications/Outsource_Feb_2006_corr.pdf>; Timothy Banks, "Cloud Computing And The USA Patriot Act: Canadian Implications" (2012) 13:3 *Internet and E-Commerce Law in Canada*.

security of Canadian's electronic information brought to light by the Snowden revelations.[8]

4. The Missing Constitutional Question

Contrary to what the 'similar risk' analysis argues, the key question regarding privacy in electronic information is not *if* a given government can access the information, but *on what standards* it can access it. This is what constitutional jurisprudence regarding privacy concerns itself with, and it is what we call the 'missing' constitutional question: an inquiry into what substantive and procedural requirements authorities within each country are required to meet before they can access communications data.

4.1 What Is the Constitutional Question and Why is it Missing?

Data protection laws such as the federal PIPEDA or Ontario's *Freedom of Information and Protection of Privacy Act* (FIPPA) implement what are known internationally as "Fair Information Practices" (FIPs). These principles include purpose specification and limitations on collection, use, retention and disclosure of personal information. While also intended to protect privacy, FIPs have a different focus than the "reasonable expectation of privacy" analysis that is undertaken in constitutional search and seizure jurisprudence.

The constitutional framework focuses on 1) the appropriate threshold, or standard, under which state interests override individual privacy interests, and 2) the framework of oversight and accountability. The default constitutional position, in both Canada and the US, is that in the law enforcement context the appropriate standard for state intrusion is "reasonable and probable cause"[9] that what is searched will provide evidence of an offence. Furthermore, both jurisdictions require prior authorization through a warrant issued by a judge, ensuring that this standard has been met before a search or seizure can legally take place.

---

[8] Lisa Austin et al. "Our Data our Laws" *The National Post* (12 December 2013), online: The National Post <http://news.nationalpost.com/2013/12/12/our-data-our-laws/> (This editorial was also co-authored by Michael Geist, whose previous work also served as key support for the 'similar risk' analysis).
[9] The statutory language is "reasonable grounds to believe". See *Criminal Code, RSC 1985, c C-46* s.487.

The "similar risk" analysis was undertaken within a FIPs framework, not a constitutional one. The main question asked was whether US authorities *could* get access to Canadian information, whether Canadian authorities *could* get access to Canadian information, and whether these authorities *could* share information. The "similar risk" analysis failed to ask the key *constitutional* questions about privacy – access on what standard and with what measure of oversight and accountability. Furthermore, it failed to ask the key constitutional *comparison* question – whether Canadian persons information in the US receives a similar level of constitutional protection. The following section takes up the comparison question.

4.2 Differences Between Canadian and US Constitutional Privacy Protection

Despite the many similarities between the US 4th Amendment protection of privacy and the Canadian *Charter* s.8 protection of privacy, there are some key differences. One such difference is that Canadian constitutional jurisprudence offers Canadians a higher level of protection against electronic surveillance than US constitutional jurisprudence offers Americans. This difference is a result of American 4th Amendment jurisprudence known as the "third party doctrine", a legal interpretation that was used as the justification for the mass warrantless collection of American's phone metadata under the USA Patriot Act.[10] Canadian jurisprudence has consistently rejected this doctrine.

4.2.1 The Third Party Doctrine

The 'third party doctrine' was first articulated by the US Supreme Court in the 1979 decision *Smith v Maryland*, in which the Court ruled that a police request for a phone company to install a 'pen register' (a device which records the numbers of all outgoing call made from a specific phone number) did not constitute a search for the purposes of the 4th Amendment, and thus attracted no constitutional protection.[11]

The key part of the decision was the Court's ruling that Smith (the accused) did not have a reasonable expectation of privacy in this information. The court reasoned that by using the phone company Smith must have known they had access to which

[10] *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from* [REDACTED], No. BR 13-109 (FISA Ct. 2013) at 6 [*Application of the FBI for Tangible Things*].
[11] *Smith v Marlyand* 442 US 735 (1979), at 742 [*Maryland*].

numbers he was calling, and that as a result he had voluntarily assumed the risk that company would record and turn over this information to the police.[12] This decision has been interpreted broadly in what is known as the 'third party' doctrine: there is no warrant requirement for state access to information that has been shared with, or is otherwise available to, a third party.[13]

This doctrine has been upheld by a number of courts as justification for warrantless metadata collection. The 9th circuit in *United States v. Forrester* found that a warrantless collection of both IP address and to/from email information was not protected under the 4th amendment.[14] In *Re: Zynga Privacy Litigation*, the same court ruled that web addresses were also unprotected.[15] Most significantly, the doctrine was accepted by the FISA court as the legal justification for the constitutionality of the controversial 'metadata' phone collection program, in which thousands of American phone metadata was collected without a warrant.[16]

The Supreme Court of Canada explicitly rejected the third party doctrine in a trilogy of electronic surveillance cases in the early 1990s: *R v Duarte* (warrantless interception of communication where one party consents is unconstitutional);[17] *R v Wong* (warrantless video surveillance of a hotel room to which the public is invited is unconstitutional);[18] and *R v Wise* (warrantless installation of a tracking device to locate a car on public roads is unconstitutional).[19] In all three cases the court stated that there was a crucial difference between individuals accepting the risk that *an individual* might have access to certain information (and testify about that information in court) and the risk created by allowing *state authorities* to make recordings of the same information without a warrant.

---

[12] *Marlyand, supra* note 11 at 744.
[13] Laura Donohue, "Bulk metadata collection: Statutory and constitutional considerations." (2014) 37 *Harvard Journal of Law and Public Policy* 757 at 866. [Donohue, "Bulk metadata collection"].
[14] *United States v. Forrester*, 512 F 3d 500 (9th Cir. 2008).
[15] *Re: Zynga Privacy Litigation*, D.C. No. 5:10-cv-04680-JW (9th Cir. 2014). (The court did recognize a possible narrow exception for search engine headings that may reveal the specific search a user used and not just the website they visited).
[16] *Application of the FBI for Tangible Things*, *supra* note 10 at 6.
[17] *R v Duarte*, [1990] 1 SCR 30, [1990] SCJ No 2.
[18] *R v Wong*, [1990] 3 SCR 36, [1990] SCJ No 118..
[19] *R v Wise*, [1992] 1 SCR 527, [1992] SCJ No 16.

4.2.2 Recent Notable Canadian Decisions

A number of recent decisions by the Supreme Court of Canada have reinforced the rulings in the electronic surveillance trilogy and indicate that our court is highly cognizant of the dangers posed by state surveillance of electronic information. The Court has repeatedly ruled that searching the contents of one's computer or electronic information intrudes upon one's reasonable expectation of privacy and will usually be justified only with a warrant.

In the 2012 decision *R v Cole* the court re-iterated its ruling in *R v Morelli* that personal computers contain very private information and thus can only be searched with a warrant.[20] The court then ruled that while the fact that Cole's employer had access to the his work issued laptop for the purposes of maintenance did diminish his expectation of privacy, he nonetheless has a reasonable expectation of privacy in the contents of the laptop such that the state needs a warrant to search its contents.[21]

In *R v Vu*, the court ruled that personal computers were significantly different from file drawers or cupboards because they could "potentially give police access to vast amounts of information that users cannot control, that they may not even be aware of or may have chosen to discard and which may not be, in any meaningful sense, located in the place of the search."[22] As a result the court held that a general search warrant for premises was insufficient to allow a search of a computer found at that premise; a separate warrant for the contents of the computer was required given the incredible wealth of personal information any computer could potential contain.[23]

In *R v TELUS*, the Supreme Court held that the state's attempt to pre-emptively compel the production of future stored text messages temporarily stored by TELUS amounted to 'interception of private communications' despite the fact the information was not technically in transit. As a result, the state was required to meet the more restrictive requirements of wiretap authorization under Part VI of the *Criminal Code*, rather than the easier to fulfill general warrant authorization.[24] While the specific facts of this case may not repeat themselves, of much greater importance is the carefulness with which the court

[20] *R v Cole* 2012 SCC 53 at para 1, [2012] 3 S.C.R. 34 [*Cole*].
[21] *Cole, supra* note 20 at paras 57-59.
[22] *R v Vu*, 2013 SCC 60 at para 24, [2013] 3 SCR 657.
[23] *Ibid.*
[24] *R v TELUS Communications Co.*, 2013 SCC 16.

ensured that constitutional privacy protections were maintained despite unforeseen technological developments.

Most recently, in *R v Spencer* the court ruled that the police could not request Internet service providers link an IP address with a specific customer's account without a warrant.[25] The court unanimously rejected the argument that all that would be revealed would be an individual's name and address. Instead of looking at the 'name' and 'address' information in isolation, the Court held that it was important to examine "the connection between the police investigative technique and the privacy interest at stake."[26] In this case, the police were seeking subscriber information in order to identify a particular individual and link him to his online activities. The court expanded its understanding of informational privacy to include an interest in anonymity, and found that the states request to de-anonymize Spencer "engages a high level of informational privacy,"[27] and thus that a search triggering s.8 protections had taken place.

