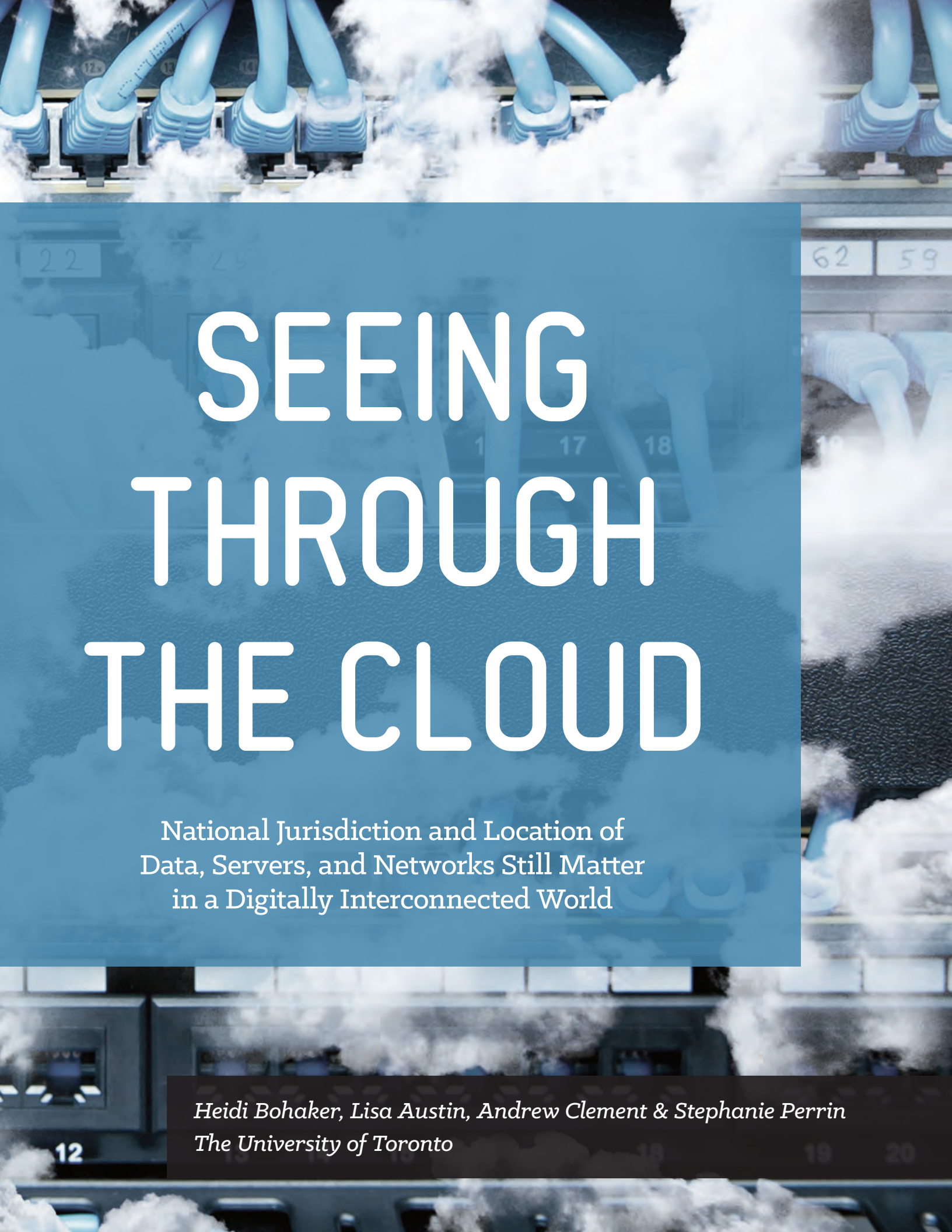

SEEING THROUGH THE CLOUD

National Jurisdiction and Location of Data, Servers, and Networks Still Matter in a Digitally Interconnected World

Heidi Bohaker, Lisa Austin, Andrew Clement & Stephanie Perrin
The University of Toronto

ACKNOWLEDGEMENTS

The production of this report has been supported by a grant from the Office of the Privacy Commissioner of Canada through the 2014–2015 Contributions Program. We are very grateful for this support. The argument and interpretation expressed in this report are those of the authors, and do not purport to represent the views of the Office of the Privacy Commissioner.

We would also like to acknowledge the support of the University of Toronto. Specifically, the Faculty of Information is hosting our website (ECOMMOUTSOURCING.ISCHOOL.UTORONTO.CA) and provided the space for the public forum we held on March 6, 2015. The Faculty of Arts and Science Information and Instructional Technology department provided both technical assistance and secure document storage. Research Services and our departmental and faculty research officers and administration staff provided operational assistance. This support reflects the University of Toronto's ongoing commitment to faculty research and academic freedom; however the findings of the report should not be taken to reflect an official position of the University itself.

We received additional feedback on our findings from participants at the March 6 forum, both at the event itself and in response to draft versions of this report. We are very grateful for this feedback. Any errors remain the responsibility of the authors.

Finally, we thank our talented contributing researchers: Ms. Andi Argast, Mr. Daniel Carens-Nedelsky, Ms. Susan Colbourn, Dr. John Dirks, Dr. Jonathan Obar, Ms. Dawn Walker, current and former graduate students and postdoctoral fellows in Law, History and Information at the University of Toronto. Co-authors of specific detailed reports are listed in the appendices.

Cover design by Jennette Weber. Cover photography courtesy of © iStock.com/troyek and © iStock.com/ranplett.

Table of Contents

This page intentionally left blank.

Seeing Through the Cloud: National Jurisdiction and Location of Data, Servers, and Networks Still Matter in a Digitally Interconnected World

Heidi Bohaker, Lisa Austin, Andrew Clement and Stephanie Perrin.

Executive Summary

Moving to the Cloud? Many Canadian organizations are doing so, contracting with third party vendors to provide a wide range of digital services over the global Internet.

"Moving to the Cloud" really means creating content and storing the digital archives of information produced—including confidential, proprietary and deeply personal information—outside of your organization's physical control, on someone else's computers, somewhere else in the world.

In the short term, such extra-national outsourcing may appear to make financial sense, especially for those in the education sector who can access these services for little to no cost, at least for a limited period of time. But what are the broader and longer-term consequences of doing so?

The authors of this report undertook a year-long study to investigate the privacy implications of using services hosted in the global cloud where the data at issue would be stored or processed in another nation's jurisdiction, regardless of whether it was encrypted or not.[1] As academics from the humanities, law, and information studies, we were drawn to this question following Edward Snowden's 2013 release of documents which revealed the sweeping extent of domestic state surveillance activities by the United States, especially those targeting "non-US" persons. We could not reconcile this information with claims that data faced a "similar risk" from such surveillance regardless of where in the world it was stored or processed.

In our research, we examined relevant statutes, constitutional doctrine, and other case law in Canada and the USA, investigated the history of transborder data flows and current North America Internet traffic patterns, and studied decisions by Canada's major public universities to use Google Apps for Education or Microsoft Office 365,

[1] Our research was funded by Canada's Office of the Privacy Commissioner's Contributions Program, 2014-2015. This document is the executive summary for our public report. Detailed research reports are listed as appendices at the end of the public report and are also available for download as pdf files from our project website: http://ecommoutsourcing.ischool.utoronto.ca/.

suites of eCommunications and collaboration software (which includes email, messaging, telephony, video-conferencing and document creation, editing and storage).

Such systems are particularly sensitive with respect to privacy concerns because they are archives of conversations and ideas that are internal to organizations, such as intellectual property, strategic planning, confidential employee medical and performance issues and research and development data. These digital archives also contain *metadata*, or data about content, the "to" and "from" of a message and dates of creation and modification that themselves reveal significant personal information.

Based on our research, we found that for sensitive digital data **national jurisdiction matters: where in the world your data is located affects which third parties can legally access it, and on what terms.** Governments around the world can and do legally access digital data; the important question is *access on what standards*? When Canadians store their data, for example, in the United States, their data can be accessed by United States government authorities on standards that would be unconstitutional if applied within Canada. Nor can Canadians expect that United States constitutional standards will apply to them. Furthermore, specific US legislation explicitly provides a lower level of privacy protection to the digital data of non-US persons.[2]

Canadians and Canadian organizations have significantly better legal privacy protection from state surveillance when their data are processed, stored, routed or more generally kept exclusively within Canadian jurisdiction than elsewhere. This protection extends to valuable intellectual property which is also vulnerable to industrial espionage from state surveillance in foreign jurisdictions. Canadians have significantly more options to address data protection concerns through their own courts, legal reform and the electoral process.

Organizations should plan their use of externally-hosted services carefully, based upon a thorough analysis of the data to be processed or stored extra-nationally. For content that is intended for sale or dissemination globally (for example, movies, books, music) or for records whose data classification is "public," the use of globally-provisioned cloud-based hosted services may be an appropriate choice.

However, for data classified as personal, confidential or otherwise sensitive, moving to the global Cloud requires Canadians or those living in Canada to forfeit their rights and

[2] For the full legal report, see Lisa Austin and Daniel Carens-Nedelsky, "Why Jurisdiction Still Matters," available as a pdf file at http://ecommoutsourcing.ischool.utoronto.ca/.

protections as citizens and residents—particularly their constitutional protections—in the name of potential savings that may be realized from extra-national outsourcing. The expectation of privacy in law is not only a human right; the Supreme Court of Canada has repeatedly affirmed that it is also necessary to preserve a free and democratic society. Control over one's personal information is required to maintain individual autonomy and dignity which are crucial social values; by restricting the right of the government to pry into the lives of its citizens, democracies protect fundamental freedoms.

Based on the findings of our research, we strongly recommend that:

1. Canadian organizations should not outsource eCommunications services beyond Canadian jurisdiction until adequate measures for ensuring legal and constitutional protections equivalent to those in Canada are in place.
2. When considering eCommunications options, including outsourcing, organizations should conduct thorough and transparent Privacy Impact Assessments (PIAs) and Threat Risk Assessments (TRAs), taking into account constitutional and other protections provided under Canadian law, as well as the risks of using services hosted in foreign jurisdictions. The "similar risk" assertion should no longer be used in PIAs to support extra-national outsourcing.
3. Organizations that have already outsourced to companies that place data outside Canadian jurisdiction should revisit these decisions in light of the deeply flawed "similar risk" assertion and what is now known about, for example, mass surveillance practices in the USA. Organizations should consider the risk of similar practices occurring in other countries.

There is an urgent need in Canada for a combination of technical, policy and legal expertise to conduct further research in this area and to develop new regulatory and IT solutions in order to safely realize the benefits of cloud computing technologies. These could include everything from amendments to and enforcement of existing privacy laws, to regulations that keep domestic Internet traffic from leaking out to the global Internet, to international treaties on data protection and improved encryption technologies. Making an informed decision about moving to the cloud requires seeing through it, to the reality of existing national jurisdictions and state surveillance practices with which we still live.

This page intentionally left blank.

Introduction

The widespread use of electronic communications–or eCommunications technologies- in the twenty-first century is profoundly affecting how we work, play and interact with one another. These technologies are now an integral part of our lives and allow us to imagine that we are living in a borderless, truly global world. Use of the word "cloud" as a metaphor for globally-accessible Internet services reinforces this idea.

But this mythology is far from the reality. We still live in a bordered world of nation-states; the legal jurisdictions of each determine the rules by which governments and citizens operate within them. Jurisdiction applies also to our digital data. The computers and electronic devices that store and process this data, and the networks over which the data travel, are all subject to the laws of the jurisdictions in which the equipment is located. Adding complexity to this picture are governments like that of the United States of America which attempt to extend their jurisdictional reach extra-territorially, to access data on foreign soil that is under the control of US-headquartered companies.[1]

Despite these facts, most Canadians, it is fair to say, do not think about the privacy implications of using global cloud Internet services that include Gmail, Office 365, Skype and many others. Such services involve extra-national data handling, storing data outside Canada, or at least by companies operating outside exclusive Canadian jurisdiction. Nor do many Canadians attend to the routing paths of their other Internet transactions and the increasing quantities of data traveling outside Canada and through US networks, even if travelling from one Canadian destination to another.

