Privacy Impact Assessments and Microsoft & Google Vendor Contracts: Examining Canadian University eCommunications outsourcing decisions.

Heidi Bohaker & John Dirks.

Introduction

How does a study of university outsourcing decisions contribute to a broader conversation about the privacy implications of using extra-national eCommunications services? As with the recent and burgeoning adoption of "cloud technologies" in all areas of the economy, eCommunications outsourcing in the education sector is a significant global trend, not only for universities, but also for colleges and the K-12 level. ECommunications outsourcing affects many millions of students, staff and faculty around the world. Many Canadian universities are moving to the Cloud, turning either to Google or Microsoft as the providers of their eCommunications services.

Our study examines the phenomenon of Canadian university eCommunications outsourcing and puts the very recent trend of using such cloud-based services in historical context. The authors of this report are both historians, and John Dirks is also a trained archivist formerly with the province of Ontario. Our professional experience and training gives us a particular perspective on eCommunications systems. We see products such as Microsoft Office 365 and Google Apps for Education/Business as much more than communication tools. They are in fact digital archives that contain not only significant personal information belonging to individuals in their user accounts, but are also in fact a comprehensive digital archive of the organization as a whole, comprising complete records not only of external conversations, but of internal ones as well.

As historians, we are trained to see patterns in textual information and to read the implications of conversations between people through their correspondence. But when correspondence becomes digital, and when that digital correspondence is paired with other types of digital data, sophisticated search engines and data analysis tools can find information and makes connections far more quickly than a human can, making it possible to interpret the present as much as the past.

Given the level of sensitivity of the information contained within eCommunications systems, why are so many organizations, including universities, willing to place their digital archives outside of their control with third-party vendors who store that data in the global cloud? By examining the decisions of some of Canada's largest and leading provincial universities to outsource their eCommunications and the contracts signed with these vendors, we have been able to identify a set of problematic assertions that have served to rationalize extra-national outsourcing and the confluence of factors that have led those assertions to be accepted uncritically to date.

Heidi Bohaker and John M. Dirks, "Privacy Impact Assessments and Microsoft & Google Vendor Contracts: Examining Canadian University eCommunications outsourcing decisions," June 30, 2015. This analysis was prepared as part of a research project funded by the Office of the Privacy Commissioner of Canada's 2014-2015 Contributions program "Assessing the Privacy Risks of Extra-National Outsourcing of eCommunications" and forms Appendix A of the final public report. The complete project findings and recommendations are available at http://ecommoutsourcing.ischool.utoronto.ca/.

These ideas include the widely circulated but false notion that the data of Canadians and permanent residents faces a "similar risk" of access by government agencies regardless of whether that data is hosted in Canada, the United States, or in another national jurisdiction. Because of the legal analysis of Lisa Austin and Daniel Carens-Nedelsky in their report "Why Jurisdiction Still Matters," we now know that extra-national hosting and transiting of eCommunications data belonging to Canadians and permanent residents exposes that data to significantly greater privacy risks than if their data were hosted in Canada.[1] In addition to the "similar risk" argument, other widespread fallacies were also used, including the false analogy that "email is like a postcard" or is "no more secure than a postcard" and the false equivalency of privacy and security issues. Although a third party may be better able to handle security issues, they may be in a far worse position to deal with privacy issues. Equating privacy and security leads to the false conclusion that better security means better privacy protection.

The vendor contracts/license agreements we received likewise raised privacy concerns. By examining a set of such contracts, we were able to identify specific clauses that raise significant questions about the ability of the vendors to adequately protect the privacy of Customer data and metadata when it is stored in the global cloud, particularly from third party or law enforcement/government requests of foreign countries. As much as these vendors employ industry best practices to prevent and detect unlawful access to data, the contracts are quite clear about the requirements of the vendor to comply with the lawful requests of government agencies of countries in which they are operating.