One exception to this trend must be noted. In *R v Fearon* the Supreme Court ruled that cellphones could be searched 'incident to an arrest' without a warrant. While this is certainly a limitation on Canadian's privacy, it is a fairly limited one. This warrantless search can only take place after a lawful arrest has been made, and only if it is truly 'incidental' to the arrest. The search may only be undertaken for one of three reasons: 1) protecting the police, the accused or the public, 2) to preserve evidence, or 3) because the investigation would be significantly hampered without a prompt search. In addition, the search must be narrowly tailored to its intended purpose and notes must be taken on what information was sought and why.[28] Restrictions notwithstanding, *Fearon* clearly grants the police an additional means by which Canadian's electronic information can be searched without a warrant. However, due the highly specific nature of the ruling, it is unlikely to have a wider impact on Canadian's constitutional protection of electronic information.

Finally, in *R v Wakeling*, the Supreme Court considered the application of s.8 of the *Charter* when Canadian authorities share information with US authorities.[29] Six of the seven justices agreed that s.8 was engaged when Canadian authorities shared lawfully obtained wiretap information with US authorities, but split on the question of whether the

---

[25] *R v Spencer*, 2014 SCC 43, [2014] 2 SCR 212 [*Spencer*].
[26] *Spencer* at para. 26.
[27] *Spencer* at para. 51.
[28] *R v Fearon*, 2014 SCC 77 at para 83, [2014] SCR 621.
[29] *R v Wakeling*, 2014 SCC 72, [2014] 3 S.C.R. 549.

sharing was reasonable in the circumstances. Justice McLachlin did not think that s.8 was engaged, because the information was being shared for law enforcement purposes – the same purpose for which it was obtained by Canadian authorities. However, her reasons leave open the possibility that s.8 could be engaged in cross-border information sharing contexts where the information is collected for one purpose and shared for a very different purpose.[30] The case is clear authority, therefore, for the proposition that cross-border information sharing attracts *Charter* scrutiny.

4.3 Who Is Protected?

While it is important to understand the different interpretations Canada and US courts have given to constitutional protections for electronic information, it is even more crucial to understand the jurisdictional limits of these protections. In general these protections extend only to activities undertaken by authorities within their own jurisdiction.

In the 2007 decision *R v Hape*, a case dealing with a warrantless search by Canadian agents in a foreign jurisdiction, the Supreme Court of Canada found that the key question was whether application of the *Charter* would have an objectionable extraterritorial effect. The majority found it would, stating that "[a]s a result of the principles of sovereign equality, non-intervention and comity, Canadian law and standards cannot apply to searches and seizures conducted in another state's territory."[31] As a result *Charter* search and seizure protections do not apply to actions undertaken in foreign jurisdictions.[32]

The majority did note that *Charter* protections regarding rights to a fair trial still apply when such extraterritorially obtained information is used in a Canadian court. However, this should be of limited comfort to Canadian's. *Hape* states that individuals should be expected to rely on the protections provided by foreign jurisdiction, even where these protections are lower than those offered Canadians on Canadian soil.[33]

---

[30] *Ibid* at paras 94- 95.
[31] *R v Hape*, 2007 SCC 26 at para 87, [2007] 2 SCR 292 [*Hape*].
[32]. *Hape, supra* note 31 at para 113 (The court did contemplate two exceptions to this general rule, but neither are likely to occur in cases involving Canadian's data).
[33] *Hape supra* note 31 at para 111.

After *Hape,* the key question is clearly what legal protections Canadians have for their electronic information in the United States. The answer is almost none. Since the 1990 US Supreme Court decision *United States v. Verdugo-Urquidez*, 4th amendment protections have been interpreted to apply only to those who are lawfully present in the United States, or who have some substantial connection to the United States, such as citizenship or permanent residency.[34] This means that Canadians who do not meet these requirements do not receive *any* constitutional protection for their electronic information when it is in the United States. For these Canadians the American government can access their information on whatever standards they legislate. To make matters worse, two critical pieces of legislation, the USA Patriot Act and the FISA 702 Amendment's specifically target non-US persons outside of the United States for a lower standard of protection.

5. US Statutes: The Non-US Person Issue and the Need to Move Beyond the USA PATRIOT Act

When comparing regimes, it is important to compare how Canadians (as non-US persons) are treated under US law with how Canadians are treated under Canadian law. If the comparison is between how Americans are treated under US law and how Canadians are treated under Canadian law then the wrong question is being asked. Furthermore, it is imperative to look beyond the USA Patriot Act and take into account both the 2008 *FISA Amendments Act* and the *Electronic Communications Privacy Act*.

5.1. Non-US Persons

A number of US statutes, including the USA Patriot Act, provide more protections for a "United States person" than to a non-US person. A "United States person" is defined to include US citizens, permanent residents, unincorporated associations that include a substantial number of US citizens and permanent residents, and corporations incorporated in the US.[35]

---

[34] Orin Kerr, "The Fourth Amendment and the Global Internet." (2014) 67 *Stanford Law Review* 285 at 292 (There is significant uncertainty in the correct interpretation of both 'lawfully present' and 'substantial connection as a result of the plurality opinion in *Verdugo* as well as conflicting lower court rulings).
[35] See 50 USC § 1801(i).

Under the USA Patriot Act, US persons receive a higher level of protection than non-US persons.[36] For example, under the Act a US person can only be investigated in cases involving international terrorism or clandestine intelligence activities. Furthermore, the investigation cannot be based on speech activities and is subject to minimization procedures. Non US-persons can be investigated not only for the same reasons but *also* to obtain "foreign intelligence information" and are not subject to speech and minimization protections. "Foreign intelligence information" is a very broad category of information and includes information that "relates to … the conduct of the foreign affairs of the United States."[37]

5.2 FISA 702

The *FISA Amendments Act of 2008* (FAA) amended the Foreign Intelligence Surveillance Act (FISA) and significantly expanded American authority to gather intelligence on non-US persons outside of the US borders.

From the perspective of Canadians, the most significant amendment was the addition of FISA section 702. In the words of the Privacy and Civil Liberties Oversight Board, "[s]ection 702 of FISA permits the Attorney General and the Director of National Intelligence to jointly authorize the (1) targeting of persons who are not United States persons, (2) who are reasonably believed to be located outside the United States, (3) with the compelled assistance of an electronic communication service provider, (4) in order to acquire foreign intelligence information."[38] This is the legal authority under which NSA operates its PRISM and Upstream programs.[39] It is important to underscore that 702 allows for the capture of *content* as well as the metadata associated with

[36] Section 215 of the USA PATRIOT Act amended the *Foreign Intelligence Surveillance Act* and is codified in 50 USC § 1861.
[37] See 50 USC § 1801(e).
[38] US, Privacy and Civil Liberties Oversight Board, *Report On The Surveillance Program Operated Pursuant To Section 702 Of The Foreign Intelligence Surveillance Act* (2014) at p. 20 [*PCLOB 702 Report*]. Specific provisions come from 50 U.S.C. § 1881a(a), (b)(3), (g)(2)(A)(vi).
[39] Laura Donohue, "Section 702 and the collection of international telephone and internet content." 38 Harv. J.L. & Pub. Pol'y..[Forthcoming in 2015].at 2, 11th February 2015 draft online: Georgetown Law Faculty Publications and Other Works <http://scholarship.law.georgetown.edu/facpub/1355> [Donoghue, "Section 702"].

internet communications. This includes emails, instant messages, internet phone conversations, and documents stored online.[40]

The introduction of FISA 702 marked a substantial change in intelligence practices, as previously under FISA only 'agents of a foreign' power could be targeted, not foreigners more generally.[41] The only major limitations to FISA 702's expansive power are that it cannot be used to target United States persons or those believed to be within the United States and that "a significant purpose of the acquisition is to obtain foreign intelligence information."[42] However, as foreign intelligence is defined the same way as in USA Patriot Act, it offers non-US persons very little protection.