This is not to say that concerns have not been raised in the past in Canada about transborder data flows, mostly to the United States. These were heightened especially after 9/11 with the application of the *USA PATRIOT Act*[2] to Canadian information when

[1] For example, at time of writing there is the "Microsoft Ireland" case: *In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation*. The issue is whether an American judge can issue a warrant compelling Microsoft to hand over email content whose data was stored in Microsoft's Dublin, Ireland data centre. Microsoft did hand over the metadata (non-content data) it had about the user's account on its servers in the USA, but baulked at handing over the content stored in Ireland. The case is under appeal. For information about the case, see http://digitalconstitution.com/about-the-case.

[2] *USA PATRIOT* Act is an acronym for the full title of the statute: *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001*.Public Law 107-56, October 26, 2001. http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf

stored or processed in the US or by American companies. But for many Canadian organizations, this debate ended when our privacy oversight agencies, both federally and provincially, adopted the position that there is no relevant difference between Canada and the United States with respect to the risk of state access to information.[3]

However, the implications of the documents released by Edward Snowden beginning in June of 2013 brought these concerns to the foreground again. The documents provided evidence of mass surveillance by the United States of America and its Five Eyes partners (Australia, Canada, New Zealand and the United Kingdom). It is now clear that such state surveillance has been conducted under legal authorities such as the *USA PATRIOT Act* as well as the USA's *Foreign Intelligence Surveillance Act Amendments Act* (FISAAA) of 2008, particularly section 702. Section 702 makes it legal for the National Security Agency (NSA) to intercept the data of non-US citizens, compels US corporations to cooperate with these requests and forbids these corporations from revealing access requests for the data of non-citizens.

Public disclosure of some of the otherwise secret interpretations of these legal authorities by these security agencies and overseers such as the US Foreign Intelligence Surveillance Court has further heightened concerns. These disclosures reveal positions that are remarkably far-reaching in their implications, are of contested constitutionality and are threatening to human rights, especially for non-US persons.[4] As a consequence, many individuals, enterprises and nation-states have been actively re-examining

---

[3] The notable exception is British Columbia, where the province's public sector Freedom of Information and Protection of Privacy Act ("FIPPA") was amended 21 October 2004 to require personal information held by public bodies be stored exclusively within Canada. British Columbia. *Freedom of Information and Protection of Privacy Act* [RSBC 1996] Chapter 165, s.30.1. http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/96165_00. The amendment followed the findings in the report issued by David Loukedelis, British Columbia's Information and Privacy Commissioner (1999-2010): British Columbia, *Privacy and the USA PATRIOT Act*, *Implications for British Columbia Public Sector Outsourcing*, 2004, https://www.oipc.bc.ca/special-reports/1271. Nova Scotia has a similar blocking requirement, but the statute allows for extra-national outsourcing if the head of the public body permits it and is now testing the use of Google Apps for Education in its K-12 school boards. See http://novascotia.ca/News/Release/?id=20150213003.

[4] See for example: Caspar Bowden, *The US surveillance programmes and their impact on EU citizens' fundamental rights*, a briefing note to the European Parliament's Committee on Civil Liberties, Justice and Home Affairs., September 2013. http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf

assumptions about the privacy and security of their communications, and making a variety of legislative, policy, technological and behavioural changes in response.[5]

The issue of private and secure digital communications affects us not only as individuals, but as researchers concerned about ensuring protection for the principle of academic freedom and as teachers concerned about the potential impact of state surveillance activities on our students.[6] As a result, we embarked on the year-long research study reported herein. While addressing key issues central to the privacy of electronic communications generally, we examined them in the specific case of university extra-national outsourcing of eCommunications. Canadian universities have also been increasingly embracing the extra-national outsourcing of eCommunications, principally to either Microsoft or Google, two leading cloud service providers for many industry sectors.

We chose to focus on the university sector not only for the obvious reason that as academics we understand its mission and purpose well, but also because universities' eCommunications systems contain a wealth of private and confidential information that overlaps with many other industries and organizations in Canada, including medical data (faculties of medicine, medical research), financial data, intellectual property, inventions and patents, private and confidential HR information, information about confidential informants, research in progress, student records and correspondence with students. This means our results are more broadly applicable to other sectors.

Several major concerns motivated our research and structured our investigations. First, we became aware that university extra-national outsourcing decisions, even when accompanied by Privacy Impact Assessments (PIAs), relied heavily on the claim of a supposedly "similar risk" of state surveillance of and state access to eCommunications,

---

[5] This includes everything from individual use of non-tracking search engines like DuckDuckGo and use of the Tor browser for anonymously using the Internet (www.torproject.org), to efforts by nation-states to locate and route domestic data in country and to develop better regulations and laws protecting digital data. See for example, DuckDuckGo's 600% increase in use since 2013: http://www.theguardian.com/technology/2015/jun/17/duckduckgo-traffic-snowden-revelations. The European Union is working towards a soon-to-be-finalized Data Protection Regulation. See the Joint Statement of the European Data Protection Authorities press releases and updates at http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/index_en.htm.

[6] Canadian Association of University Teachers (CAUT), "Email Outsourcing Threatens Privacy & Academic Freedom," CAUT Bulletin, Vol 54, No 5, May 2007. https://www.cautbulletin.ca/en_article.asp?ArticleID=239, Taylor Stinson, "Concerns over NSA monitoring as students' emails now stored in US," The Varsity, 25 November 2013, Modified: 28 November 2013. http://thevarsity.ca/2013/11/25/concerns-over-nsa-monitoring-as-students-emails-now-stored-in-us/.

independent of whether data was in Canada or the US; from this perspective, it does not really matter in which jurisdiction the data were stored or routed. As this position appeared to be based on faulty assumptions, factual errors and a surprisingly limited expectation for privacy in eCommunications, we conducted a close legal comparison of the various Canadian and US statutory and constitutional protections of data, questioning in particular the "similar risk" assertion.

Second, the now well-known details about the extent of the NSA's secret surveillance programs, especially targeted towards non-US persons, and the wide range of individuals and communications activities that the NSA is permitted to lawfully target further heighted our concerns. The PRISM surveillance program, also enabled by section 702 of the *FISA Amendments Act* of 2008, is particularly troubling, as it allows the NSA access to data held by Internet Service Providers without judicial review of individual requests.[7] Among the listed PRISM data sources are Google's and Microsoft's servers; these two vendors are the principal providers of outsourced eCommunications services for universities and are also widely used across business, government and non-profit sectors. Another set of NSA surveillance programs known as UPSTREAM, which intercept communications while in transit across the Internet, captures an even wider range of individual communications. Simply fitting a profile of behavior or affiliation and thereby becoming a 'person of interest' to one of the NSA's many client agencies' such as the FBI, CIA, or Customs and Border Protection, can have serious negative consequences. We have seen US security agencies use the personal data of innocent Canadians to deny them entry into the US, block them from airplane travel, and in the extreme case of Maher Arar, subject him to third country rendition and torture.[8] While some of these known cases involve inappropriate disclosures by Canadian law enforcement agencies to their American counterparts, the consequences which occurred reveal the harm that can be done by the collection and disclosure of personal information without proper legal safeguards.

---

[7] *Washington Post*, NSA slides explain the PRISM data-collection program, June 6, 2013, Updated July 10, 2013. http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

[8] Maureen Webb, *Illusions of Security: Global Surveillance and Democracy in the Post 9/11 World*, City Lights, 2007; Ann Cavoukian, *Crossing the Line: The Indiscriminate Disclosure of Attempted Suicide Information to US. Border Officials via CPIC: A Special Investigation Report*, (Toronto, Ontario: Office of the Information and Privacy Commissioner, 2014). In the Cavoukian report, the Commissioner discovered that the RCMP were giving access to a Canadian police database to US officials, which included information on non-criminal police responses to medical emergencies. https://www.ipc.on.ca/images/Resources/indiscriminate_disclosure.pdf.

In light of these concerns, a major strand of our research was to review the Privacy Impact Assessments of the Canadian universities that had outsourced their eCommunications extra-nationally, focusing on such questions as:

- What expectations of communications privacy do outsourcing universities aim for?
- How do these universities evaluate privacy risks in comparison to other criteria, such as cost reduction?
- How do universities treat eCommunications in relation to their teaching and research missions?
- To what extent did universities rely on the 'similar risk' argument?
- Did those universities that conducted PIAs after June 2013 take into account the new evidence of the sweeping extent of NSA surveillance programs, especially the PRISM program?

We also examined the contracts that universities made with Google or Microsoft, to assess among other features:

- The extent of contractual protections for privacy and other academic values (essential to supporting the core mission of universities),
- What jurisdictions personal data will be exposed to,
- How and under what terms the vendors will respond to third-party requests for personal information,
  and
- What privacy protections are explicitly given to a person's metadata?

This report summarizes the findings of our investigations into these various concerns. We begin with "Understanding Cloud Technologies," a necessary precursor to the analysis which follows. "Observations from University Outsourcing Decisions" discusses our particular findings with respect to University contracts and Privacy Impact Assessment documents. The next section, "Why Jurisdiction Still Matters" outlines the specific faults in the legal reasoning of the "similar risk" analysis that has been the primary legal support for extra-national outsourcing to date.

Much domestic Internet traffic is also inadvertently exposed to US mass surveillance as it transits the United States on its travel between Canadian cities. "Jurisdiction of Internet Routing Matters Too" describes this risk, and what we can do about it. The

privacy challenges we are facing with the cloud technologies are not new; indeed the privacy concerns we have today were predicted and discussed extensively in the seventies and eighties. "Transborder Dataflows (TBDF) in Historical Context" looks back to the 1970s for early debates on this issue and describes what we can learn from the past.

Based on the results of our research, and drawing on previously published Canadian reports on the issue of TBDF, we also developed an assessment framework designed to assist Canadian organizations conducting PIAs and Threat Risk Assessments (TRAs) in relation to extra-national outsourcing deliberations. The next section "A Framework for Canadian Organizations" summarizes the approach of the longer guideline document available for download on our website.

Looking ahead, the "Moving Forward: Protecting the Privacy of eCommunications" section describes concrete actions that can be taken now to secure the benefits of cloud-computing technologies without the cost of our privacy rights and flags additional areas of concern where further research is urgently required, such as the applicability of US law and the reach of American warrants on data hosted in servers on Canadian soil owned by companies headquartered in the United States.

The report concludes with our formal recommendations. The appendix lists the full titles of the longer reports that support the findings presented within this document.

Understanding the Cloud

What is "the Cloud?" When Information Technology professionals talk about cloud computing, they are talking about the ability to sell or buy slices of computer services over the global Internet. Most commonly, these services are known as IaaS (Infrastructure as a Service) – where you purchase access to entire remote servers, PaaS (Platform as a Service) – where you buy access to portions of servers running a particular system) or SaaS (Software as a Service) – where you purchase access to a specific software tool or product.

Organizations make these Cloud choices to leverage the considerable economies of well-managed server farms over smaller scale in-house operations, as well as the Disaster Recovery benefits of data duplicated in multiple locations off-site. The eCommunications services provided by Microsoft's Office 365 and Google's Apps for Business/Education products are examples of Software as a Service offered in the "public" cloud – that is, as a cloud technology service available to anyone who wants to buy it, rather than a publically-funded service. Consumers who use Gmail, Office 365, Dropbox or other such web-accessible services are also using Software-as-a-Service in the public cloud.