As Lisa Austin and Daniel Carens-Nedelsky show, the standards under which governments and government agencies can lawfully request access to the data of a Canadian or Canadian resident are much lower when that data is stored outside of Canada. The standards by which the U.S. government can access the data of "non-US" persons would be unconstitutional if applied by the Canadian government to Canadians whose data was stored in Canada. Furthermore, the scope of the "foreign intelligence" information that can be gathered under US law about non-US persons is much broader, and goes far beyond seeking information about "actual or potential attack or grave hostile acts of a foreign power" to include "information with respect to a foreign power or foreign territory that relates to…the conduct of the foreign affairs of the United States."[2] Not only does this definition effectively legitimate political surveillance of the data of non-US persons, because of the extent of the information released by Edward Snowden beginning in 2013 we now know that bulk surveillance of data stored in or transiting the USA is occurring, and on a massive, unprecedented scale.

While the United States is the "primary" region of data storage for both Microsoft and Google, the contracts that universities signed with these vendors indicate that Customer Data can be stored in any country in the world in which these countries do business, making the data of Canadians stored in those jurisdictions also vulnerable to "lawful requests" of government agencies there. Some of these concerns were raised or noted in the Privacy Impact Assessment documents completed by some of the

[1] This statement is based upon the full legal analysis produced for this project. See Lisa Austin and Daniel Carens-Nedelsky, "Why Jurisdiction Still Matters" http://ecommoutsourcing.ischool.utoronto.ca/.

[2] This is the provision in section 702 of the *Foreign Intelligence Surveillance Act Amendments* Act of 2008.

universities, but these concerns did not affect the decision by the university to sign with the outsourcing provider.

The focus of this report is on the outsourcing decisions of Canadian universities, and includes discussion of the potential impact of such extra national outsourcing on the teaching and research missions of Canadian public universities which are to serve the public good, and on the principle of academic freedom. In presenting our findings here, our intention is not to single out any specific Canadian university for criticism, but rather to draw attention to the confluence of factors behind these extra-national outsourcing decisions that reflect ideas in circulation well beyond the academy. Because of this, many of the findings presented here will also be relevant for other Canadian organizations that have either already outsourced extra-nationally or are still considering the option. In exploring the erroneous assumptions behind extra-national outsourcing decisions to date, it is first necessary to understand the metaphorical power of "the cloud" as a false analogy that effectively masks the national jurisdictions in which the software, servers and networks that comprise these systems operate.

eCommunications in the Global Cloud[3]

Another way to talk about extra-national outsourcing of eCommunications is to use a short hand of "moving to the Cloud" or "moving to the Global Cloud." But what is the Cloud in this context? What are the benefits to universities of using "cloud" technologies for their eCommunications services? What are the risks? 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 either 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. Microsoft's Office 365 and Google's Apps for Education, Business and Government products are "Software as a Service."

Organizations, including universities, 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

[3] A slightly expanded version of this section also appears in the public summary report "Seeing Through The Cloud: National Jurisdiction and Location of Data, Servers, and Networks Still Matter in a Digitally Interconnected World," available for download on the project website: http://ecommoutsourcing.ischool.utoronto.ca/.

(known as 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.[4] These organizations using private and community cloud can secure their eCommunications through geographically-separate servers through the use of encrypted end-to-end connections (VPN or virtual private network). Cloud technology services do not by definition have to be extra-national, with data travelling 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.[5]

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 technology infrastructure is located. 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.

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 are stored 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.[6]

Furthermore, in each case, in the development of the international postal system, the telegraph system, and the international phone system, the privacy of communications were not guaranteed. The privacy rights that we expect now with our postal system in Canada, the USA, the United Kingdom and in other Western democracies, actually emerged slowly over the eighteenth and nineteenth centuries. During the eightieth century in the United Kingdom and in the American colonies people faced an intrusive Crown that authorized the opening of mail with impunity from or to anyone suspected of engaging in opposition or potentially seditious political activities. The British government had a secret office attached to its postal office that was tasked with opening mail and collecting intelligence. Seals had been used keep contents from prying eyes, but wax seals often broke in transit. In an era when paper

---

[4] 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.