Courts have a very limited role in overseeing the acquisition of this information. Not only are all proceedings heard only by the non-adversarial and classified FISA court (FISC), but the court's activities are limited to an annual certification of the procedures the NSA proposes to fulfill the statutory requirements. This means the court plays no role in authorizing individual targets or information gathering procedures.[43] More troubling still, the NSA has been accused of exceeding its authority under both the USA Patriot Act and FISA 702 authorities.[44] Considering many of these violations remained hidden for years, there are serious concerns about the FISC's ability to effectively oversee the NSA actions.[45]

After the FISC has certified the general procedures, that Attorney General (AG) and Director of National Intelligence (DNI) can authorize the targeting of any statutorily permitted individual. This targeting is done by choosing 'selectors' likely to give information relating to the target by searching for information to, from, or about

---

[40] *Ibid.*
[41] Donoghue, "Section 702", *supra* note 39 at 18 (technically the temporary Protect America Act was the first piece of legislation to make this change, however the FAA was the first to codify it in the long term).
[42] 50 U.S.C § 1881a(g)(2)(A)(v).
[43] Donoghue, "Section 702", *supra* note 39 at 22.
[44] See Donoghue, "Bulk metadata collection", *supra* note 13 at 806-821, Donoghue, "FISA 702", *supra* note 39 at 72-76; Jennifer Granick "New FISC Pen Register Opinion: It's Just a Matter of Time Before Somebody Gets Hurt" *Just Security* (21 November 2013), online: Just Security < http://justsecurity.org/3576/fisc-pen-register-opinion-its-matter-time-hurt/>; Cyrus Farivar, "Judge: 'NSA exceeded the scope of authorized acquisition continuously'"*ArsTechnica* (19 November 2013), online: Ars Technica <*http://arstechnica.com/tech-policy/2013/11/judge-nsa-exceeded-the-scope-of-authorized-acquisition-continuously/>.*
[45] Jennifer Granick "Don't Close Your Eyes to Surveillance Dangers: A Response to Richard Epstein" *Just Security* (29 January 2014), online: Just Security < http://justsecurity.org/6479/dont-close-eyes-surveillance-dangers-response-richard-epstein/>.

the chosen selector.[46] What selectors are appropriate is a topic of substantial controversy. The PCLOB report on the FAA offers examples of clearly permissible selectors (such as an email address or a phone number belonging to the target), and clearly impermissible ones (choices like the word 'bomb' or the name 'Osama Bin Ladin')[47] but provides no guidance as where the line is drawn within the extremes.

Selectors are then used in two different programs. Under the PRISM program the government sends the selector to a US based electronic communications provider that has previously been served a directive by the FBI informing them of their requirement to comply with NSA information requests. These providers are then compelled to share all information to or from the given selector, or risk being held in contempt of court.[48] For example, if the provider is Microsoft, the government may compel them to provide all emails sent to or from a 'selected' Hotmail address. If a company encrypts information stored on their servers to ensure consumer privacy, the government can compel the company to decrypt this information. FISA 702 overrides any contractual arrangements relating to privacy of information, and targeted companies are forbidden from informing costumers that their information has been the target of an NSA investigation.[49]

Under the Upstream program information is gathered directly from the 'backbone' of the internet by intercepting information as it travels. Use of this program is divided into two groups, telephone communication and Internet 'transaction'. Phone communication selectors work just like those chosen by PRISM, and are restricted to 'to' and 'from' collections, thus only communications to or from a number used by a targeted person will be collected. Internet information gathered under the Upstream program includes the use the very controversial 'about' selectors. These selectors gather information not just 'to' or 'from' the chosen selector, but also 'about' it, which means any mention of the chosen selector in the content of communications. [50]

A further controversial element of Upstream collection is the fact that it collects Internet 'transactions' rather than communications. Because information is 'packaged' together as it travels around the Internet the Upstream program frequently collects

---

[46] Donoghue, "Section 702"„ *supra* note 39 at 22.
[47] *PCLOB 702 Report, supra* note 38 at 33.
[48] *PCLOB 702 Report, supra* note 38 at 32-33.
[49] 50 U.S.C. § 1802(a)(4)(A).
[50] *PCLOB 702 Report, supra* note 38 at 35.

what are referred to 'multi-communication transaction'. These transactions include the communication with the relevant selector, as well as potentially large numbers of entirely unrelated communications. The NSA acquires and stores all of this information, subject to the appropriate minimization procedures.[51]

How much 'unintentional' data is caught up in NSA surveillance is a topic of ongoing concern, and one with no definitive answers. However, a Washington post analysis of over 160,000 communications collected by the NSA between 2009 and 2012 found that nine out of ten of the communications captured were not from the target of an NSA investigation, suggesting that concern on this front is justified.[52]

5.3 The Electronic Communications Privacy Act

Even less frequently mentioned in public discourse regarding outsourcing to the US is the *Stored Communication Act* (SCA), Title II of the *Electronic Communications Privacy Act* (EPCA). The EPCA was passed in 1986 to create statutory protections for electronic communications. These protections were deemed to be necessary because of the limitations of 4th Amendment protections for electronic communications created by the third party doctrine.[53] Unfortunately, the SCA is widely understood to be poorly drafted,[54] and has been the subject of sustained concern regarding the effectiveness of the privacy protection it provides.[55]

The SCA creates mechanisms for the compelled disclosure by electronic service providers of the contents of electronic communications. Two crucial distinctions

---

[51] *Section 702, supra* note 39 at 46.
[52] Barton Gellman, Julie Tate, & Ashkan Soltani "In NSA-intercepted data, those not targeted far outnumber the foreigners who are" *The Washington Post* (July 5, 2014). online: The Washington Post <http://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html.>.
[53] See Orin Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending it." (2004) 72 *George Washington Law Review* at 3-6.
[54] Orin Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending it." (2004) 72 George Washington Law Review at 1 [Kerr, *A User's Guide*].
[55] See Kerr, *A User's Guide, supra* note 54; Ilana Kattan, "Cloudy Privacy Protections: Why the Stored Communications Act Fails to Protect the Privacy of Communications Stored in the Cloud." (2010) 13 Vand. J. Ent. & Tech. L. 617 [Kattan]; Charles Kennedy, "ECPA for the 21st Century: The Present Reform Efforts and Beyond, An." (2011) 20 *CommLaw Conspectus* 129; and Dana Benedetti, "How Far Can the Government's Hand Reach inside Your Personal Inbox-Problems with the SCA." (2013) 30 *J. Marshall J. Info. Tech. & Privacy L.* 75.

regarding the type of service and the length of time a document is stored serve to substantially limit the protection the statute provides for electronic communication. The SCA differentiates between electronic communication services (ECS) and remote computing services (RCS). ECSs provide "the ability to send or receive wire or electronic communications,"[56] email being the obvious example of such a service. RCSs provide computer storage or processing services to public, online storage services such as Dropbox being a clear example. This distinction is hard to maintain in practice, as many email providers such as Hotmail or Gmail store emails on their servers indefinitely to allow individuals access to them at any time. Yet it is vital to the act, as RCS providers can be compelled to disclose content on substantially lower standards than ECS providers. Unfortunately, even services classified as ECSs are provided limited protections, as communications stored for greater than 180 days can be accessed on the same standards as if they were RCS.[57]

The Electronic Privacy Information Center provides this excellent table for understanding how email is treated under the ECPA[58]:

Type of Communication	Required for Law Enforcement Access	Statute
Email in Transit	Warrant	18 USC § 2516
Email in Storage on Home Computer	Warrant	4th Amendment, US Constitution
Email in Remote Storage, Opened	Subpoena	18 USC § 2703
Email in Remote Storage, Unopened, Stored for 180 days or less	Warrant	18 USC § 2703
Email in Remote Storage, Unopened, Stored for more than 180 days	Subpoena	18 USC § 2703

[56] USC *§* 2510(15).
[57] Kattan, *supra* note 55 at 629.
[58] Epic.org, "Electronic Communications Privacy Act (ECPA)" *Electronic Privacy Information Center*, online: EPIC <https://epic.org/privacy/ecpa/>.

Under the ECPA, remotely stored email can be accessed without a warrant once it is opened, and after 180 days if it remains unopened. The subpoena process involves a much lower standard than a warrant – the government only has to show that evidence that information sought is 'reasonably relevant' to a criminal investigation. The ECPA also permits compelled disclosure of subscriber information and some other forms of metadata with only a subpoena.[59] One limitation on ECPA subpoenas for content information is the planned use of the subpoena must be disclosed to the subscriber/customer before the subpoena is issued. However, the government can delay this notice by 90 days "upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result."[60] Worse still, it can renew the delay indefinitely, significantly limiting this protection.

One recent case relating the SCA has garnered a fair amount of attention. Its official name is *In re Warrant to Search Certain E-mail Account Controlled and Maintained by Microsoft Corporation*, but it also referred to as the 'Microsoft Ireland' case. The case began with the government seeking a warrant under the SCA that would compel Microsoft to provide (among other things) all emails associated with a specific account. Normally this would be straightforward request under the SCA, but in this case the information requested was stored electronically in Dublin, not in the United States. In December of 2013 a magistrate issued the warrant, and Microsoft moved to have the order quashed. A district court ruled in the government's favour, and the issue has now been appealed to the second circuit, where Microsoft, the government, and a large number of interveners have filed briefs.[61]

All parties concede that the government does not have power to issue a 'standard warrant'[62] that would apply extraterritorially. However, the magistrate ruled that a 'warrant' under the SCA is a hybrid between an administrative subpoena and a traditional warrant, requiring the level of proof of a traditional warrant, but operating like subpoena. The concerning thing about this ruling is that it sets a precedent for the extraterritorial application of American search and seizure power. If upheld all data

---

[59] 18 USC § 2703.