Some companies choose to use cloud technology to ensure their data are secure in multiple locations and readily available to employees across multiple devices, but they own the servers themselves. This is known as private cloud. Some organizations use a combination of public and private cloud services (hybrid cloud) and some (including in the public sector) form their own private type clouds, shared with multiple other non-profit organizations. This is known as community cloud.[9] Cloud technology services do not by definition have to be extra-national, with data transiting the global Internet, but public cloud services typically are. As server farms are expensive to operate, vendors look for the most suitable locations to ensure speedy access and low costs in terms of both labour and energy for operational and air conditioning needs.[10]

---

[9] Peter Mell and Timothy Grance, "The NIST Definition of Cloud Computing," Special Publication 800-145, (United States of America, Department of Commerce, National Institute of Standards and Technology: September 2011), 2-3, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[10] Vincent Mosco, *To The Cloud: Big Data in a Turbulent World*, (Paradigm Publishers, 2014), 124-137.

The word cloud has therefore come to have multiple meanings within the field of information technology, creating much scope for confusion. Further, the ubiquitous use of a term like the cloud or the related term cyberspace has privacy implications as it encourages us to think of our eCommunications happening somewhere distinct from the physical world, independent of the jurisdictions in which the servers and routers and other telecommunications equipment on which the software and networks run. This is simply not true. Referring to transborder data flow as "the cloud" does not get rid of the complex problems created by storing private, confidential and/or sensitive data extra-nationally.

Prevailing definitions of the cloud and cyberspace contribute to this problem by conveying a false sense of realness to these terms.[11] Our federal government's own definition of cyberspace also reinforces this idea. Canada's Cyber Security Strategy defines cyberspace as "the electronic world created by interconnected networks of information technology and the information on those networks. It is a global commons where more than 1.7 billion people are linked together to exchange ideas, services and friendship."[12] That same definition has been cited in more recent reports, including a December 2014 report on Privacy and Cyber Security issued by the federal Office of the Privacy Commissioner.[13]

Adding to the confusion, academics and policy experts continue to discuss and debate whether and how cyberspace should be governed as if it was a real place that actually could be regulated independent of the nation-states in which the servers and networks are housed.[14] Indeed, part of Canada's official Cyber Strategy argues that "the cyber world in which Canadians live, work and play lacks the regimes of law and order that govern our physical world." But the servers and networks that we use do exist in the

---

[11] The US National Institute of Standards and Technology's definition, in contrast, correctly focuses on the hardware, software and networks involved, defining cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services). See Mell and Grance, "The NIST Definition," page 2.

[12] Public Safety Canada, *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada*, Ottawa, 2010. http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx.

[13] Canada, Office of the Privacy Commissioner, "Privacy and Cyber Security Emphasizing privacy protection in cyber security activities," December 2014, https://www.priv.gc.ca/information/research-recherche/2014/cs_201412_e.asp.

[14] For example, in January of 2015 the London School of Economics hosted an "After Snowden" IDEAS-Public Discussion "What conversations do we need to have about the rules of cyberspace?" http://www.lse.ac.uk/publicEvents/events/2015/01/20150120t1830vOT.aspx.

physical world, and our existing laws already apply to them. There is no separate "cyber world," however much we imagine otherwise.[15]

When considering the privacy implications of extra-national outsourcing, it is essential to have a solid understanding of what cyberspace is, what the cloud is, and what is meant when we talk about outsourcing to the cloud. All data and software "somewhere in the cloud" is always on a physical machine or is transiting a network somewhere in the world.

The reality is that the establishment of communications through networked devices did not create a new jurisdiction any more than did the postal system, the development of telegraph networks in the mid-19th century, or the ability to make an international telephone call. These communication systems are all borderless like the Internet in that data flows across international borders. But in all of these cases the data itself, and who has legal access to it and under what conditions (i.e. can the state open your mail or tap your phone calls without a warrant) are all subject to the laws of the country in which the data exist or are passing through, and possibly also to the laws of the country to which the enterprise owning these facilities is subject. Or in the case of trans-oceanic transmission, to whatever countries possess the technology and interest in tapping undersea telecommunications cables.[16]

The privacy risks and efficiency benefits of the different cloud-computing technologies and options are well known in the Information Technology field, but less well known to the broader public. Nevertheless, even IT professionals can be swayed by the warm, fluffy impression created by the meteorological connotation of the word "cloud." One British IT security consultant argues that such use of the word cloud has created a culture of "carelessness by organizations as they ship their data off to cloud providers without properly considering how sensitive data could be vulnerable if stored this way, especially if it isn't encrypted."[17] Or we need to add, vulnerable *en route* or if the data

---

[15] For the sake of completeness, it is important to note that even outer space is regulated by what is in effect an extension of terrestrial international law. See United Nations, Office for Outer Space Affairs, "Space Law," http://www.unoosa.org/oosa/en/ourwork/spacelaw/index.html.

[16] See for example, the work of British spy agency GCHQ, revealed by Edward Snowden. "GCHQ taps fibre-optic cables for secret access to world's communications," *The Guardian*, 21 June 2013, http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

[17] Graham Cluley, quoted in Danny Palmer, "We should replace the word 'cloud' with 'somebody else's computer', says security expert," *computing*, 2 December 2013, http://www.computing.co.uk/ctg/news/2316368/we-should-replace-the-word-cloud-with-somebody-elses-computer-says-security-expert.

are processed on an outsourced server, rather than simply stored encrypted there. For example, if you want to edit an encrypted document that you have stored on a cloud service, that document must be decrypted first in order to edit it. Encryption can only protect data that is stored (at rest) or being transmitted across networks. Processing data (i.e. writing an email message, editing a spreadsheet) at present requires that the software on the remote server be able to read and display the contents of the file, and the file must be decrypted to do so.[18]

Since outsourcing to public cloud systems means placing your data on **someone else's computer systems,** where it must be decrypted before using Software-as-a-Service, the next crucial questions are in what country are those systems located? Through what other locations must the data pass to get there, and who handles it on the way? Vendors of public cloud services, like Microsoft, Google and Amazon, will tell you that the benefits of cloud computing mean that you don't need to know or care where your data are stored, via which countries it transits and whose hands it passes through. Amazon's description of cloud computing, for example, emphasizes the economic benefits: Amazon's global server farms achieve "massive economies of scale," so users can "stop spending money on running and maintaining data centers."[19] Organizations can host data in different jurisdictions around the world, an attractive proposition for many who perceive that the benefits of being "global" outweigh the information security and privacy risks.

Both Microsoft and Google, as leading providers of eCommunications solutions, have their primary data centers in the US for the North American market, but, as the contracts with Canadian universities we examined clearly state, user data can also be stored anywhere in the world that they, their subsidiaries or their subcontractors have facilities, (except the US embargoed countries, typically listed explicitly in contracts and currently consisting of Cuba, Iran, Syria, North Korea, Myanmar (formerly Burma) and Sudan). Some of the world's largest cloud computing data centres, even so-called "cloud

[18] There is some intriguing work on the use of new technology to work with encrypted data (homomorphic encryption) but it is not yet realized and it may not be practical for many years yet, despite the press claims of IBM, which has filed for a patent on the idea. See the comments of noted Internet security expert Bruce Schneier on this topic: https://www.schneier.com/blog/archives/2009/07/homomorphic_enc.html.

[19] Amazon.com, "What is Cloud Computing," https://aws.amazon.com/what-is-cloud-computing/.

cities," are also now in China, for example, a country without the protections for individual rights including privacy rights afforded in constitutional democracies.[20]

Users need to be aware that not only do different countries have different standards for accessing private data, they do not typically offer a higher or even the same level of protection for the data of non-citizens and non-residents stored within their borders or transiting through. We argue therefore that the jurisdiction of data storage needs to be the primary consideration in Privacy Impact Assessments when extra-national outsourcing of eCommunications is considered. Extra-national outsourcing may in fact be appropriate for some organizations, and for some classes of data, but certainly it is not for all.

We think that it is time to start seeing through the cloud.

[20] Mosco, *To the Cloud*, 72-74.

Observations from University Outsourcing Decisions

Canadian Universities are increasingly outsourcing their eCommunications services to one of two multi-national providers: Google Incorporated or the Microsoft Corporation, both with headquarters in the United States. Beginning with Lakehead University's move to Google Apps for Education in 2006, universities have opted for either Google's Apps for Education product or Microsoft's Office 365 to provide not only email but entire suites of productivity software and eCommunications tools.

Both of these products allow customers to maintain their own domains (e.g. @lakehead.ca) while the data resides on the vendor's servers. Students, faculty and staff may think that their virtual campus resides in the same place as the physical one, but when these services are outsourced, the link between the two is severed. What are the privacy implications of doing so? [21]

Canadian universities are actually arriving late to what is a rapidly accelerating global trend. The delay in moving Canadian university eCommunications data to the cloud appears to have been influenced initially by concerns about the privacy implications of the *USA PATRIOT Act*, but after Lakehead University's and then the University of Alberta's successful migrations, outsourcing plans accelerated. To explore the privacy implications of these decisions, we used provincial Freedom of Information (FOI) laws to request information from twenty-one Canadian universities who had outsourced at least student (and in some cases faculty and staff eCommunications services) to either Microsoft or Google. These twenty-one were drawn from a pool of thirty-five of Canada's largest or leading provincial institutions.[22] Others, including those in British Columbia, francophone universities in Quebec, McGill University, the Universities of Saskatchewan and Regina and the University of Calgary, have not outsourced as of writing. Table 1 lists those we included in our study. Most universities have only outsourced eCommunications for students; names in ***BOLD italics*** indicate schools that

[21] The longer report on which this summary is based is available on the project website as a downloadable pdf. "Appendix A: Heidi Bohaker and John M. Dirks, "Privacy Impact Assessments and Microsoft & Google Vendor Contracts: Examining Canadian University eCommunications Outsourcing decisions," http://ecommoutsourcing.ischool.utoronto.ca/.

[22] We included Lakehead, although a smaller school, as it was the first to outsource. The Ontario College of Art and Design University (2002) and Ontario University Institute of Technology (2002) are two of Canada's newest Universities and we included them to complete the set of universities in the Greater Toronto area.

have outsourced faculty and staff eCommunications systems as well. Note that some schools made use of the new systems mandatory, while others allowed users to "opt in" to the extra-national systems.

Table 1: Universities asked for PIAs and Vendor Contracts

Year [23]	University (bold, italics indicates faculty/staff outsourced as well)	Province	Vendor
2006	***Lakehead University***	Ontario	Google
2010	***University of Alberta***	Alberta	Google
2011	University of New Brunswick	New Brunswick	Microsoft
2011	University of Prince Edward Island	Prince Edward Island	Google
2011	University of Toronto	Ontario	Microsoft
2011	***Carleton University (Faculty, 2014)***	Ontario	Microsoft
2011	McMaster University	Ontario	Google
2012	Ontario College of Art and Design University	Ontario	Google
2012	University of Ottawa	Ontario	Google
2012	***Ontario University Institute of Technology***	Ontario	Google
2012	***Ryerson University***	Ontario	Google
2012	Memorial University	Newfoundland and Labrador	Google
2012	University of Windsor	Ontario	Google
2012	***Queen's University (Faculty, 2013)***	Ontario	Microsoft
2013	***Dalhousie University***	Nova Scotia	Microsoft
2013	University of Manitoba	Manitoba	Microsoft
2014	Concordia University	Quebec	Microsoft
2014	University of Guelph	Ontario	Google
2014	Western University[24]	Ontario	Microsoft
2014	York University	Ontario	Google
2015	Brock University	Ontario	Microsoft

In our Freedom of Information requests, we asked for copies of the vendor contracts, and any Privacy Impact Assessment documents (PIA) that had been prepared when

[23] For most schools, the year is the date the contract with the vendor was signed. The University of Prince Edward Island, Concordia University and Brock University separately informed us that they had no signed contract with the vendor. Instead, users at these schools accept the terms of use as provided by the vendor.
[24] Formerly the University of Western Ontario.

making their decision to outsource. PIAs are documents that describe the work that an organization has done to assess how its policies and procedures affect the organization's ability to protect the personal information in its custody.[25] They are used "to identify the potential privacy risks of new or redesigned … programs or services. They also help eliminate or reduce those risks to an acceptable level."[26]

Although each of the universities we studied made their outsourcing decision independent of each other and in accordance with the regulatory and statutory requirements of their respective provinces, when we examined the Privacy Impact Assessment documents we observed a common and yet problematic set of assertions and lapses.