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

[6] 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.

was still expensive, the envelope was invented from the initial idea of wrapping an extra sheet of paper around a letter, a cover, as a privacy protective measure. Legal reform over more than a century was required to create and then enshrine the principles we in Western democracies now take for granted.[7] And further reforms were required when new technologies such as the telegraph and telephone were developed. But these privacy principles were not universally recognized, and are certainly not guaranteed in many countries today where information technology companies operate.

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."[8] Or we need to add, vulnerable *en route* or if the data 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.[9]

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."[10] 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.

---

[7] Anuj C. Desai, "Wiretapping Before the Wires: The Post Office and the Birth of Communications Privacy," *Stanford Law Review* Vol. 60, Issue 2 (Nov. 2007): 553-594; Colin Agur, "Negotiated Order: The Fourth Amendment, Telephone Surveillance, and Social Interactions, 1878-1968." *Information & Culture: A Journal of History*, Vol. 24, No. 4 (2013): 419-447.

[8] 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.

[9] There is some intriguing work on the use of newer technologies (such as homomorphic encryption) which seek a general solution to this problem.

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

Both Microsoft and Google, as leading providers of eCommunications solutions globally, 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 the vendors, their subsidiaries, their affiliates, or their subcontractors have facilities, (except the US embargoed countries, typically listed explicitly in contracts and at time of writing consisting of Cuba, Iran, Syria, North Korea, Myanmar (formerly Burma) and Sudan).[11] Some of the world's largest cloud computing data centres, even so-called "cloud cities," are also now in China, for example, a country without the protections for individual rights including privacy rights afforded in constitutional democracies.[12] Global data centre traffic has been projected to grow to 8.6 zettabytes (ZB) by 2018, up from 3.1 ZB in 2013.[13] The global education eCommunications market sector, now dominated by Microsoft and Google, is but one sector of a much larger and rapidly growing global cloud economy.

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 transiting through or stored within their borders. For particularly sensitive classes of data, including those most in need of privacy protection such as an organization's complete archive of eCommunications, the jurisdiction and location of data, servers and networks are crucial considerations. And yet as the services available in the global cloud market have developed and matured over the past decade, the implications of such extra-national outsourcing have not been rigorously considered.

Microsoft, Google, and a Brief History of the Global Education eCommunications Market

Microsoft and Google are the two main providers of eCommunications services to the global higher education and K-12 markets, through their Microsoft Office 365 and Google Apps for Education products. Each vendor provides their service "free of charge" to qualifying educational institutions and with significantly reduced rates for additional enterprise–level cloud eCommunications products. They are also the overwhelming choice of the Canadian University sector. Both of these products allow customers to maintain their own domains (e.g. @lakehead.ca, @utoronto.ca) while the data resides on the vendor's servers, wherever they are located.[14] Both Microsoft and Google offer their Software-as-as-Service eCommunications platforms in the global public cloud; the data however resides on servers

[11] See Agreement between Google Apps for Education and the University of Alberta, December 2010, section 1.2. Released under FIPPA 2015-01, which list the prohibited countries under US Foreign Assets Control legislation as being Cuba, Iran, Myanmar, North Korea, Syria and Sudan.
[12] Mosco, *To the Cloud*, 72-74.
[13] A zettabyte is 1 trillion gigabytes. The forecast data comes from Cisco, Incorporated's Global Cloud Index white paper. http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.html .
[14] This option of retaining one's domain name while providing a service on another company's server is not a feature unique to Microsoft or Google's products; other eCommunications and cloud vendors can provide this service as well.

owned or leased by these companies or their subsidiaries, subcontractors or affiliates, under their respective controls.

The use of email systems at Canadian universities dates from the 1970s when universities began to provide email to their staff, faculty and students (initially in computer science and the computationally-heavy disciplines) through on-campus systems, either with commercial or open-source software solutions, along with other locally provided software productivity tools. With such platforms, the complete archive of digital data produced by these institutions remained on their premises, under the control of their IT staff and within Canadian jurisdiction, even as some (but certainly not all) email messages produced by faculty, staff, and students travelled across computer networks to their many destinations around the world.