60 18 U.S.C. § 2705(a)(1)(B). Both "supervisory official" and "adverse result" are specifically defined terms for the purpose of delaying notice. See 18 U.S.C. § 2705(a)(2) (defining "adverse result"); 18 U.S.C. § 2705(a)(6) (defining "supervisory official").

[61] The list of amici includes: Apple, Amazon.com, Accenture PLC, AT&T, Verizon, Cisco, Hewlett-Packer, Ebay, Inc; the U.S. Chamber of Commerce and the National Association of Manufacturers; companies representing a range of media outlets, including ABC, Fox News, Forbes, The Guardian, McClatchy, NPR, and the Washington Post; the Irish government; the vice-chair of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs; computer and data science experts writing to clarify how the cloud operates; and non-profits. Links to the amici briefs are available: <http://digitalconstitution.com/about-the-case/>.

[62] A warrant under rule 41.

that American companies have access to, no matter in which jurisdiction it is stored, might be accessible to the US government. Indeed, concern over just such a possibility is clear in a letter written by the former European Union Justice Commissioner who warned that execution of the warrant might constitute a breach of international law.[63]

Orin Kerr has argued that even if the second circuit rules that a SCA 'warrant' cannot be applied extraterritorially, the government will still be able to achieve the same results through an administrative subpoena.[64] Unlike warrants, administrative subpoenas do have precedents for applying extraterritorially. In *Marc Rich* a district court held that a business must still provide its business records when given an administrative subpoena, even if those records are stored overseas.[65] However, in its brief to the second circuit, Microsoft argues that this application of administrative subpoenas has only been applied to a company's own records, not private information it holds on trust for costumers.[66] Kerr also noted that when subpoenas are applied overseas courts often apply a balancing test that could draw out litigation and act as significant check on the use of this power. Arguable the even more critical question is whether the search even took place outside of the US, since an American company was targeted and all of the actions required of it could be done from within US soil.[67] How the second circuit court (and possibly SCOTUS) rule on this issue will have a significant impact on the future privacy implications of dealing with American companies.

It is worth noting that there is currently proposed legislation that would prevent the extraterritorial application of the SCA.[68] At the same time, the Judicial Conference Advisory Committee on Criminal Rules has recommended a rule (to what is known as Rule 41) change in relation to warrants that would allow judges to grant warrants for remote searches of computers that are outside of their local jurisdiction.[69]

---

[63] Letter from Viviane Reding to Sophie in 't Vent (June 24, 2014), online: <http://www.nu.nl/files/nutech/Scan-Ares-MEP-in%27t-Veld-.pdf>.

[64] Orin Kerr, "What legal protections apply to e-mail stored outside the U.S.?" *The Washington Post* (7 July 2014), online: The Washington Post <http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/07/07/what-legal-protections-apply-to-e-mail-stored-outside-the-u-s/>.

[65] *In re Grand Jury Subpoena Directed to Marc Rich*, 707 F.2d 663 (2d Cir. 1983), and see In re Grand Jury Proceedings Bank of Nova Scotia,740 F.2d 817 (11th Cir. 1984) for the only similar ruling from an appellate court.

[66] *In re Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft*, no. 14-2985-CV (2d Cir. Mar. 9, 2014) (Factum of the Appellants at 36).

[67] Jennifer Daskal "The Un-Territoriality of Data" *Yale Law Journal* [Forthcoming 2015/2016], March 14 2015 draft online: SSRN: <http://ssrn.com/abstract=2578229>.

[68] Patrick Maines, "The LEADS Act and cloud computing" *The Hill* (30 March 2015), online: The Hill < http://thehill.com/blogs/pundits-blog/technology/237328-the-leads-act-and-cloud-computing>.

[69] Dustin Volz, "FBI's Plan to Expand Hacking Power Advances Despite Privacy Fears" *National Journal* (17 March 2015), online: <http://www.govexec.com/management/2015/03/fbis-plan-expand-hacking-power-advances-despite-privacy-fears/107712/>.

In addition to the Microsoft Ireland case, the SCA has been the subject of a number of 4th Amendment challenges, although none have yet been heard by the US Supreme Court. The leading appellate level decision, *Unites States v Warshak,* did find that compelled disclosure of emails on a standard lower than 'probable cause' violated the 4th Amendment.[70] However, this is of little comfort to Canadians who are not entitled to 4th Amendment protection for our communication data stored in the US. As long as the SCA remains valid law it remains another tool with which American authorities can access Canadian's electronic information on standards that are significantly lower than if the information resided within Canada, and on standards that would be unconstitutional within Canada.

5.4 EO 12333

The US also collects communications data under Executive Order 12333, which pertains to signals intelligence activities outside of the US. Because this report is primarily concerned with the situation of storing communications data within the US, EO 12333 is of limited relevance. However, to the extent that an institution's outsourcing contract permits a provider to send data to data centers located in other countries, then that data is vulnerable to being collected under EO 12333. This collection occurs without oversight from Congress or the FISC.

In July 2014, John Napier Tye, a former State Department official published an article in The Washington Post about the problems with EO 12333. He writes:

> Unlike Section 215, the executive order authorizes collection of the content of communications, not just metadata, even for U.S. persons. Such persons cannot be individually targeted under 12333 without a court order. However, if the contents of a U.S. person's communications are "incidentally" collected (an NSA term of art) in the course of a lawful overseas foreign intelligence investigation, then Section 2.3(c) of the executive order explicitly authorizes their retention. It does not require that the affected U.S. persons be suspected of wrongdoing and

[70] *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir, 2010).

> places no limits on the volume of communications by U.S. persons that may be collected and retained.[71]

Tye's focus is on the limited protection for US persons. However, non-US persons would receive less protection under EO 12333, as they would not be protected by the requirement that they can only be individually targeted with a court order or where their communications are collected incidental to a lawful foreign intelligence investigation.

5.6 Justifications for Differential Treatment

The President's Review Group, in its report on the NSA, defends the differential treatment of non-US persons. Although it argued that "[s]ignificant steps should be taken to protect the privacy of non-US persons",[72] the Review Group also defended the distinction between US and non-US persons found in FISA 702. According to the Review Group:

> To understand the legal distinction between United States persons and non-United States persons, it is important to recognize that the special protections that FISA affords United States persons grew directly out of a distinct and troubling era in American history. In that era, the United States government improperly and sometimes unlawfully targeted American citizens for surveillance in a pervasive and dangerous effort to manipulate domestic political activity in a manner that threatened to undermine the core processes of American democracy. As we have seen, that concern was the driving force behind the enactment of FISA.
>
> Against this background, FISA's especially strict limitations on government surveillance of United States persons reflects not only a respect for individual privacy, but also – and fundamentally – a deep concern about potential government abuse *within our own political system*. The special

[71] John Napier Tye, "Meet Executive Order 12333: The Reagan rule that lets the NSA spy on Americans" *The Washington Post* (18 July 2014), online: <http://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html>.

[72] US, The President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World*, (Princeton University Press 2013) at 19, online: The White House <https://www.nsa.gov/civil_liberties/_files/liberty_security_prgfinalreport.pdf>. [*Security in a Changing World*].

> protections for United States persons must therefore be understood as a crucial safeguard of democratic accountability and effective self-governance within the American political system. In light of that history and those concerns, there is good reason for every nation to enact *special* restrictions on government surveillance of those persons who participate directly in its own system of self-governance.[73]

There are several problems with this position. First, it suggests that there are no similarly serious problems with government abuse in relation to non-nationals. If the US experience is framed by its history and experience with the Church Commission, then Canadian experience is framed by its history and experience with the Arar Commission. Information about Canadian persons in the hands of foreign states can lead to serious human rights abuses. Canadians are particularly sensitive to the power of the US given our proximity to the US, the amount of travel that Canadians do to the US (for business and personal purposes), and the use of US airports as a transit stop en route to other destinations. Second, it ignores the fact that state surveillance is no longer merely a domestic matter but involves the widespread sharing of information between allies. Information about Canadian persons can be shared with other nations, which also raises questions about potential abuse. There are no proper transnational oversight capabilities for this information sharing. Third, when nations only extend strong protections to their own nationals, this actually provides the legal basis for widespread surveillance. If the US is allowed to collect non-US person information on a lower standard (and with no constitutional protections) and other countries are allowed to collect non-resident alien information on a lower standard, then given the "borderless" technology of the internet, everyone's communications information can be collected on a lower standard. If this raw data is then shared between allies what we have is the *enabling of global surveillance*, not the enabling of democracy.

6. Post-Snowden Developments

After the Snowden revelations there have been a number of responses by both the executive and legislative branches of the US government. This section will outline the most significant of these responses, with an emphasis on what effects they may have for non-US persons.

[73] *Ibid* at 153-4.