The authors of these university PIAs:

1. **Relied on the "similar risk" argument,** that the risk of disclosure to third parties is roughly the same regardless of where the data are stored. In doing so, we noticed that these authors were drawing on conclusions reached by some privacy commissioners and asserted by some privacy experts and product vendors. As we have found in our research, this argument is deeply flawed.[27] Canadian jurisdiction offers significantly better privacy protection to Canadians and residents than US jurisdiction does, for example.

2. **Lowered the expectation of privacy for university users of eCommunications systems,** by repeating the assertion that email is "like a postcard" and is also "fundamentally insecure" because people cannot control if messages are forwarded on to others.

   Email systems do not have to be insecure. The level of security possible depends upon the technology being used. Furthermore, internal communications within an organization can be made very secure using modern enterprise-class eCommunications systems. Second, any possible breach of confidentiality by either senders or receivers (as can also occur with regular mail) cannot be used to justify storing eCommunications in jurisdictions where third parties (i.e. government

[25] PIAs are widely seen as a "best practice" but are not required by statute in Canada for universities. However, they are required, for example, in Alberta in the health care sector. See Alberta. *Health Information Act*, RSA 2000, Ch. 5, s.64. http://www.qp.alberta.ca/documents/Acts/H05.pdf.
[26] Office of the Privacy Commissioner, *Fact Sheet*, https://www.priv.gc.ca/resource/fs-fi/02_05_d_33_e.asp.
[27] The full legal analysis which conclusively demonstrates why the similar risk argument is flawed is available as an appendix to this report. See Lisa Austin and Daniel Carens-Nedelsky, "Why Jurisdiction Still Matters," available as a pdf file at http://ecommoutsourcing.ischool.utoronto.ca/.

agencies) have greater access to such communications than is the standard in Canada.

3. **Conflated privacy and security issues by using the "incremental risk" argument.** This argument asserts that even factoring in the risk of disclosures to foreign governments, eCommunications data will have better protection overall from risk of disclosure because of purportedly better data security measures when outsourced to major cloud providers.

   This argument asks Canadians to forfeit their rights and protections as citizens and residents in the name of the savings to be realized from universities not having to invest in secure computing solutions.

4. **Focused on email only or nearly exclusively**, when the outsourced product under consideration is actually a full suite of eCommunications and productivity tools.

   The PIAs we examined talk nearly exclusively about the privacy risks to email. The new services also provide calendaring, instant messaging, file storage and document creation utilities, among others, and yet the privacy implications of using them were typically not assessed at all, or only in a very minor way.

   Further, in some PIAs, while making the flawed case that email was inherently insecure, there were recommendations that faculty, staff and students conduct confidential communication using alternative means, for example, talking on the phone. But many Universities are looking to replace or are replacing their land-line phone systems with the integrated digital voice and audio services (i.e. Skype for Business from Microsoft) bundled with the eCommunications suites offered by these vendors.

   Such advice is logically incoherent. Faculty and staff cannot be told to use alternative communications technologies as a workaround to the purported privacy implications of using email that is created and archived extra-nationally, when those alternate technologies are provisioned by the same extra-national vendor and the digital records of voice and video calls are also stored on the same extra-national system.

5. **Gave limited or no consideration to the privacy and security implications of mass surveillance activities by the United States National Security Agency.** In addition, mention of Canada's own surveillance apparatus, the Communications Security Establishment (CSE) was typically brought up only in support of the "similar risk"

argument, rather than any substantive engagement with the different statutory terms under which the data of Canadians can be collected under Canadian law. In particular, no PIA that we examined which was authored after the Snowden revelations of June 2013 examined significantly or at all the privacy implications for University users of the NSA's reported collection of eCommunications data directly from Google and Microsoft through the PRISM program.

6. **Defined eCommunications as separate from the teaching and research missions of universities.** This assertion, which occurs in many PIAs, justifies outsourcing on the grounds that outsourcing eCommunications frees up university IT resources to focus on the "teaching and research mission."

   But communication *is at the heart* of what universities do; today that communication increasingly happens over digital networks. Secure and private digital communications are therefore necessary to fulfill the academic mission. In our digital era, university eCommunications systems are part of critical infrastructure that supports a university's core mission in the same ways that libraries and laboratories do. The PIAs we examined did not assess the impact of outsourcing on academic freedom. Neither did these PIAs consider the ways in which academic conversations between faculty and the students they teach are increasingly occurring over digital networks. In other words, by focusing solely on FIPPA compliance and/or security threats to data, these documents did not consider the risk of extra-national outsourcing to their university's mission and purpose as a whole.

Vendor Contracts

Microsoft and Google typically offer access to their educational Software as a Service offerings through contracts signed between the institution and the vendor, although these are increasingly taking the form of either volume license agreements or no contract at all between the university and the vendor, where the End Users simply accept the terms of use of the vendor when they activate their accounts on the respective systems.[28] We noted that the contracts do not guarantee the provision of eCommunications systems free of charge in perpetuity, or indeed, for any term beyond

[28] Note that the agreement between the institution and the vendor comprises not a single document but rather a set of documents. Some were obtained through FOI requests (and partially redacted) and others, such as terms of use agreements, were referenced in the contract and were available on the web.

the length of the contract.[29] Once universities are "locked in," they may well find it very expensive to move to a competing service, if the vendor begins to charge for a formerly free service upon renewal.

We observed the following key concerns related to privacy:

1. Customer Data are not stored solely in the USA, but in any country in the world in which the vendor, its subsidiaries or affiliates do business (excepting of course the US-embargoed countries).[30]

2. Microsoft and Google contracts both say that they respect the privacy of customer data and will only hand over data to third parties in the case of lawful requests made by government agencies. These contracts **do not** however specify **which laws, or which governments**.[31] In fact, these contracts mean all countries in which these vendors do business. Corporations must respect the laws of the countries in which they operate. If that country submits a lawful request to a cloud provider for access to data stored within their jurisdiction, the company will comply. By signing the contract, customers acknowledge this risk.

3. The contracts provide protection for customer data only, not metadata. Further research is required to determine if these contract provisions permit Microsoft and Google to harvest or "mine" the metadata associated with institutional customers and sell access to metadata or aggregate data to businesses and government agencies for analysis with business intelligence tools that look for patterns in the data.[32]

---

[29] While both Google Apps for Education and Microsoft Office 365 for Education are promoted as "free" to qualified schools, the contracts are term limited (two to five years) and contain reference to services for which fees are currently charged (such as Google Vault, or encryption provisions). The fee structure for paid services is based upon monthly subscription fees on a per user basis.

[30] Contracts refer to the "primary" storage region for Canada as data centres located in North America (which could include Mexico and the Caribbean), but this does not mean the *exclusive* data storage region, and indeed both vendors acknowledge that data can be moved out of the primary storage region for a variety of purposes, including access by affiliates in other parts of the world.

[31] Microsoft is at time of writing accumulating significant fines for failure to comply with a US request to hand over data on a Microsoft server in Ireland. However, this case concerns the limits of the reach of US law.

[32] Google has already been the subject of lawsuits in both the UK and the US alleging it has done just that with student data. While students were not subjected to targeted advertisements within Google Apps for Education, the profiles generated by metadata analysis of their institutional accounts had been allegedly passed to third party advertisers, who could then target students more precisely. Google has admitted the practice after lawsuits were filled in the US and UK, and clams it is no longer doing so. Karis Hustad, "Google will no longer data mine student e-mail accounts" *The Christian Science Monitor*, 30 April 2014,

Once reassured through PIAs and legal consultations that they would not run afoul of federal and provincial privacy law, it is fair to say universities looked to the outsourcing on offer as a "win" on multiple levels: a decision that would provide significantly enhanced services and redirect cost savings towards other badly needed services. Investing in enterprise quality in-house or in-country eCommunications services certainly costs money. But the choice of eCommunications provider should be made in full consideration of the impact of extra-national outsourcing on the mission and purpose of universities, on teaching and research activities and of the fiduciary-like obligation that universities have to protect the privacy of their faculty, staff and students and to uphold the principle of academic freedom.

While the focus of our research has been on the extra-national outsourcing of eCommunications services in Canadian universities, the implications of our findings apply as well to the K-12 and post-secondary education sectors, the public sector more broadly, and to private companies also considering extra-national outsourcing. We anticipate that a larger study would likely find similar types of assertions in PIAs, following the advice of federal and provincial privacy commissioners, and of course, similar clauses in contracts with multi-national vendors. We found that the assertion that data faced a "similar risk" from surveillance underpinned all of these decisions; in the next section we explain why the similar risk analysis is so deeply flawed.

---

http://www.csmonitor.com/Technology/Horizons/2014/0430/Google-will-no-longer-data-mine-student-e-mail-accounts.

Jurisdiction Still Matters: Why the "Similar Risk" Argument is Deeply Flawed

In our review of university decisions to outsource their email services extra-nationally, we found many of them were alive to the possibility that American authorities at the very least might be able to access their communications data. Often they addressed this concern by referring to decisions by federal and provincial privacy commissioners who held that the risk of state access to personal information is similar whether this information is stored in Canada or abroad. **In our discussion of why jurisdiction still matters, we argue that this "similar risk" analysis is deeply flawed.** [33]

The 'similar risk' analysis rests on three propositions. First, it acknowledges that outsourcing means that the information involved is subject to foreign laws and that no contractual provisions can override those laws. Second, it points to the fact that state authorities can also access personal information under Canadian laws as well. Third, it indicates that there are bilateral agreements that permit information sharing between countries. The conclusion of the analysis is that there is a similar risk of state access to information no matter where the information resides.

We argue that this analysis focuses too much on the question of ***whether*** the state can access information and does not focus at all on the question of access ***on what standards***.

The issue of "on what standards" is central to constitutional protections for privacy. Under the Canadian *Charter of Rights and Freedoms*, the question is never whether the state can access personal information but rather what kinds of protections should govern the terms of that access (such as the requirement of a warrant on reasonable and probable grounds). This constitutional question needs to be asked when comparing privacy protections across jurisdictions.

In failing to ask this question, the "similar risk" analysis also fails to focus on the crucial differences between Canadian and American constitutional protections for privacy. In general, Canadian constitutional privacy norms are more privacy-protective than US

[33] The full report on which this summary is based is available on the project website: Lisa Austin and Daniel Carens-Nedelsky, "Why Jurisdiction Still Matters" http://ecommoutsourcing.ischool.utoronto.ca/.

norms. Moreover, the constitutional norms of neither country protect communications data when that information is within US territory but the person to whom that data pertains is within Canadian territory. A Canadian resident, for example, whose data are stored in the US, cannot expect protection from third party access under Canadian constitutional norms *or* US constitutional norms. **Their data falls into a constitutional black hole, where the constitutional protections of *neither* country apply**.

In failing to address the issue of "on what standards", the "similar risk" analysis also fails to take into account important differences between Canada and the US in relation to their statutory frameworks for lawful access. **Although it is true that state authorities *can* access communications data in both countries, the standards differ.**

These differences become particularly acute when the different treatment afforded to US persons (citizens or residents) in comparison to non-US persons is factored in. The legal comparison must be between Canadian persons with their data in Canada and non-US persons with their data in the US, and *not* between Canadian persons with their data in Canada and US persons with their data in the US.

Taking into account both these constitutional considerations and the relevant statutory frameworks, **we conclude that Canadian persons have more protection under Canadian law when their data are within Canada** than Canadian persons (as non-US persons) have under US law when their data are within the US.