In the last decade, the development and widespread use of cloud-based suites of integrated eCommunications, calendaring and other productivity tools offered on the Software-as-a-Service (SaaS) cloud computing model has fundamentally changed the way organizations manage information by separating the location of the physical workspace from the virtual one. For the many universities around the world who have already adopted this model, the link between the physical campus and the digital campus has been severed. Such a division is obvious for online universities; much less so for traditional ones whose identities are tied to their geographical location. With integrated eCommunications and productivity suites, the options have effectively narrowed to Microsoft or Google, making their data centres the archives for many of the world's educational institutions. Such repositories contain not only email archives, but also much other digital content: documents, spreadsheets, presentations, and voice and video records containing sensitive research files, intellectual property, student grades and other confidential information.

Over the past decade, both Microsoft and Google have successfully competed for market share in the global K-12 and higher education sectors by offering these services free of charge for students, staff and faculty. Interestingly, some of the world's top research universities have been slowest to embrace the trend.[15] Microsoft entered the free-for-all web-based email service in 1997 with the acquisition of Hotmail. In 2005, Microsoft entered the education eCommunications sector by rebranding Hotmail as "Live at Edu," bundled with other tools such as instant messaging and cloud-based data storage.

In 2011, Microsoft began transitioning their Canadian Live@Edu customers to the Office 365 cloud-based SaaS offering, which now includes online access to all Office applications (Word, Excel, PowerPoint, One Note, Publisher, Access, etc.), Skype for telephony and video-conferencing, as well as shared and private file storage, shared and private online calendars, hosted voicemail and collaborative online workspaces. The basic plan (E1) is free of charge at time of writing (although there is no guarantee that it will remain so). Additional services (the E3 level) are offered on a monthly subscription fee per user and include, in addition to all of the E1 offerings, installed versions of Office applications (on up to five computers and five tablets or phones per user for work offline), and tools for the institution to

[15] Oxford, Cambridge, MIT and Harvard run email in house. Princeton uses Gmail for students; but an in-house Microsoft Exchange system for faculty, graduate students and staff. http://helpdesk.princeton.edu/kb/display.plx?ID=5088.

manage its use of Office 365 and analyze its own data with Business Intelligence tools.[16] While Microsoft encrypts data in transit between its servers and the customer; to use cloud-based software services, the files must be decrypted on Microsoft's server's first.

Google Inc. launched its free-for-all web-based Gmail service in 2004; in 2006 it released the Google Apps suite which included Gmail along with collaboration and calendaring tools. While Google charges subscription fees for its Google Apps for Work, Google Apps for Education is offered free of charge to qualified educational institutions, and includes Gmail, online storage (Google Drive), shared calendar and document collaboration tools (documents, spreadsheets and presentations), websites, voice, video or text messaging (Hangouts) and social media. In addition, Google Apps offers a "Classroom" App designed to create paperless assignments for teachers to distribute to students and grade online. As with Microsoft's Office 365 offering, the Google Apps product is also designed to work on phones and tablets. Google also sells premium services that let business and education customers have access to tools that manage the institutional archiving of their e-Correspondence for regulatory and compliance reasons and Business Intelligence tools that let organizations analyse the patterns in their own "big data."[17]

There are many other vendors who also provide eCommunications services on the public cloud or who sell eCommunications or collaboration suite solutions that can be used on in-house systems or private clouds.[18] We focus on Microsoft and Google here because these two companies are by far the dominant choice of Canadian universities. Both Microsoft and Google offer their services "free of charge," at least for student email and basic plans, to the education sector broadly. Both companies are competing for the entire education market (K-12 and post-secondary) with free eCommunications and cloud-based collaboration tools for students, discounted services and faculty and staff, and with low-price point hardware designed for schools that are integrated with each company's cloud Software-as-a-Service offerings (the Surface tablet by Microsoft, the Chromebook by Google).

There are as yet unconsidered implications of having so many schools and education systems around the world using one of only two companies for their eCommunications needs. What will it mean for a child born now to have records of their entire educational experience, including copies 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 future, will they?