The first major response to the Snowden revelations was the formation of the President's Review Group on Intelligence and Communications Technologies, which released a report titled "Liberty and Security in a Changing World."[74] The report took a strong stance against mass collection of data, and specifically called for the end of the NSA phone metadata program authorized under 215 of the USA Patriot Act, in addition to recommendations for increased transparency, better protection for whistleblowers, and reforms to minimization procedures.[75]

The report was mixed in its treatment of non-US persons. Although mostly focused on US Persons, recommendation 13 called for two important changes to FISA. First, it recommend non-US persons who were *not* agents of a foreign power should only be allowed to be targeted for national security purposes, a much narrower requirement than the current 'significant foreign intelligence purpose.' Second, it recommended prohibiting the dissemination of any non-US person's information unless it related to national security purposes.[76] If adopted these changes would place important limits on the NSA, although they would not end 702 collections.[77]

On January 17th, 2014, shortly after the President's Review Group report was released, President Obama announced Presidential Policy Directive 28 (PPD-28), which combined with a long speech given on the same day outlined his proposed reforms to US intelligence gathering. Many of recommendation were in the form of broadly worded principles, leaving specific details to be worked out by congress and the relevant administrative agencies.[78] While the president was legally limited in what he

[74] *Ibid*
[75] Marty Lederman "Highlights of the Report of the President's Review Group on Intelligence and Communications Technologies" *Just Security* (December 22, 2013), online: Just Security <http://justsecurity.org/4903/highlights-prgict/>.
[76] Jennifer Granick "Foreigners and the Review Group Report: Part 2" *Just Security* (December 19, 2013), online: Just Security < http://justsecurity.org/4838/foreigners-review-group-report-part-2/>.
[77] Cindy Cohen and April Glass, "President's Review Group Puzzler: Why is Massively Overbroad Surveillance Wrong under 215 but OK under Section 702?" *Electronic Frontier Foundation* (January 10, 2014), online: Electronic Frontier Foundation <https://www.eff.org/deeplinks/2014/01/presidents-review-group-puzzler-why-mass-surveillance-wrong-under-215-ok-under>.
[78] Thomas Earnest "Overview of Proposals to Reform Signals Intelligence Programs in Today's Speech by the President" *Just Security* (January 17, 2014), online: Just Security <http://justsecurity.org/5885/proposals-reform-signals-intelligence-programs-todays-speech-president/>.

could enforceably demand, the directive fell well short of the type of reforms called for by the PCLOP report.[79]

Of the reforms in PPD-28, Section 4 is the most significant for non-US persons. It opens with the rather compelling statement that

> All persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and all persons have legitimate privacy interests in the handling of their personal information. U.S. signals intelligence activities must, therefore, include appropriate safeguards for the personal information of all individuals, regardless of the nationality of the individual to whom the information pertains or where that individual resides.[80]

However, the specific recommendations regarding non-US persons are quite limited. Of these, the most significant requirement is that the retention or dissemination of non-US person's information is only permissible if the same actions would be authorized for a US person's information under section 2.3 of Executive Order 12333. Unfortunately, the justifications for retaining and disseminating information under 12333 are extremely broad.[81] Information can be stored for a maximum of five years, unless a determination is made that the information is related to an authorized foreign intelligence purpose *or* the DNI determines it is the best interest of national security to maintain the information, in which case it may be stored indefinitely.[82] Similarly, information can be disseminated for a wide range of purposes, including "Information constituting foreign intelligence" and "Incidentally obtained information that may indicate involvement in activities that may violate federal, state, local or foreign laws."[83] While a recent report from Office of the Director of National Intelligence suggests that these changes are

[79] Benjamin Wittes, "The President's Speech and PPD-28: A Guide for the Perplexed" *Lawfare* (January 20, 2014), [Wittes "The President's Speech"] online: Lawfare <http://www.lawfareblog.com/2014/01/the-presidents-speech-and-ppd-28-a-guide-for-the-perplexed/#.Uvk7YnlYXnc>.
[80] Office of the Press Secretary, "Presidential Policy Directive/PPD-28" *The White House* (January 17th 2014). (footnotes removed) Online: The White House <https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities>.
[81] Wittes "The President's Speech" *supra* note 79.
[82] *Ibid.*
[83] Exec. Order 12,333, 3 C.F.R. 200 § 2.3 (b) and (i).

being implemented by US intelligence gathering agencies, it also indicates no broader changes with regards to non-US persons are being made.[84]

The most comprehensive information about US intelligence gathering to date comes from a pair of reports from the Privacy and Civil Liberties Oversight Board (PCLOB). The PCLOB is an independent agency of the executive branch created to review the intelligence gathering activities of the executive branch to ensure their efforts are balanced with privacy and liberty concerns.[85] Their first report released on January 23 2014 was focused on section 215 of the USA Patriot Act, and called for an end to mass collection of information.[86] The second, released on July 2nd 2014 was about intelligence gathering under FISA 702.[87] The report revealed in some detail how the NSA operated under FISA 702, but still left many significant questions about the NSA's operations unanswered.[88] The report also made ten recommendations about reforming FISA 702 and the FISA Court. While these recommendations would provide greater oversight for collection under FISA 702, they would still leave the fundamental architecture of the NSA surveillance power unchanged.[89] All told, this strongly suggests that non-US persons will have to look to legislative change for hope of more substantial protections.

Unfortunately as of the date of writing this report no legislative change to either the USA Patriot Act or the FISA 2008 Amendments has been passed,[90] despite a flood of bills providing a wide ranger of different reforms.[91] The bill that was the closest to becoming law, the USA FREEDOM Act, passed the house the House of Representatives, although was criticized for significantly for its watered down efforts at reform.[92] A

---

[84] Rainey Reitman "Obama Announces New Privacy Rules for the World. World Not Impressed." *Electronic Frontier Foundation* (February 10, 2015), online: Electronic Frontier Foundation <https://www.eff.org/deeplinks/2015/02/obama-announces-new-privacy-rules-world-world-not-impressed>.
[85] Privacy and Civil Liberties Oversight Board "About the Board," Online: PCLOB <https://www.pclob.gov/about-us.html>.
[86] Privacy and Civil Liberties Oversight Board *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court* (2014).
[87] Privacy and Civil Liberties Oversight Boad, *Report On The Surveillance Program Operated Pursuant To Section 702 Of The Foreign Intelligence Surveillance Act* (2014) at p. 20 [*PCLOB 702 Report*].
[88] Jennifer Grannick "Did PCLOB Answer My Eight Question about FISA 702" *Just Security* (July 2, 2014), online: Just Security <http://justsecurity.org/12516/pclob-answer-questions-section-702/>.
[89] *Ibid.*
[90] Nadia Kayyali, "Section 215 of the Patriot Act Expires in June. Is Congress Ready?" *Electronic Frontiers Foundation* (January 29, 2015), online: Electronic Frontier Foundation <https://www.eff.org/deeplinks/2015/01/section-215-patriot-act-expires-june-congress-ready>.
[91] Mark Jaycox, "EFF's Cheat Sheet to Congress' NSA Spying Bills" *Electronic Frontiers Foundation* (September 11, 2013), online: <https://www.eff.org/deeplinks/2013/08/effs-cheat-sheet>.
[92] Dan Roberts and Karen McVeigh "NSA surveillance reform bill passes House by 303 votes to 121" *The Guardian* (May 22, 2014), online: The Guardian <http://www.theguardian.com/world/2014/may/22/nsa-reform-bill-usa-freedom-act-passes-house>.

Senate version of the bill offering somewhat more substantial reforms failed to garner the 60 votes necessary to end debate and was defeated.[93] The bill was recently revived, and once again passed the house, and once again failed to pass the Senate. As a result of this inaction the deadline for re-authorization of three significant provisions of the USA Patriot Act (including the 215 powers) has passed, and those provisions have been rendered temporarily inoperative.[94] However, the USA FREEDOM Act has finally received the greater than 60 votes necessary to end debate and proceed to a final vote.[95] While the bill includes important protections for US citizens, such as ending the bulk collection of telephone metadata, it provides little substantive reforms to the surveillance of non-US persons.[96] It also worth noting that 2nd Circuit court recently ruled the bulk metadata collection under 215 illegal.[97]

A bi-partisan bill titled *The Surveillance Repeal Act* has been introduced that would not only completely repeal the USA Patriot Act and the 2008 FISA Amendments, but also introduce reform to the FISA Court and increase whistleblower protection has been introduced the House.[98] Unfortunately, it seems extremely unlikely to gain enough support to pass. As the FISA 702 amendments are authorized until December 31st 2017, non-US persons would be prudent assume that at least in the short term American authority to surveil them is unlikely to significantly change.[99]

---

[93] Spencer Akerman "Senate Republicans block USA Freedom Act surveillance reform bill" *The Guardian* (November 19th 2014), online: The Guardian <http://www.theguardian.com/us-news/2014/nov/18/usa-freedom-act-republicans-block-bill>.

[94] Mark Jaycox & Nadia Kayyali, "Section 215 Expires: For Now" Electronic Frontier Foundation (31 May 2015), online: Electronic Frontier Foundation <https://www.eff.org/deeplinks/2015/05/section-215-expires-now>.