We conclude with the following five points:

1. US authorities can access Canadian persons' communications data within US jurisdiction on statutory standards that are lower than those that apply within Canadian jurisdiction and would be unconstitutional if applied within Canada.

2. 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.

3. Even if US constitutional law did apply, Canadian constitutional law offers more privacy protection to communications data.

4. 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.

5. Mutual Legal Assistance Treaties ensure that the constitutional norms of the "assisting" country are applied. Therefore US authorities obtaining personal information through the MLAT process are subject to stricter norms than US authorities obtaining the same information within US jurisdiction, because Canadian constitutional norms offer higher privacy protection.

Jurisdiction of Internet Routing Matters Too: Canadian Internet Traffic Patterns and Mass NSA Surveillance

Most of the privacy and security concerns about organizations outsourcing their eCommunications have focused on email and other services, with personal and corporate data being stored and processed in the "cloud", or more precisely on other organizations' servers that typically are outside Canadian jurisdiction.[34] Less attention has been given so far to the less visible, but longer standing surveillance risks that come from the capture of data on the move across the Internet. Because of the way the networks that make up the Internet are configured in North America, much domestic Internet traffic passes through the United States on its way between Canadian end-points, even when geographically close. We refer to this as "boomerang" routing.

Telecommunication carriers like Bell, Rogers, Telus and others are the companies that control the data flows between local devices and servers on the Internet. Because no single network carrier reaches every device, outsourcing of the task of providing Internet connectivity, or transit, is an inherent feature of contemporary data communications. The issues of foreign jurisdiction and risk of mass state surveillance relevant to data storage apply to transit as well - even more so when one considers the wide range of personal, confidential and sensitive data that is transmitted over the Internet and not necessarily stored in readily identifiable or locatable data stores.

Everything we do on the Internet (i.e. beyond our own immediate local network) involves transit – routing data through devices on someone else's network, and hence opens the opportunity for surreptitious interception by those with access to the routers and cables carrying the data from one location to another. In 2006 the public learned from retired telecom technician turned whistleblower, Mark Klein that the National Security Agency installed "splitter" facilities in major switching hubs controlled by AT&T so it could analyze and selectively store all the data passing through these vital

[34] The full report on which this summary is based is available as a pdf file on the project website: Andrew Clement and Jonathan Obar, "Canadian Internet 'Boomerang' Traffic and Mass NSA Surveillance: Responding to Privacy and Network Sovereignty Challenges", http://ecommoutsourcing.ischool.utoronto.ca/.

Internet "choke" points. Splitters in roughly 18 American cities are all that are needed to capture nearly 100% of all Internet traffic flowing within the U.S.

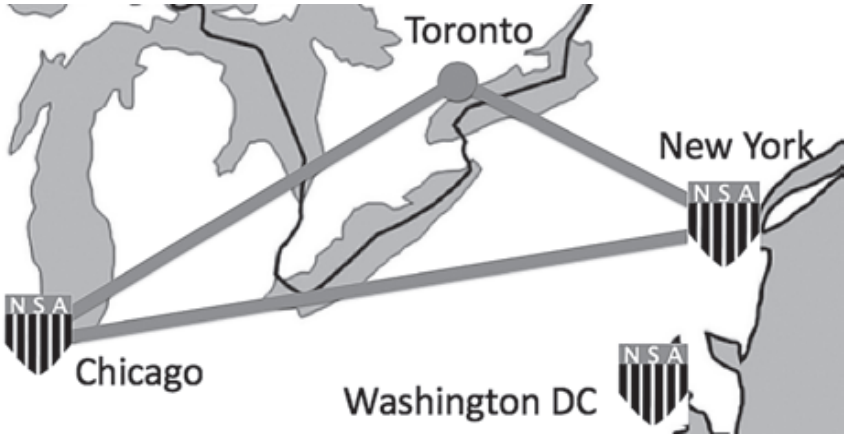

Figure 1: Boomerang Routing: The recorded path of an Internet message (more accurately, a data packet) travelling between a University of Toronto computer and the Provincial Office for the Ontario Student Assistance Program.

Surprisingly, even traffic between two points in the same Canadian city often travels via the United States. This needlessly exposes domestic Canadian traffic to capture by US state surveillance programs. Many Canadians, wherever they may be, communicating via the Internet with their federal or provincial government departments will have their data transit the United States. This can even occur between public bodies in the same province, the same city or even the same neighbourhood block. For example, we have traced Internet traffic from the University of Toronto to Ontario government departments located across Queen's Park Circle, just across the street from the downtown campus. This data travels via New York and Chicago, both prime cities for NSA interception, because these government departments, or their Internet Service Providers, typically Telus and Bell in these cases, do not exchange traffic directly with University of Toronto, nor with the network servicing Toronto area universities, called GTAnet. To send a message across the street, the GTAnet network is thus required to contract with a transit provider that does provide this interconnection, which occurs inside the United States.

This boomerang Internet routing pattern not only presents risks from US-based mass surveillance but also has significant economic disadvantages to Canadian business - it contributes significantly to transmission delays (latency) while adding to the expense of

moving data. In 2012 the Canadian Internet Registration Authority (CIRA) commissioned an expert report on Canadian Internet routing, which found that "Canadian Internet access is heavily and unnecessarily dependent upon foreign infrastructure, especially U.S. infrastructure … impos[ing] significant burdens on Canadian Internet users" in terms of higher prices, slower speeds and additional interception risks.[35]

To mitigate these burdens, CIRA has adopted the principle of "keep local traffic local" and actively promotes the development of Canadian public Internet exchange points (IXPs). IXPs are effectively not-for-profit cooperatives that enable member carriers operating in a particular region to exchange traffic between each other at no cost ("peer") and thereby avoid the following: paying transit providers for this service, slowing response times due to longer routing paths; and exposing data to foreign surveillance. Since 2013 CIRA has contributed to increasing the number of such public IXPs from 2 to 7, and is pursuing further measures to keep domestic traffic within Canada.

Organizations can begin to address the surveillance risks caused by routing of domestic Internet traffic via the US or US carriers by recognizing them in PIAs and TRAs. Furthermore, when contracting with ISPs they can insist on Canadian carriers and intra-Canadian routing for domestic communication. Bell and Telus in particular, which are the ISPs for many government agencies, do not currently peer at any Canadian IXPs. Were they to do so, they would significantly reduce the incidence of boomerang routing, and thereby significantly reduce the privacy implications for Canadians. This is very much a problem that can be mitigated, while strengthening Canada's Internet infrastructure.

[35] Bill Woodcock & Benjamin Edelman, *Toward Efficiencies in Canadian Internet Traffic Exchange*, Canadian Internet Registration Authority (September 2012).

Transborder Dataflows in Historical Context

While concerns over the privacy issues raised by extra-national outsourcing may seem quite recent, many of the privacy implications were actually flagged decades ago, when the technology of today was only being imagined. Far-sighted anticipation of increasing Internet traffic and loss of user control over data has been at the heart of data protection discussion for a surprisingly long time: the past half century. Transborder dataflow, or TBDF, was a major driver for the development of data protection law during the 1970s, as nations realized that there were economic benefits in sending data offshore for processing. Concerns were soon raised about the privacy implications of doing so. There are important lessons to be learned from examining this older history, most importantly that legal reform and public attention to this issue is needed to ensure that the privacy rights of Canadian citizens and residents are protected.[36]

While privacy laws have been passed in Canada both federally and provincially, many practical issues have interfered with the enforcement of data protection law in the context of transborder dataflow, including:

- When the issue was raised and studied exhaustively in the 1970s, politicians and business leaders felt at the time that the lowering of communications costs and the creation of better global networks was so vital to economic development that there should not be barriers to dataflow.

- Some key players in the international debate about dataflows in the early period of the 1970s, notably the United States, were also actively campaigning against privacy law for the same reason, to promote private sector economic development.[37]

- The technology has been changing so quickly it has been difficult to get new laws passed or older laws updated to improve TBDF protection. British Columbia is a lone exception, amending its privacy legislation in 2004 in the immediate wake of

[36] The longer report on which this summary is based is available on our project website as Appendix D, Stephanie Perrin, "Transboundary Challenges to Privacy Protection," http:// http://ecommoutsourcing.ischool.utoronto.ca/.
[37] This opposition crystallized when the European Community brought out their draft Directive for the protection of personal data in 1990, to ensure the same level of data protection for member states. "Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data," 1990 oJ. (C 277) 3. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:51990PC0314%2801%29&from=EN.

its Privacy Commissioner's report expressing concerns over transborder dataflow, prohibiting public bodies at least from storing data outside of Canada.[38]

- Even where a law has been enacted (such as the federal privacy law PIPEDA) there are not always sufficient resources to support individuals exercising control of their own data. Individuals must file complaints to the Privacy Commissioners if they have concerns. There is only a very limited compliance role for Federal or Provincial Privacy Commissioners to ensure that companies and public bodies are taking adequate care of the personal information in their custody.

- The funding of the Internet has essentially been based on advertising. That advertising has now become profiling, employing cookies, beacons, and extensive tracking of individuals and their choices and preferences. The pace of development of the Internet has exceeded the ability of courts and regulators to take decisions on matters respecting privacy of this information. This does not mean that the law and/or the decision-making powers of data protection authorities and the courts are irrelevant; it means that the Internet will necessarily be subject to some retro-fitting as rulings occur, and the privacy and human rights impacts of certain aspects of the networks and technology become apparent and rights are enforced.

- The complexity of extra-jurisdictional enforcement of law complicates trans-boundary privacy protection, especially where fundamental rights are assured by constitutional law in some but not in all jurisdictions.

Some argue that personal dataflow does not appear to result in significant harm to other human rights of individuals, and advocate a "risk-based" approach to the protection of personal data. Individuals are largely unaware of where their data goes, the extent to

[38] BC's Freedom of Information and Protection of Privacy Act ("FIPPA") was amended 21 October 2004 following the findings in the report issued by David Loukedelis, then British Columbia's Information and Privacy Commissioner: (British Columbia, *Privacy and the USA PATRIOT Act, Implications for British Columbia Public Sector Outsourcing*, 2004) https://www.oipc.bc.ca/special-reports/1271.

which their data is collected by various government and private sector organizations, or the kinds of risk that they might be running in terms of what digital data can reveal about them. In the age of "big data", it is almost impossible to determine exactly which bits of data or which disclosure of your profile has caused or might cause you harm.[39]

Whether or not an individual can trace the path of their own profiles, the lack of evidence of harm for the majority does not excuse a growing disregard for the rights of those for whom trans-border dataflow could cause harm. Discrimination can occur to individuals when their personal data or profiles are transferred into the hands of hostile parties. That can happen through data breaches, criminal penetration of institutions, or even changes of regime which put the rights of individuals to freedom of political, religious, and sexual expression in jeopardy. Old data can become a new threat when placed in hostile hands.

TBDF has been a difficult problem to solve in law and policy; that fact has been proven over the past forty years. Laws have attempted to address the issue, but enforcement requires resources that have not been available. Law enforcement authorities have not had sufficient resources to deal with inter-jurisdictional serious organized crime or white collar crime, so getting resources to investigate and sanction transborder privacy breaches has been almost impossible. Development of the Budapest Convention, or Cybercrime treaty, took many years; there are still only 46 countries that have ratified since the Convention came into force in 2004. TBDF is one of the hardy perennials in this tangled garden of new information technologies. However, we remain optimistic that some of the ideas suggested decades ago can be usefully applied.

Some of these include:

- Accepted, harmonized international standards for data protection,
- Transboundary cooperation between data protection authorities,
- Development of mutual assistance treaties for prosecution of data related offences,
- Keeping data within Canadian jurisdiction where appropriate.

[39] http://www.worldprivacyforum.org/2014/04/wpf-report-the-scoring-of-america-how-secret-consumer-scores-threaten-your-privacy-and-your-future/.