---

[16]Microsoft Corporation, "Office 365 Education plans and pricing," n.d. 2015. https://products.office.com/en-ca/academic/compare-office-365-education-plans.

[17]Google Incorporated. "Innovative Tools to Enable New Ways of Learning," https://www.google.ca/edu/higher-education/.

[18]See for example, Zimbra Collaboration Suite by Zimbra, Inc, which offers both free open-source and paid versions with commercial support (http://zimbra.com); Open-Exchange (open-exchange.com), IceWarp (icewarp.com); Bell Canada WebMail and Bell Mail Suite (support.bell.ca/Internet/Email) This is not an endorsement of any of these companies, either Canadian or multi-national.

Canadian Universities and eCommunications Outsourcing

To better study outsourcing in the Canadian University sector, we examined the eCommunications status (in-house or outsourced) of the 30 largest universities in Canada by combined graduate and undergraduate student enrollment, which included the U15 (Canada's' leading research universities) as well as several smaller schools (including the University of New Brunswick and the University of PEI) to ensure representation across the country, for a total of 35 universities.[19] We excluded British Columbia schools, as that province prohibits publically-funded bodies by statute from storing personal information in their custody outside the jurisdiction of Canada.[20] To date, Francophone universities in this group have been providing services through in-house solutions.[21]

We initially identified nineteen universities in this group of 35 that had already outsourced at least some of their eCommunications needs (either for students, staff, faculty and/or alumni) to either Microsoft or Google as the basis for our sample set. They are listed in Table 1, which follows. We learned later that York, and Brock had outsourced, and we subsequently added them to the study.[22] Most universities have only outsourced eCommunications for students; names in ***BOLD italics*** **in Table 1(on page 12)** indicate schools that have also outsourced faculty and staff eCommunications systems. Note that some schools, like the University of Alberta, made use of the new systems mandatory for all users, other schools, such as Ryerson University, allowed faculty at least to "opt in" to the extra-national systems. York and Concordia Universities allow students to use either a university account or to provide their own.[23] Students are typically provided with an email account at time of enrollment through which they receive official communications from the university.

We wrote to the Provosts (the chief academic officers) of the universities in our sample set to confirm our findings about their eCommunications products and for those who had already outsourced, to request their participation on our study. We were particularly interested in copies of Privacy Impact Assessment Documents, copies of vendor contracts and any relevant information about outsourcing decisions. Privacy Impact Assessments (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. PIAs are widely seen as a "best practice" but are not required by

[19] The University of Alberta, the University of British Columbia, University of Calgary, Dalhousie University, Université Laval, University of Manitoba, McGill University, McMaster University, Université de Montréal, University of Ottawa, Queen's University, University of Saskatchewan, University of Toronto, University of Waterloo, Western University (formerly the University of Western Ontario). See the U15 Group of Canadian Research Universities: http://www.u15.ca/ .

[20] 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.

[21] For example, faculty and staff access at the Université de Sherbrooke access email through either Microsoft Outlook or Outlook Web Access.

[22] We learned of McGill's outsourcing to Microsoft Office 365 just as this report was ready for publication, so we have not yet been able to access its contracts or PIA documentation.

[23] York University, "Student Email and Collaboration Tools Initiative: Privacy Impact Assessment," 19 December 2014, Released under Freedom of Information Access Request No. 2015-009: Google Apps For Education," 4.

statute in Canada for the higher education sector.[24] Nearly all of the universities who outsourced had completed such a PIA or a more comprehensive Information Risk/Risk Management (IRRM) process that includes both a study of risks to privacy of personal information along with risks to information security by the proposed plan. While most universities responded and at least confirmed their eCommunications outsourcing status, none were initially forthcoming with the requested documents.[25] One transparent exception was the University of Toronto, whose PIA/TRA document (called an IRRM: Information Risk/Risk Management Document) was available for download in a publically accessible place on the Information Technology + Services website. The University of Toronto also made publically available its reports on the student, faculty and staff consultation process.[26] No other university in our sample set was as transparent, or even had a publically accessible PIA.