[95] Dan Roberts et al. "NSA reform: Bush-era powers expire as US prepares to roll back surveillance" The Guardian (1 June 2015), online: The Guadian <http://www.theguardian.com/us-news/2015/may/31/nsa-reform-senate-deal-as-patriot-act>.

[96] Harley Geiger "Q & A on the USA FREEDOM Act" *Center for Democracy and Technology* (28 April 2015), online: CDT <https://cdt.org/blog/q-a-on-the-usa-freedom-act-of-2015/>.

[97] Charlie Savage & Jonathan Wiseman "N.S.A. Collection of Bulk Call Data Is Ruled Illegal" *The New York Times* (7 May 2015), online: The New York Times <http://www.nytimes.com/2015/05/08/us/nsa-phone-records-collection-ruled-illegal-by-appeals-court.html?_r=0>.

[98] Steven Nelson, "'Surveillance State Repeal' Push Resumes on Capitol Hill" *US News and World Report* (March 24 2015) online: US News and World Report <http://www.usnews.com/news/articles/2015/03/24/surveillance-state-repeal-push-resumes-on-capitol-hill>.

[99] FISA Amendments Act Reauthorization Act of 2012, Pub. L. No. 112-238, 126 Stat. 1631 (2012).

7. Rejecting The "Similar Risk" Analysis

This section compares the US and Canadian legal frameworks regarding lawful access to communications data. It does so by paying attention to what we have claimed is missing from the "similar risk" analysis: the constitutional question, a focus on how US law treats non-US persons, and attention to statutes other than the USA Patriot Act.

7.1 Access for Law Enforcement Purposes

The previous section outlined how email is treated under the *Electronic Communications Privacy Act* (ECPA), both in terms of access to content and access to metadata. This is not at all comparable to the legal framework in Canada. Within Canada it is clear that access to the content of email requires a warrant, as does access to subscriber information. Some forms of metadata can be accessed through new warrants and production orders that adopt a lower threshold of "reasonable suspicion". [100]

US	Canada
Can get access to subscriber information, or content of unopened stored communications after 180 days, without a warrant. Can get access to content of opened stored communications without a warrant.	Need a warrant for access to subscriber information or content of stored communications. Some forms of access to stored communications are treated like a wiretap, with more stringent protections.
Do not need a warrant for access to metadata. Standard for subpoena is "reasonably relevant."	Warrants and production orders for some types of metadata on basis of "reasonable suspicion" under new *Criminal Code* provisions.

7.2 Access for National Security/Intelligence Purposes

Previous sections have already outlined the terms under which US authorities are permitted to access non-US persons communications data under the USA Patriot Act and FISA. The relevant comparators in Canada are the *Canadian Security Intelligence*

[100] See Bill C-13, *Protecting Canadians from Online Crime Act*, which received Royal Assent 2014-12-09.

Service Act (CSIS Act), which regulates CSIS, and the *National Defence Act*, which regulates the CSE. Despite the ongoing debate about the USA Patriot Act at the time of the writing of this report, in this section we continue to use it as a basis for comparison. Even if it changes, it has been invoked in many Canadian privacy debates and has played a starring role in the "similar risk" analysis that it remains relevant to the comparison.

Under s.12 of the CSIS Act, CSIS is granted the authority to collect, analyze and retain information. This is limited in a number of ways by the language of s.12 itself: it can only do so "to the extent that it is strictly necessary" and the information must concern activities "that may on reasonable grounds be suspected of constituting threats to the security of Canada". "Threats to the security of Canada" are defined broadly in s.2 of the Act and includes espionage, sabotage, and a number of violent, covert and clandestine activities. However, it is not as broad as the "foreign intelligence information" definition that is used in FISA. CSIS also has intelligence-gathering authority granted under s.16 of the CSIS Act, but it is not permitted to exercise this in relation to Canadian citizens or permanent residents.

CSIS is subject to the *Charter*. Therefore if the activities CSIS undertakes intrude upon a reasonable expectation of privacy then it requires a warrant. The s.21 warrant provisions require reasonable grounds to believe "that a warrant … is required to enable the Service to investigate a threat to the security of Canada".[101] The Federal Court of Appeal has said that s.21 means that a judge issuing the warrant "is required to be satisfied, on reasonable and probable grounds established by sworn evidence, that a threat to the security of Canada exists and that a warrant is required to enable its investigation."[102] In addition, s.21 requires CSIS to show "that other investigative procedures have been tried and have failed" or that there is some special urgency.[103]

US: USA Patriot Act 215	Canada: CSIS Act
Compelled collection where reasonable grounds to believe "relevant" for an investigation to obtain	Compelled collection where reasonable grounds to believe "required" to investigate a

[101] *Canadian Security Intelligence Service Act*, RSC 1985, c C-23, s.21(1), 21(2)(a) [CSIS Act].
[102] *Atwal v Canada*, [1987] 2 FC 309 at para. 36.
[103] CSIS Act, supra note 101, s. 21(2)(b).

"foreign intelligence information" not about a US person "protect against international terrorism or clandestine intelligence activities"	"threat to the security of Canada"
	Have to show that other investigative techniques have/will fail, or there is urgency, or there is likely no other way to obtain this information.
Compelled nondisclosure of order.	Possible nondisclosure of order.

Under the *National Defence Act*, one of the mandates of the CSE is "to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence" but this activity "shall not be directed at Canadians or any person in Canada".[104] There has been significant controversy over the question of what is means to "direct" activities at Canadians. The CSE has a metadata collection program and there is evidence that Canadian information has been collected "incidental" to this. In the US there is compelled assistance from service providers. The *National Defence Act* does not have provisions for this. There is evidence of voluntary cooperation on the part of telecommunications companies in Canada, although this involved the sharing of subscriber information prior to the Supreme Court of Canada's decision in *R v Spencer*, which held that such warrantless access was unconstitutional.

Under the *National Defence Act*, the Minister can authorize the interception of "private communications" for the "sole" purpose of obtaining foreign intelligence information. Private communications are those where either the sender or recipient is in Canada. This has to be directed at foreign entities located outside of Canada, the information cannot be reasonably obtained in any other way, the foreign intelligence value must justify its collection, and there must be satisfactory measures to protect the privacy of Canadians. These measure are meant to shield CSE from *Criminal Code* liability for their unintentional collection of private communications. However, it contemplates the incidental collection of Canadian communications. This is still more restrictive than the powers granted to US authorities under FISA 702 in relation to non-US persons.

[104] *National Defence Act*, RSC 1985, c N-5, s.273.64.

US: FISA 702	Canada: *National Defence Act*
Broad warrantless authorization to target non-US persons located outside of the US to collect "foreign intelligence information"	Broad warrantless authorization to acquire foreign intelligence information but CSE is prohibited from targeting Canadians or persons within Canada.
Collection of content and metadata of communications.	"Incidental" collection of metadata.
	Where minister authorizes interception of private communications, cannot direct at Canadians, can only do so when information cannot be obtained in another way, foreign intelligence value must justify interception, measures must be in place to protect privacy of Canadians.
Compelled assistance from electronic service providers.	Possible voluntary assistance from electronic service providers.

7.3 Information Sharing

The "similar risk" analysis also points to "longstanding formal bilateral agreements" between the US and Canada which allow for cooperation and information sharing. Indeed, under the *US-Canada Mutual Assistance Treaty* (MAT),the US government can require Canadian officials to help obtain information even if that information is stored within Canada.[105] The argument seems to be that since the US government can obtain information through the MAT anyway, it does not matter whether the information is stored within the US or within Canada. However, this seriously overlooks several key aspects of the Treaty. For example, Article XVI, section1, indicates that "[a] request for search and seizure shall be executed *in accordance with the requirements of the law of the Requested State*"; Article VII, section 2, states that "[a] request shall we executed *in accordance with the law of the Requested State* and, to the extent not prohibited by the law of the Requested State, in accordance with the directions stated in

[105] Treaty Between the Government of Canada and the Government of the United States of America on Mutual Legal Assistance in Criminal Matters, 18 March 1985, CTS 1990 No 19.

the request"; and Article V, section 1(b), states that the Requested State may deny assistance to the extent that "execution of the request is contrary to its public interest". In other words, when Canada cooperates with the US under the MAT, it is Canadian law that governs the exchange.

8. Legal vs. Practical Risks

The forgoing critique of the "similar risk" analysis focuses on legal risk. There is also the question of practical risk. For example, one could argue that even though Canadian law is more protective of Canadians than US law there is still the risk that Canadian authorities are operating in violation of Canadian law. Given the weak oversight of Canadian spy agencies this is a practical risk. However, it would be striking for a public institution to make a decision based upon the argument that the practical risk of Canadian agencies acting illegally nullifies Canadian legal privacy protection. Such a claim accepts the proposition that Canadian agencies are likely acting illegally and accepts this with little actual evidence.