We must exert more control over transborder dataflow if we hope to manage ubiquitous cloud computing and preserve our privacy rights. As we engage in the necessary work to create and strengthen international agreements to protect the privacy of individuals, it is crucial to remember that we are not there yet. The interim recommendation and prudent practice, in our view, must be to localize data within Canada, especially for particularly sensitive data such as private correspondence or communications internal to an organization.

Those who studied this issue in the 1970s and 1980s not only predicted the development and growth of these new networked technologies, they also correctly identified the risks of data captured by foreign governments and other non-state actors. We now understand that mass surveillance is actual practice. Legal reform and data localization were known to be privacy-protective solutions more than forty years ago; given the current legal contexts addressed earlier in this report, they appear to be the right choices now.

A Framework for Canadian Organizations Assessing the Privacy Risks of Extra-National Outsourcing

The complete framework document is available for download on our website: http://ecommoutsourcing.ischool.utoronto.ca/. It contains a fully documented process to follow and a set of key questions to ask, intended to assist Canadian organizations in assessing their data and privacy risks, especially those concerned with the privacy and security implications of their eCommunications outsourcing decisions. What follows is a brief summary of the framework.

In our framework, we help organizations to differentiate between the risks inherent in all communications systems, the risks in outsourcing, and the additional risks in outsourcing where data holdings are outside Canada, or otherwise subject to foreign control. This three-tiered approach investigates the following key risks:

1) Privacy Risks Inherent in all eCommunications Systems

- Accessibility of switching equipment to physical or logical intrusion,
- Data breach,
- Accessibility of servers, or "in the cloud", which really means in servers and back up servers, wherever those are located,
- The risk of deep packet inspection as messages transit networks,
- Transit of some external messages through foreign countries.

Potential mitigations for these basic risks include the following:

- Full, broadly scoped security threat risk assessments (TRAs) in meaningful consultation with implicated data subjects,
- Full, broadly scoped privacy impact assessments (PIAs) in meaningful consultation with implicated data subjects,
- Scanning of the systems for malware and other software threats,
- Traffic analysis and other types of network scanning to determine unusual patterns,
- Accreditation of eCommunications systems to ISO or equivalent standards,

- User training, to reduce exposure to malware, phishing attacks, interception, etc.
- Mandatory breach reporting,
- End to end encryption of messaging,
- Audits of server farms, help desk functions, data backups, system management, etc.
- Penalties for abuse.

2. Risks of Outsourcing: "Someone Else's System"

- Quality control for information management is outside the control of the organization.
- When eCommunications services are being offered at no charge, as a loss leader for other goals, the client has little to no leverage on the contractor.
- 'Vendor lock-in' risks are widespread in the IT industry.

Potential mitigations include the following:

- Contracts must cover all policy and legal requirements,
- Oversight and audit must be rigorous,
- An exit strategy in the event of price increases, changes in the management of the contractor, or sale or takeover of the division. How will the data come home? Will the metadata and log files be returned as well? Will the vendor retain copies?

3. Risks of Foreign Control of Outsourced Communications

- Contractor staff, operating in different or multiple jurisdictions (and languages), may be less familiar with the legal and policy regime in which the organization operates.
- Distance from the organization may decrease the sense of loyalty to the client.
- There is a now documented risk of mass surveillance by security agencies, and government actors who are interested in the data, not necessarily for criminal law enforcement.
- Foreign governments have reduced responsibilities to respect the rights of "aliens."
- Data protection and IP (intellectual property) law may not be enforceable in foreign courts.

Potential mitigations:

- Avoiding extra-national outsourcing,
- Contractor staff training,
- Keeping up to date lists of contractor staff who have access to the information,
- Require transparency reports on the rate of access of data, and notification of data subjects.

A Five-Step Framework for Understanding Your Organization's eCommunications Risk Profile

This is a brief summary of the five-step framework to guide those tackling the comprehensive risk assessment necessary prior to an outsourcing decision. We have omitted the detailed questions, which are in the complete framework document.

Step 1: ***Consider the full of range of data and metadata generated by your organization that is to reside outside of Canada.*** Here we give an example using types of digital data common in universities.

- Instructional correspondence, including assignments, draft and completed work;
- Library research, including catalogue search terms, documents and books downloaded, page reading list and sequence of pages read, time spent per page;
- Research, results of studies and trials, draft articles, trademark and patent applications;
- Discussions of an inherently personal nature such as personal circumstances, health issues, stress and psychological matters which interfere with work, etc.;
- Personal email between students/faculty and others of a social or romantic nature;
- Pictures, images, videos, scans or downloads of documents;
- Personal email used for everyday transactions such as banking, credit card information, travel, etc.;
- Date and timestamps of content creation and modification which reveal work habits;
- To/from email addresses which reveal social networks;
- Internet Protocol (IP) addresses which can reveal user location.

Step 2: ***Assess whether any data or metadata identified in Step 1 meet the definition of personal information with respect to your provincial jurisdiction's privacy legislation before proceeding with Steps 3-5.***

Step 3: ***Identify fully the nationalities of your eCommunications systems end users.***

For most organizations, end users in Canada will be Canadian citizens and permanent residents. Many Canadian universities will have a significant percentage of foreign nationals, be they on student visas, visiting or new faculty on work visas, or permanent residents.

Step 4: ***Identify the potential interest in the personal information by various actors:***

- Market competitors, law enforcement authorities, tax authorities.
- Personal enemies of an individual, or hackers and criminals.
- Security and intelligence authorities, particularly in the case of foreign students or faculty or those engaging in political activities which challenge prevailing policies or ideologies of the governments in relevant jurisdictions.

Step 5: Identify the ways in which your organization can protect the personal information of all of your end users in the face of lawful requests or illegal access attempts by the above actors identified in Step 3

Consider the extent of your organization's ability to act in:

- Your own location (i.e. "in house"),
- Within your jurisdiction (outsourced within in Canada),
- Within each foreign jurisdiction where your outsourced data may be stored or processed.

Engaging in a comprehensive exercise following the detailed questions in our framework document will help Canadian organizations to evaluate the appropriateness of extra-national outsourcing for the data and services in question.

Moving Forward: Protecting the Privacy of eCommunications.

Whether we think in terms of transborder data flows or outsourcing extra-nationally to "the cloud" it is time for Canadians to have a renewed conversation about the privacy of their digital data. Outsourcing may in fact be fine for some classes of data, but it is not privacy protective for personal information and particularly for archives of eCommunications conversations that would otherwise be primarily internal to an organization. Yet within Canada, only one provincial jurisdiction recognizes this risk for information in the custody of publically-funded bodies: British Columbia. BC would seem to be a model that other provincial jurisdictions could emulate.

However, there are now indications that at least one BC organization is looking to the "consent" provision in BC's FIPPA legislation, to permit university and college community members to access and use Microsoft's Office 365 extra-national cloud-computing Software as a Service (SaaS) product. Has the new technology effectively trumped our privacy expectations and rights? Has the move "to the cloud" so transformed the ways in which we work that there is no going back?

We think not. We can keep the technology; we just need much better laws and policies, along with much more effective enforcement, to shape and limit their use. Despite the image promoted by Hollywood movies and fiction writers on the subject of state surveillance, the historical record indicates that governments and large corporations of Western democracies prefer to operate within the law. The releases of classified documents about US state surveillance practices are so revealing because they showed the extent to which certain US laws, notably the *USA PATRIOT Act*, and the *FISA Amendments Act* of 2008, supported bulk surveillance of entire populations on an unprecedented, staggering scale. It is the legal framework and the associated funding which permits the surveillance.

Fortunately, citizens in constitutional democracies have tools at their disposal to rein in mass surveillance activities and to ensure that all organizations, public and private, do a much better job protecting the privacy of data in their custodial control and limiting the uses to which that data can be put. This includes legal and regulatory reform, with much tougher consequences for organizations who fail to meet their responsibilities. To

start, we need a vigorous public debate on the issue of privacy in the digital world. Election campaigns are excellent times to focus public attention on these issues.

In order for public debate to take place, voters will need accurate, accessible information. We hope this report and its associated appendices are a contribution towards filling this need. It is unreasonable to expect members of the public to be able to keep pace with a field that requires combined and extensive legal and technical knowledge. Practices that allow organizations to outsource services extra-nationally while retaining their institutional domain names make it very difficult if not impossible for the average user to know who has their data, and to make an informed decision.

We need to be able to rely on public institutions, universities and Privacy Commissioners to take leadership roles and continue to actively research these issues. Such a leadership role may be particularly challenging to undertake in provincial jurisdictions that have already outsourced parts of government operations such as Ontario. Or in Nova Scotia, for example, where the province is currently testing Google Apps for Education for use in all K-12 schools. But a change of direction is not impossible. The federal government contractually requires in-country storage for its eCommunications systems (now outsourced to Bell). Other provinces can require the same, as BC has done in its FIPPA legislation.

For the broader public sector's eCommunications needs, one model of particular interest is BC-Net. A not-for-profit consortium of BC's universities and research institutions, BC-Net offers IT services, such as off-site backup and video-conferencing, high-speed network connectivity, and bulk purchasing of hardware and software to its members, with prices thirty to fifty percent below market rates. BC-Net also develops IT capacity and shares knowledge amongst its members, so that even smaller schools can benefit from specialized IT expertise without requiring it in-house. Other jurisdictions could adopt a similar model. With the right vision, coordination, policy changes and an appropriate funding model, the higher education and/or broader public sectors outside of British Columbia could reap similar financial benefits while ensuring privacy protection for their eCommunications systems.

BC-Net has a well-defined governance structure, led by a Board of Directors comprised of representatives from its member universities and institutes. Although most of its funding comes from its members, BC-NET provides an option for vendor sponsorship

called the "Industry Partner Program," raising concerns that it is not truly vendor independent or appropriately arms-length. Platinum sponsors, (currently Microsoft, IPS Security Compliance Managed Services and Long View Systems) have at least recently received 30 minute keynote presentations at the annual conference and the opportunity to "collaborate with influential decision-makers in these communities, influence the development of technology standards, interact with IT professionals on emerging technology services and applications, and showcase emerging technologies at committee meetings." Platinum, Gold and Silver sponsors all receive an invitation to lunch with the CIOs of member universities and research institutes.[40]

Such relationships can be benign, as Universities, like all organizations, do need to build and manage relationships with vendors for purchasing needs. But such relationships can raise questions. On the 9th of April 2015 BC-NET announced a new "strategic alliance" with Microsoft through its reseller, Long View. The agreement, worth three million dollars, was for a sector-wide software licensing agreement between BC's higher education institutions and Microsoft products including Lync Unified Communications (voice and video over the Internet), SharePoint file storage and Office 365. Long View will oversee the deployment of Office 365 across BC-Net members.[41]

How will BC-Net get around the problem of its FIPPA restrictions with this outsourcing deal? They will need to use the "informed consent" clause in BC's FIPPA legislation. Users will be required to accept the risk of outsourcing if they wish to use the service. BC universities will likely have to provide an alternative for those who do not wish to use Office 365. We can hope that users will have access to better information than the flawed arguments which have supported outsourcing decisions at universities in other provincial jurisdictions. Lisa Austin and Daniel Carens-Nedelsky's full legal report "Why Jurisdiction Still Matters," (and available on our project website) contains an appendix which discusses the problem of relying on user consent in this way.

Public awareness of state surveillance activities has certainly escalated since 2013; the member states of the European Union have been particularly vocal about data sovereignty issues, and the protection of private and confidential data. US

[40] BC Net, "Industry Partner Program, 2015-2016," https://www.bc.net/sites/default/files/uploads/documents/2015/2015BCNETIndustryPartnerProgramBrochure3.pdf.
[41] https://www.bc.net/bcnet-higher-education-members-unite-establish-sector-wide-strategic-alliance-microsoft.

headquartered, multi-national vendors are responding. IBM, Microsoft and SAP, for example, have recently announced the construction of new data centres in Canada, specifically to address data sovereignty issues.[42] There are Canadian-owned companies who also provide in-country cloud services, including Stage2Data, CloudA, Cogeco, CaCloud and many others, and use data-sovereignty as a selling point. Other cloud computing companies have critiqued this approach. These critiques come from companies offering up their own privacy-protective solutions for using the cloud, such as secured gateways to permit encrypted access to third party services like Salesforce and Office 365.[43] While these secured gateways address some privacy concerns; they are not a complete solution, because they cannot secure metadata. Data sovereignty and data control are very much hot topics in the global Information Technology sector, with billions of dollars and significant market share at stake.

In the course of our research, we identified many other areas of concern that were beyond the scope of our project—which focused on the implications of extra-national outsourcing of eCommunications—that urgently require additional research. In general we feel a much larger research project on the privacy implications of transborder data flows more generally would help to address these issues. One of the most pressing questions raised in our project is the "Microsoft Ireland" case currently under appeal. It raises troubling questions about the potential extra-territorial reach of US law into other countries. The recent openings of data centres by US headquartered companies within Canada are offered as alternatives that provide real data sovereignty and control. The Microsoft Ireland case suggests otherwise. However, the issue is complicated and the implications are not clear at this point. The issue deserves its own longer treatment and analysis. It would be inappropriate to make any definitive conclusion about the risk of outsourcing within Canada to subsidiaries of US companies. However, we strongly

[42] "IBM Opens for SoftLayer Data Centre in Canada, 12 August 2014, http://www.newswire.ca/en/story/1397074/ibm-opens-first-softlayer-data-centre-in-canada; "Data centres proliferating in Canada as companies play catch-up amid security concerns," Financial Post, 25 August 2014, http://business.financialpost.com/fp-tech-desk/cio/data-centres-proliferating-in-canada-as-companies-play-catch-up-amid-security-concerns; Shane Dingman, "Microsoft to build two data centres in Canada as it expands cloud services," *The Globe and Mail*, 2 June 2015, http://www.theglobeandmail.com/technology/microsoft-to-build-two-data-centres-in-canada-as-it-expands-cloud-services/article24756853/.

[43] This is not an endorsement of any of these companies, either Canadian or multi-national. These names are provided solely to illustrate the point that data sovereignty concerns are being addressed by cloud companies, and are increasingly being understood as important to customers. Organizations should undertake their own independent investigation into cloud-service vendors.

recommend that organizations contemplating outsourcing bear this risk in mind, support additional research into this question and keep a close eye on this case.

The rush to use hosted-services in the global cloud raises other privacy-related questions that were also outside the scope of this project, but also urgently need further research. To what uses are our personal data being put? How effective are our existing audit and regulatory regimes at ensuring compliance with privacy legislation even for data stored within Canada? Note that our legal analysis of case law and statutes focused on the United States. What are the privacy implications for storing data in other jurisdictions? What are the privacy implications for an organization or for members of an organization whose data is stored in the European Union? In China? In Russia? We only considered eCommunications in the global cloud. What are the privacy implications for other types of cloud-based hosted services: human resources management tools, camp registrations for children (especially where medical information is included), applications for hunting and fishing licenses, to give but a few examples?

In the vendor contracts we noted a lack of clarity around the question of metadata. Is metadata in fact Customer data? Who owns the data generated by users in the course of using the software? Are companies in fact free to mine that data and/or sell that data to third parties? Will the Internet of Things bring fresh threats to this situation?[44] When a customer ends their contractual relationship with the vendor, is the metadata returned along with the customer data? Does the vendor get to retain copies? These questions are unanswered.

We also observed the growing global trend among both K-12 education and institutions of higher learning to outsource their eCommunications to either Microsoft or Google. What are the long term privacy implications of doing so? What will it mean for a child born now to have records of their entire educational experience, including records of all their schoolwork ever completed online, as well as their reading habits and learning patterns, stored in the global cloud under the control of one of two major international corporations? Students at present do not choose post-secondary education based on whether a university or college is a "Google" school, or a "Microsoft" school. But in the

[44] The "Internet of Things" is the term to describe the increasing number of devices in our homes (and even our cars) that can be accessed over the global Internet.

future, will they? What happens to the data if a company from a nation that is not one of our trade allies buys the service provider?

As the history of transborder dataflow reveals, TBDF is not a new concept, nor are the privacy and sovereignty issues we have identified. However, the scope and the scale of digital data production and shipment of the last decade have been difficult for non-specialists to grasp. As we continue to grapple with the rapid pace of technological change and the corresponding impact on our privacy, there are privacy-protective actions that have or can now be taken. Experts in the privacy field are already rethinking their support for extra-national outsourcing decisions based on new evidence.[45] Network security experts are pursuing stronger, usable end-to-end encryption techniques. Changes to Internet traffic patterns required by regulation would keep domestic traffic within Canada.

For the present, we advise Canadian organizations who have not yet outsourced extra-nationally to think carefully about doing so. It should go without saying that organizations and individuals must be skeptical of vendor claims, and do their own thorough due diligence with respect to contracts, license agreements and terms-of-use. To ensure protection for the data of Canadians in this rapidly expanding digital world, we also need to place our surveillance agencies under greater scrutiny, rethink recently passed legislation including Bill C-51 – the *Anti-terrorism Act, 2015*, ensure much better enforcement of our existing privacy laws, provide more resources to the oversight agencies, and promote vigorous public discourse on privacy risks in the context of trans-border data flow and data mining.

Sustained public pressure is now required to encourage our politicians, organizations and corporations to act with renewed vigour on our behalf.

[45] Lisa M. Austin, Heather Black, Michael Geist, Avner Levin and Ian Kerr, "Our data, our laws" *The National Post* (12 December 2013), http://news.nationalpost.com/2013/12/12/our-data-our-laws.

Conclusion

Canadians have a right to privacy of their personal information, which includes their correspondence in whatever form.

This right to privacy is protected in federal and provincial privacy statutes, which the Supreme Court has repeatedly characterized as "quasi-constitutional" because of the fundamental role played by privacy in preserving a vibrant democracy. Other sources of protection include tort law and numerous international instruments.

Cloud-computing vendors of software, platforms and infrastructure, on the other hand, need customer organizations to believe that jurisdiction does not matter when it comes to protecting the privacy of data.

"The cloud" as a marketing concept is certainly an effective one. Cloud-computing technologies offer real benefits to organizations, but their use comes at significant costs.

We find ourselves increasingly asked to trade our privacy rights to vendors in order to obtain goods and services, or even to interact with publicly funded bodies including Canada's education sector.[46]

More research is needed on an ongoing basis to assess privacy risks associated with these new technologies. Legal and regulatory reform is required to push back against these intrusions.

Although we have drawn extensively in this report on the examples of universities outsourcing to either Microsoft or Google, the issues we have raised are not limited to these vendors alone or to the higher education sector.

The crucial points are these:

a) Where data resides and transits, and under whose control, determines what legal protections it has from the actions of third parties.

[46] "What can be done?" blog entry for The New Transparency Project, http://www.surveillanceincanada.org/trends/what-can-be-done. See the report of the project: Colin J. Bennett, Kevin D. Haggerty, David Lyon, and Valerie Steeves, eds., *Transparent Lives: Surveillance in Canada* (Athabasca University Press, 2014).

b) We do not live in a borderless world. The similar risk argument is deeply flawed. Canadians do have better legal protection when their data remains within Canadian jurisdiction.

To assist Canadian organizations who are either contemplating extra-national outsourcing or who now wish to undertake a review of a previous outsourcing decision, we have developed a comprehensive privacy impact assessment framework that takes into account the findings of our research. This framework is available for download as a pdf file on our website: (http://www.ecommoutsourcing.ischool.utoronto.ca),

Readers will also find additional resources there, including archived webcasts of two public events: one organized by Andrew Clement in November 2013 prior to the study period of our grant, and the second on March 6, 2015, where we presented our preliminary findings to an audience that including privacy officers and senior Information Technology staff from the Canadian University sector.

We need a much broader policy debate, both within Canada and internationally, to ensure that the benefits of new communications technologies do not come at the cost of losing the human rights we fought so hard for in the last century. We encourage readers of this report to become engaged with these issues we have discussed here, and press politicians at all levels for legal reform and better public policy.

Recommendations

Introduction

We propose these recommendations based on our research into the outsourcing of eCommunications by universities. We believe they apply broadly to public institutions and indeed to some organizations in the private sector who handle the sensitive personal data and communications of their clients as well as to outsourcing of services to the cloud beyond eCommunications.

In this increasingly digital world, greater efforts must be made to protect personal information, and to ensure that individuals retain the ability to control their own records and determine the uses to which that information will be put. We echo the Supreme Court of Canada's argument that, "the importance of the protection of privacy in a vibrant democracy cannot be overstated."[47]

In making these recommendations we recognize some of the pressing opportunities and constraints that have encouraged decisions to outsource:

- Many new technologies are only available as cloud services; furthermore those services are desirable, enhancing productivity and collaboration;
- The Internet is constantly changing and threats/risks evolve rapidly;
- Public institutions are all subject to serious cost containment pressures; some cloud services are being offered at considerably lower or no cost, an attractive inducement;
- The risk of harm to individuals from data mining and profiling is not well understood in privacy risk management, and certainly not by the individuals subject to it.

The media attention given to the disclosures of US state surveillance activities in the past two years have helped us understand these new risks, from weakening of encryption standards, malware attacks and espionage, to intrusion on civil liberties and undermining of democratic institutions. We now know that the similar risk argument is deeply flawed; the export or routing of data outside of Canadian jurisdiction exposes

[47] *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*, 2013 SCC 62.

sensitive information to many kinds of intrusion and deprives Canadians of constitutional protection.

This is not to dismiss well-founded concerns about the risks from mass surveillance conducted by the Communications Security Establishment of Canada (CSE), the Canadian signals intelligence counterpart of the NSA. Nevertheless, the CSE is required to operate within Canadian legislation and constitutional bounds. If these laws are not appropriate or not being followed, Canadians have much more effective means for remedying the situation than if the surveillance is conducted outside Canadian jurisdiction.

There are specific actions that can be taken to improve data protection and privacy in Canada. Based on the research conducted for our report we therefore make the following recommendations:

1. ***Recommendations for Canadian Organizations***

1. Canadian organizations should not outsource eCommunications services beyond Canadian jurisdiction until adequate measures for ensuring legal and constitutional protections equivalent to those in Canada are in place.

2. When considering eCommunications options, including outsourcing, organizations should conduct thorough and transparent Privacy Impact Assessments (PIAs) and Threat Risk Assessments (TRAs), taking into account constitutional and other protections provided under Canadian law, as well as the risks of using services hosted in foreign jurisdictions. The "similar risk" assertion should no longer be used in PIAs to support extra-national outsourcing.

3. In keeping with best privacy practices around openness and transparency reporting, organizations should proactively publish their current policies and practices regarding third party requests for personal, confidential and other sensitive data. They should systematically log third-party requests and disclosures, and to the extent permitted by law regularly publish detailed statistics about them.

4. Where Privacy Impact Assessments and Threat Risk Assessments have already been conducted, they should be updated annually to reflect changes in the threat and risk landscape.

5. In the interests of transparency, organizations should make their Privacy Impact Assessments, Threat Risk Assessments and Vendor Terms of Use of cloud-based services publicly available online.

6. Organizations should keep local data local where feasible. They should consider forming or joining regional networks, providing cloud-computing services that can keep data within appropriate jurisdictional boundaries where feasible. For regional and domestic internet transit, they should peer (exchange data) at local public internet exchange points (IXPs) within Canada.