Another potential argument is that because Canada is a member of the Five Eyes and the Five Eyes have "no-spy" agreements that prohibit each country from spying on the other that this means that the US will not engage in surveillance against Canadians. Therefore although there is a legal risk, given the statutory authority to engage in such surveillance, there is little practical risk. There is some evidence that the US applies some of its post-collection minimization safeguards to information associated with Five Eyes persons the same way it would to US persons.[106] However, the *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, documents the targeting procedures used to determine whether someone is reasonably believed to be a non-US person located outside of the US but never mentions any process for determining whether someone is a non-US person located outside of the US and a citizen of a Five Eyes country so it is unclear whether this also occurs with US domestic use of information collected under US domestic authorities like FISA 702.[107] At the same time, the US has been adamant that it has no such formal agreements. A report by the Presidents Review Group explicitly states that "the United States has not entered

[106] "NSA and Israeli intelligence: memorandum of understanding – full document" *The Guardian* (11 September 2013), online: <http://www.theguardian.com/world/interactive/2013/sep/11/nsa-israel-intelligence-memorandum-understanding-document>; "Communication breakdown" *The Washington Post*, online: <http://apps.washingtonpost.com/g/page/world/communication-breakdown/1153/>.
[107] PCLOB 702 Report, *supra* note 38.

into formal agreements with other nations not to collect information on each others' citizens."[108] If there are informal arrangements, these are not legally binding. Nor should they be understood to be rights-protective. The US could waive any such arrangements when its national interests called for this and Canada too might want the US to spy on Canadians of interest – allowing US authorities to do what Canadian authorities are prohibited from doing.

There are additional questions that need to be asked in relation to the Five Eyes. For example, in the 2013-2014 Annual Report of the Communications Security Establishment Commissioner, Commissioner Plouffe states that "[t]he allies recognize each other's sovereignty and respect each other's laws by pledging not to target one another's communications."[109] It is easy to see how this applies when dealing with the collection of communications in a foreign territory. If the US, under its EO 12333 authority, were to collect communications *within* Canada, then this would be in violation of Canadian law and Canada's sovereignty. However, it is not clear that this same reasoning applies to the kind of case contemplated by FISA 702 – where the US collects communications data within its own territory. To do so neither interferences with the sovereignty of another state nor disrespects their laws.

In the report, Plouffe made several recommendations concerning information sharing with international partners:

> I recommend that the Minister of National Defence issue a new directive to CSEC on information sharing activities with its second party partners in the United States, the United Kingdom, Australia and New Zealand (that is, second party partners are CSEC's counterparts in the Five Eyes alliance), to clearly set out expectations for the protection of the privacy of Canadians. I recommended that CSEC promulgate guidance to formalize and strengthen practices for addressing potential privacy concerns involving second party partners. I also recommended that CSEC record second party partners' confirmation that they have actioned CSEC requests to address any privacy incidents relating to a Canadian.[110]

---

[108] *Security in a Changing World*, *supra* note 72
[109] Canada, Communications Security Establishment Commissioner, *Annual Report 2013-2014* (Ottawa: Minister of Public Works and Government Services Canada 2014) at 25.
[110] *Ibid* at 15.

In addition, Commissioner Plouffe reported on the second part of former Commissioner Decary's review of CSE's information sharing with international partners. The first part of the review looked at CSE's information sharing and was discussed in the 2011-2012 annual report. The second part of the review asked about how CSEC assures itself that its international partners are following their agreements and practices, and also about the amount of private communications and information about Canadians that CSE shares with its partners and that they share with it.[111] Former Commissioner Decary was unable to determine whether CSE's second party partners (the Five Eyes) were following their agreements regarding Canadian privacy since CSE "does not as a matter of general practice seek evidence to demonstrate that these principles are in fact being followed."[112] Because of this, former Commissioner Decary recommended that the Minister of National Defence issue a new ministerial directive concerning information sharing activities and this be "informed by an in-depth analysis of the potential impact of respective national differences in legal and policy authorities on CSEC compliance with the law and the protection of the privacy of Canadians, that is, a risk assessment."[113] Although CSEC has since provided the Commissioner's office with more detailed documentation regarding its second party partners policies and procedures, Commissioner Plouffe concluded that "in light of recent controversies in some second party countries, including about alleged domestic spying by their foreign signals intelligence agencies, I remain in agreement with Commissioner Decary that a risk assessment is essential."[114]

Another issue discussed by Commissioner Plouffe is that "[t]he unintentional interception of a private communication by CSE is a different situation than the unintentional acquisition by CSE from a second party source of a one-end Canadian communication."[115] With respect to the first, CSE can seek ministerial authorization in respect of activities that risk such unintentional interception, which must meet a number of specified criteria. However, when CSE acquires the same type of information from second party sources it is not bound by these requirements. According to Commissioner Plouffe, such sharing is implicitly authorized under CSE's mandate "to acquire and use information from the global information infrastructure for the purpose

[111] *Ibid* at 24.
[112] *Ibid* at 26.
[113] *Ibid*.
[114] *Ibid* at 27.
[115] *Ibid* at 28.

of providing foreign intelligence, in accordance with Government of Canada intelligence priorities." (S.273.64(1)(a)). Because of this, "CSEC has not reported to the Minister of National Defence details, for example, regarding communications involving Canadians or information about Canadians that have been shared by its second party partners."[116] Commissioner Decary recommended that such reporting be done on an annual basis.

From this we should conclude that there are serious questions regarding Canada's information sharing arrangements with the US, including questions about its scope, the degree to which Canadian privacy is protected, and what kind of review mechanisms exist. It is notable that two Commissioners have called for a risk assessment and think that the risk assessment needs to include an examination of national legal differences.

9. Appendices

Appendix A: FIPPA Obligations

In Ontario, Universities are subject to Ontario's *Freedom of Information and the Protection of Privacy Act* (FIPPA).[117] When outsourcing, a University remains responsible for its obligations under FIPPA.

Disclosure Obligations

It is the University who is responsible for any disclosure that is prohibited by FIPPA. Any permitted disclosure to law enforcement or national security agencies is fully governed by s.42.

Section 42 allows for disclosure with consent. Suppose that the end-user agreement includes language to the effect that the provider may disclose information for law enforcement or national security purposes? This would not be adequate consent for the purposes of s.42(1)(b), for that provision requires that "the person to whom the information related has identified that information in particular". Vague and open-

[116] *Ibid* at 29.
[117] RSO 1990, c F-31, s 61.

ended language indicating possible disclosure of some undefined information does not satisfy this requirement.

Section 42(1)(g) permits disclosure to "an institution or a law enforcement agency in Canada to aid an investigation undertaken with a view to a law enforcement proceeding". This provision does not authorize disclosure to a *foreign* institution or law enforcement agency, nor does it authorize disclosure in circumstances where the information is for intelligence purposes rather than law enforcement. The only reference to foreign law enforcement agencies is in s. 42(1)(f)(i), which permits "a law enforcement institution" to disclose information "to a law enforcement agency in a foreign country under an arrangement, a written agreement or treaty or legislation authority". Therefore under FIPPA the only acceptable pathway for disclosure to a foreign agency is for the University to disclose to a *Canadian* law enforcement agency who can then disclose it to a foreign law enforcement agency under the terms of s. 42(1)(f)(i).

Disclosures by Universities to foreign law enforcement and national security agencies are therefore prohibited under FIPPA and the University remains responsible for any such disclosures.

What information is the University responsible for?

Some Universities have taken the position that they are only responsible for a small subset of personal information involved in their outsourcing arrangements. The argument seems to be that the University is only collecting, using and disclosing information such as student identification number for the purposes of authentication. After that, the information relationship is between the end user (e.g. the student) and the provider.

This argument should be rejected. When the University provides a university email account then it is providing email to its students (or faculty or staff). Indeed, most often these email accounts are the official channel of communication between the University and its students (or faculty or staff). If the University was providing this email service itself then it would be clearly be involved in collecting, using, disclosing, and storing all of the information associated with this communications system –

including the content and metadata associated with the communications of users. By outsourcing, the University cannot relinquish its obligations in relation to this information.

The collection requirements of FIPPA include the requirement, in s.39(1), that an institution collect personal information "directly" from individuals unless the collection falls within one of the exemptions (s.39(1)). This section does not mean that an institution is not responsible for information unless the institution itself collects it directly. Such a conclusion is inconsistent with other parts of the Act, such as the use and disclosure obligations which refer to personal information in the custody or under the control of an institution (ss. 41, 42). It is also inconsistent with one of the purposes of the Act, which is "to protect the privacy of individual with respect to personal information about themselves held by institutions and to provide individuals with a right of access to that information." (s.1) A University cannot claim that personal information is not being "held" by the institution or is not under its "custody" or "control" because it has entered into a contract for a third party to handle this information.

Moreover, the personal information associated with communications is personal information that is being collected, used and disclosed by the provider and as such would bring the *provider* within the scope of PIPEDA. The fact that much of this personal information is provided by the end-user in their interactions with parties other than the provider does not take this information out of the scope of PIPEDA. This is clear from the OPC decision regarding Facebook.[118] There, user-generated content had an impact on how obligations under PIPEDA were interpreted (e.g. the form that consent takes) but had no impact on whether user-generated content was considered personal information regulated under PIPEDA. It would be strange to hold that an organization that is clearly regulated by PIPEDA (Microsoft, Google) becomes exempt from its PIPEDA obligations because it is in a contractual relationship with an institution that is not regulated by PIPEDA, especially since under this contractual relationship the provider still enters into individual agreements with end-users.

---

[118] Elizabeth Denham, Assistant Privacy Commissioner of Canada, *Report of Findings Into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPC) against Facebook Inc. Under the Personal Information Protection and Electronic Documents Act* (16 July 2009), 2009-008, online: OPC https://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.asp.>

Appendix B: PIPEDA Obligations

Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA) applies to the personal information that an "organization collects, uses or discloses in the course of commercial activities" (s.4(1)(a)).[119] The Office of the Privacy Commissioner of Canada takes the position that the MUSH sector (Municipalities, Universities, Schools, and Hospitals) is not subject to PIPEDA.[120] However, third parties that a University contracts with would be subject to PIPEDA.

Under principle 4.1.3 of Schedule 1 in PIPEDA:

> An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

In the context of outsourcing to the US, contractual measures cannot protect against lawful access requests under US law. This is why the main analysis regarding extra-national outsourcing has focused on the issue of similar legal risk: if contract cannot protect against the legal risk of lawful access in the US, outsourcing is only acceptable if there is a comparable legal risk of lawful access in Canada.

PIPEDA also imposes consent requirements. Section 7(1) provides that an organization can only collect personal information without the knowledge or consent of an individual if it falls within one of the specified statutory exceptions to consent. None of these exceptions apply in the eCommunications context. Given the fact that extra-national outsourcing involves Canadian citizens and residents giving up their constitutional privacy protections (because, as described in the main body of this report, neither Canadian nor US constitutional protections apply in such a scenario), such consent requirements should be as exacting as the requirements for a constitutional waiver.

---

[119] SC 2000, c 5.

[120] Office of the Privacy Commissioner of Canada, "Fact Sheets: Municipalities, Universities, Schools, and Hospitals" (12 December 2012), online: OPC <https://www.priv.gc.ca/resource/fs-fi/02_05_d_25_e.asp>.

Moreover, section 5(3) of PIPEDA provides: "[a] organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances." It is difficult to see how a third party provider who discloses personal information to US authorities pursuant to a FISA 702 order, for example, does so for a reasonable purpose. Such disclosure happens outside of the protections of any constitutional law (Canadian or US); as this report outlines, the US authority for this disclosure conflicts with Canadian constitutional law; and this would be a prohibited disclosure under FIPPA if the University were to be asked directly. Interpreting PIPEDA to permit this type of disclosure allows organizations to do an end-run around both Canadian constitutional law and Canadian public sector privacy laws.

Appendix C: Statutory Prohibitions and Blocking Strategies

There are two legislative strategies that some Canadian provinces have taken in response to the threat of foreign demands for data: prohibitions on outsourcing and blocking of compliance with foreign demands. This appendix briefly discusses both strategies in relation to Canadian public sector privacy laws.

Where there are prohibitions on outsourcing, there are also exceptions, the most important of which is individual consent. There are many problems with ensuring that individual consent in such contexts is truly informed. This is discussed further below.

The blocking strategy is meant to apply to the situation where data is kept within Canada but still might be subject to a foreign demand for disclosure, for example when US jurisdiction is asserted over a Canadian subsidiary of a US company. This is discussed further below.

A. Prohibitions on Outsourcing and the Consent Exception

Two provinces, British Columbia and Nova Scotia, have public sector privacy statutes that prohibit the storage of data outside Canada unless it falls within the terms of statutory exceptions.

Section 30.1 of British Columbia's *Freedom of Information and Protection of Privacy Act*[121] provides: "[a]public body must ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada" unless it falls within one of three exceptions. Two of these exceptions refer to permitted disclosures under the Act (ss. 30.1 (b) and (c)) and the other exception is where an individual has consented to the storage and access.

Similarly, Section 5(1) of Nova Scotia's *Personal Information International Disclosure Protection Act*[122] [PIIDPA] provides:

> A public body shall ensure that personal information in its custody or under its control and a service provider or associate of a service provider shall ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada

[121] RSBC 1996, c 165.
[122] SNS 2006, c 3.

There are several exceptions, including where individuals consent (s.5(1)(a)), where the storage or access is for a permitted disclosure (s. 5(1)(b)), and where the "head of the public body" permits it because it is "necessary" for the functioning of that body (s.5(1)(c)).

Despite being subject to PIIDPA, Dalhousie University decided to outsource its eCommunications to Microsoft Office 365. If one goes to Dalhousie University's information site for Microsoft Office 365, information on "Privacy & Security" is found under the heading of "Support" instead of "Getting Started" or somewhere else more prominent.[123] The first statement under "Support" pertains to cloud storage: "Office 365 is a cloud-based service, meaning the application and data are hosted on a network of servers around the world to ensure continuity and quality of service."[124] There is no information regarding what this means in terms of legal jurisdiction. The site also states: "The Personal Information International Disclosure act [sic] allows the university to store information outside of Canada if certain requirements are met. Dalhousie has complied with those requirements."[125] It does not provide details regarding these requirements or Dalhousie's compliance, nor does it indicate how a user might find out more about these details.

There are two likely exceptions Dalhousie may be relying on, necessity (9(2)(c)) or consent (9(2)(b)). It is difficult to see how eCommunications outsourcing is "necessary" for a University, such that the head of the public body could permit it. It is most likely that Dalhousie's compliance with PIIDPA rests on individual consent. However, we could not confirm this as Dalhousie did not respond to our request for its PIA.

To secure truly informed consent in the context of outsourcing, individuals would need to be informed that a) their data will reside outside of Canada, b) it will be subject to foreign laws, c) these laws are less privacy-protective than Canadian laws, d) they lose constitutional privacy protection. It is highly unlikely that the notice being given to individuals includes such comprehensive information.

B. Blocking Compliance with Foreign Orders

[123] Dalhousie University, "Microsoft Office 365-PRIVACY & SECURITY", online: Dalhousie University <http://www.dal.ca/dept/its/o365/support/privacy-security.html>..
[124] *Ibid.*
[125] *Ibid.*

Just because data remains geographically within Canada does not mean it is outside of the reach of US jurisdiction. The US can exert its jurisdiction over organizations within Canada, although doing so can raise questions of interference with Canadian sovereignty. The risk of such extraterritorial reach is often thought to be strongest in the case of a Canadian subsidiary of a US company. However, as discussed in s.5.3 of this report, the Microsoft Ireland case indicates that Internet companies are contesting the reach of US law to their datacenters outside of US territory.

One strategy to deal with this potential reach of US jurisdiction is to pass a 'blocking statute' that blocks compliance with the foreign order. Such statutes make it clear that it is legally impossible for companies operating within Canada to comply with both US and Canadian law, and impose penalties for companies that do comply with US orders. Furthermore, these blocking statutes can then be an important factor in a US court's determination of whether to order disclosure from companies operating in Canadian jurisdiction.. [126]

Alberta amended its public sector *Freedom of Information and Protection of Privacy Act*[127] to block compliance with foreign disclosure orders. Section 92(3) provides:

> A person must not wilfully disclose personal information to which this Act applies pursuant to a subpoena, warrant or order issued or made by a court, person or body having no jurisdiction in Alberta to compel the production of information or pursuant to a rule of court that is not binding in Alberta.

This does not prevent foreign authorities from seeking the cooperation of Canadian authorities in obtaining information under the control of public bodies, but it does mean that such cooperation will occur under the terms of Canadian law.

British Columbia's *Freedom of Information and Protection of Privacy Act* also includes some provisions that creating a blocking effect. Disclosing information to foreign authorities is considered an unauthorized disclosure and constitutes an offence under the Act, as does the failure to report a foreign demand for disclosure.[128]

[126] For a longer discussion of blocking statutes, see Michael Geist and Milana Homsi, "Outsourcing our Privacy?: Privacy and Security in a Borderless Commercial World" (2005) University of New Brunswick Law Journal 272.
[127] RSA 2000, c F-25.
[128] *Supra* note 121, s 74.1.

It should be noted that there is no authorized disclosure to foreign authorities under Ontario's *Freedom of Information and Protection of Privacy Act* (see Appendix A) and that "wilfully" disclosing personal information in contravention of the Act is an offence.[129] The practical difference between this and Alberta's Act seems to be the amount of the potential penalty. In Alberta, an individual can be liable to a fine between $2000 and $10000 and any other person, such as a corporation, to a fine between $200 000 and $500 000. In Ontario the maximum fine for any individual or corporation is $5000. In addition, as outlined in Appendix B, it is possible that disclosure to foreign authorities under PIPEDA is not "reasonable" under section 5(3) of the Act.

[129] *Supra* note 117.