2. Recommendations for Organizations Who have Already Entered into Extra-National Outsourcing Contracts.

1. Organizations that have already outsourced to companies that may place data outside Canadian jurisdiction should revisit these decisions in light of the deeply flawed "similar risk" argument and what is now known about, for example, mass surveillance practices in the USA. Organizations should consider the risk of similar practices occurring in other countries.

   In the meantime, organizations should:

   a. Not use extra-national outsourced eCommunications systems for communicating personal, confidential or other sensitive information;

   b. Ensure that all users are appropriately informed about the specific risks of extra-national outsourcing, and reminded about the risks on an ongoing basis;

c. Immediately update any FAQ documents posted online purporting to give users advice about the risk of storing, routing or otherwise exposing their data to foreign jurisdictions to ensure their language is accurate and does not contain the faulty "similar risk" or "email is inherently insecure" arguments;

d. Offer reliable, alternative, locally hosted services.

3. Recommendations for Canada's Public Universities

1. Universities providing eCommunications services for their members, in keeping with their academic mission and to uphold the principle of academic freedom, should recognize that they have a responsibility for ensuring these services offer greater levels of privacy and security than are generally available to consumers.

2. In keeping with their responsibilities for advancing the public interest, Canada's public universities should play a leadership role in providing research and policy development in the field of transborder dataflow.

3. Universities should continue to support and where needed enhance local IT services as a means of maintaining control over their eCommunications activities and archives.

4. Recommendations for Legislators

1. To enhance and clarify data protection across Canada, we encourage legislators to actively engage in law reform in the area of transborder dataflow.

2. To reduce the transit of domestic Internet traffic through the US and therefore to capture by the NSA's UPSTREAM program, legislators should enact requirements that telecommunications carriers route domestic Internet traffic within Canada, such as via public Internet exchange points (IXPs).

5. Recommendations for Privacy Commissioners

1. Privacy Commissioners who have previously accepted the "similar risk" argument in relation to protection of Canadian's personal information under US jurisdiction should revisit their position in light of the legal arguments and findings presented in this report and its appendices.

2. Privacy Commissioners should encourage organizations to reduce the risk of domestic Internet traffic being routed through the US by strongly recommending that organizations route Internet traffic (peer) within Canadian jurisdictions, such as at public Internet exchange points (IXPs).

This page intentionally left blank.

Appendices (listed here, available for download)

http://ecommoutsourcing.ischool.utoronto.ca/

A. Heidi Bohaker and John M. Dirks, "Privacy Impact Assessments and Microsoft & Google Vendor Contracts: Examining Canadian University eCommunications Outsourcing Decisions;"

B. Lisa Austin and Daniel Carens-Nedelsky, "Why Jurisdiction Still Matters;"

C. Andrew Clement and Jonathan Obar, "Canadian Internet 'Boomerang' Traffic and Mass NSA Surveillance: Responding to Privacy and Network Sovereignty Challenges;"

in Michael Geist (ed), *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, University of Ottawa Press, 2015, pp 13-44, available for free, open access download at http://www.press.uottawa.ca/law-privacy-and-surveillance or http://hdl.handle.net/10393/32424.

D. Stephanie Perrin, "Transboundary Challenges to Privacy Protection;"

E. Stephanie Perrin, with Heidi Bohaker & Andrew Clement, "A Framework for Canadian Organizations Assessing Privacy Implications for Extra-National Outsourcing of eCommunications Services;"

F. For Further Reading: An Annotated Bibliography (Susan Colbourn, with contributions from Daniel Carens-Nedelsky and the project team).

About The Project

The authors of this report first came together on the privacy implications of extra-national outsourcing in the fall of 2013, when our organization, the University of Toronto, proposed migrating faculty and staff eCommunications to the Microsoft Office 365 platform. Prior to the initial June 13, 2013 revelations of Edward Snowden about the extent of bulk surveillance capture and retention of digital data by the United States' National Security Agency (NSA), we were like most people, using free web-based email services for personal communication, and other services for file-sharing, project-management, and social media. Such free services were certainly compelling and the productivity potential of the new platforms was enticing.

Then our University proposed outsourcing faculty and staff eCommunications to a US multi-national provider.[48] Student email had been outsourced two years earlier and many of us were not even aware at the time that it was to an extra-national provider. We knew that other universities, corporations and provincial governments were outsourcing specific eCommunications and other web-based services to industry-giant multi-national cloud-based providers. But we had questions and concerns about the implications for the privacy of our data when stored extra-nationally. Was our privacy really better protected when our eCommunications archives were stored extra-nationally with either Microsoft or Google than with an in-house solution? Was the risk of state surveillance effectively the same when data was stored in or transiting, in the US, rather than in Canada? Was the *USA PATRIOT Act* a red herring?

In response, Andrew Clement organized a "teach-in" on the issue in November of 2013; invited speakers included the University of Toronto's CIO, the president of the Canadian Association of University Teachers, and the late Caspar Bowden, Microsoft's former Chief Privacy Strategist for Europe, among others. The day-long forum and presentations (now available as archived webcasts on our project website) all underscored the urgent need for more research. These questions led to this research project, funded by a 2014-2015 Contributions Program grant from the Office of the Privacy Commissioner of Canada, which has resulted in this report.

---

[48] Lisa Austin served as a member of the Faculty & Staff e-Communications Consultation committee who were asked to consider "core expectations for faculty and staff e-Communications services" related to extending the Office 365 student email service to faculty and staff. The final report of the committee is available here: http://main.its.utoronto.ca/wp-content/uploads/2013/09/Faculty-and-Staff-eCommunications-Advisory-Committee-Final-Report-August-2014.pdf.

About the Authors

Associate Professor Heidi Bohaker, *Principal Investigator*
Department of History, Faculty of Arts and Science
Professor Heidi Bohaker is Associate Professor in the Department of History at the University of Toronto. She has a broad interest in the types of archives and categories of information both states and non-state societies kept and keep about their people. She is a practitioner of the digital humanities, exploring how to best use new technologies in collaboration with Great Lakes First Nations to reconnect people with aspects of their cultural heritage stored in museums and archives around the world.

Associate Professor Lisa Austin, *Co-investigator*
Faculty of Law
Professor Lisa Austin is Associate Professor in the Faculty of Law at the University of Toronto and a member of the Bar of Ontario. Her research and teaching interests include privacy law, property law, and legal theory. Her privacy work has been cited by various Canadian courts, including the Supreme Court of Canada (in *R v Spencer*, *R v Fearon*, *R v Wakeling*). Prior to joining the faculty, she served as law clerk to Mr. Justice Frank Iacobucci of the Supreme Court of Canada.

Professor Andrew Clement, *Co-investigator*
Faculty of Information
Andrew Clement is Professor Emeritus. He coordinates the Information Policy Research Program and co-founded the Identity Privacy and Security Institute (IPSI) at the Faculty of Information. He has had longstanding research and teaching interests in the social implications of information/communication technologies and participatory design.

Stephanie Perrin
Stephanie Perrin is a doctoral candidate at the University of Toronto, Faculty of Information. Her research focuses on privacy issues at the Internet Corporation for Assigned Names and Numbers (ICANN). She is recognized as an international expert in privacy and data protection and has served in several positions in the Canadian Government, including as Director of Research and Policy in the Office of the Privacy Commissioner, and as Director of Privacy Policy at Industry Canada where she was responsible for managing the development of the private sector privacy legislation, the Personal Information Protection and Electronic Documents Act (PIPEDA), and the CSA standard that preceded it.

Project Research Assistants and Contributing Authors

Andi Argast

Andi Argast is a strategist, writer, and researcher working at the intersection of digital technology and non-profit organizations. Her background is in marketing and communications; she holds a Master of Information from the University of Toronto and a Bachelor of Journalism from Carleton University. Andi's research and work focuses on digital advocacy, community engagement, open data, and media literacy.

Daniel Carens-Nedelsky

Daniel Carens-Nedelsky is a second year law student at the University of Toronto. He received an Hon. Bachelor of Arts and Science from the Arts & Science Program at McMaster University, and MA in Philosophy from the Institute for the History and Philosophy of Science and Technology at the University of Toronto. He works as Research Assistant for Professor Lisa Austin, exploring the legal regimes in Canada and the US regulating governmental access to Canadians' electronic information.

Susan Colbourn

Susan Colbourn is a PhD Candidate in History at the University of Toronto and is a Junior Fellow at the Bill Graham Centre for Contemporary International History. Her dissertation, tentatively titled "Out of Area? The North Atlantic Treaty Organization and the Collapse of Détente, 1951-1983," examines the alliance's response to the gradual unravelling of superpower détente. Prior to her Doctoral studies, Susan completed an MA in History of International Relations at the London School of Economics and Political Science (2011) and an Hon. BA in History and International Relations at the University of Toronto (Trinity College, 2009).

John M. Dirks

John M. Dirks completed his PhD in History at the University of Toronto in 2014. Specializing in Canadian and American diplomatic history, his dissertation "Managing a Cooperative Disagreement: Canada-United States Relations and Revolutionary Cuba in the Cold War, 1959-1980," explores the cooperative dimension of Canadian-United States relations regarding Castro's Cuba despite fundamental disagreements in approach. Prior to his Doctoral studies, John studied at Queen's University and at the University of Toronto's Faculty of Information. He worked for 18 years at the Archives of Ontario, holding numerous positions as a professional archivist, manager and policy

analyst, in the latter role he dealt with electronic records management and digital preservation.

Jonathan A. Obar
Jonathan Obar is Assistant Professor in the Faculty of Social Science and Humanities at the University of Ontario Institute of Technology. He also serves as a Research Associate at the Quello Center for Telecommunication Management and Law at Michigan State University. He received his PhD from Pennsylvania State University. Dr. Obar has published research in a variety of academic journals about the relationship between digital media technologies, ICT policy, and the protection of civil liberties.

Dawn Walker
Dawn Walker is a Master of Information student at the University of Toronto's Faculty of Information specializing in Information Systems and Design. Her research interests include community-led infrastructure development and responses to surveillance. Prior to her current studies, Dawn completed an Hon. BA in History and Philosophy at the University of Toronto (Woodsworth College, 2009).

Selected References

Archives
The Snowden Surveillance Archive, https://snowdenarchive.cjfe.org.

Edited Collections and Monographs
Colin J. Bennett, Kevin D. Haggerty, David Lyon, and Valerie Steeves, eds., *Transparent Lives: Surveillance in Canada* (Athabasca University Press, 2014).

Geist, Michael, ed. *Law, Privacy and Surveillance in Canada in the Post-Snowden Era,* University of Ottawa Press, 2015.

Mosco, Vincent. *To The Cloud: Big Data in a Turbulent World*. Paradigm Publishers, 2014.

Woodcock, Bill & Benjamin Edelman. *Toward Efficiencies in Canadian Internet Traffic Exchange*. Canadian Internet Registration Authority (September 2012).

Reports
British Columbia**,** Office of the Information and Privacy Commissioner**. *Privacy and the USA PATRIOT Act, Implications for British Columbia Public Sector Outsourcing,*** by David Loukedelis. Victoria, 2004. https://www.oipc.bc.ca/special-reports/1271**.**

British Columbia Freedom of Information and Privacy Association (FIPA)**.*The Connected Car: Who is in the Driver's Seat? A study on privacy and onboard vehicle telematics technology,*** by Phippa Lawson. Vancouver, 2015. https://fipa.bc.ca/wordpress/wp-content/uploads/2015/03/CC_report_lite.pdf.

Public Safety Canada**. *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada*.** Ottawa, 2010**.** http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx.

United States of America, Department of Commerce, National Institute of Standards and Technology. "The NIST Definition of Cloud Computing" by Peter Mell and Timothy Grance. Special Publication 800-145. Washington: September 2011. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

Websites
Transparent Lives: Surveillance in Canada: http://www.surveillanceincanada.org/.

Internet Exchange Mapping (IXmaps) https://IXmaps.ca.

For more information visit:

ECOMMOUTSOURCING.ISCHOOL.UTORONTO.CA