We subsequently used provincial Freedom of Information laws to request copies of Privacy Impact Assessments concerning eCommunications outsourcing decisions and the universities' contracts with Microsoft and Google. As of this report, we have obtained 19 contracts or links to online license agreements and 17 PIA or IRRM (Integrated Risk/Risk Management) documents. We had requested Lakehead University's original contract as well, as they were the first University in Canada to outsource (to Google in 2006) but were advised in response that the contract could not be found. Lakehead did provide additional documentation including an internal memo reviewing the privacy implications of extra-national outsourcing.[27] The University of New Brunswick did not undertake a PIA. Rather, as their response letter indicated, UNB "relied upon the PIAs produced by many other schools to inform our decision-makers about the process around Live@edu and Office365 (the next generation of Live@edu)."[28] The University of Prince Edward Island replied to our request that it is not subject to its provincial FOIPP legislation and further, that it did not conduct a formal PIA prior to outsourcing to Google Apps for Education.[29] In its response to our request, Concordia replied that they had not done a formal privacy or regulatory impact assessment, nor had they signed "a specific contract in relation to Office 365 services from Microsoft."[30] However, Concordia students are using Microsoft Office 365. They either sign for an email account via Office 365 to have a studentname@live.concordia.ca email address

[24] PIAs are required by law for the health sector in Alberta. See Alberta. *Health Information Act,* RSA 2000, Ch. 5, s.64. http://www.qp.alberta.ca/documents/Acts/H05.pdf.

[25] Waterloo University has not outsourced eCommunications at time of writing but still agreed to participate in our study. Mr. Dave Wallace, CIO of Waterloo University generously participated in a conference call with the project investigators to explain Waterloo's rationale for keeping eCommunications in house at this point. We greatly appreciate his contributions, perspective and insights. As the study unfolded we elected to focus on efforts on the implications of the jurisdiction and location questions, and so did not pursue additional interviews with CIOs at other universities who have not yet outsourced.

[26] See University of Toronto Information Risk and Risk Management, "Staff and Faculty e-Communications Outsourcing Project," August 7, 2014. Online at http://main.its.utoronto.ca/wp-content/uploads/2014/08/Office365-Staff-Faculty-IRRM-2014_0807-v2-0-9a.pdf.

[27] Letter from Dr. Millo Shaw, Director of Risk Management and Access to Information, Lakehead University to Dr. Heidi Bohaker, March 9, 2015, FIPPA Request FOIR 15-01.

[28] Email from Sarah DeVarenne, University Secretary and Head under the Right to Information and Protection of Privacy Act, University of New Brunswick to Heidi Bohaker, 3 February 2015.

[29] Mark Leggott, University Librarian, Privacy and Copyright Officer to Dr. Heidi Bohaker, March 10, 2015.

[30] Me. Bram Freedman, Vice-President, Development and External Relations and Secretary-General to Dr. Heidi Bohaker, 13 March 2015, via email.

or they provide the university with their own "current, personal email address" for the University to direct their eCommunications. [31] As of writing, Dalhousie University has yet to respond to our requests and we will be following up with Nova Scotia's Privacy Commissioner. A recently released arbitration ruling (August 2015) supported the decision of the University to outsource to Microsoft's Office 365 platform.[32]

Canadian universities have been comparatively late to this twenty-first century outsourcing trend. In 2010, the technology e-zine *ZDnet* asked "Why is Canada reluctant to adopt cloud computing? The number of cloud-using university students in Canada is shockingly low in comparison to Europe or the US. Could data protection law and privacy be a reason why?"[33] The same article reported that by 2010 Microsoft had market share in 86 countries, while Google had contracts with schools in 145 countries; in some countries such as Australia, nearly the entire K-12 and post-secondary sectors had already outsourced. While Canada is quickly catching up with this eCommunications trend, there are still universities which have not yet outsourced eCommunications including those in the U15 (group of Canada's leading research universities) and those in British Columbia, where publically-funded bodies are prohibited by statute from storing data in their custody out of Canada.[34]

[31] Microsoft Office 365 for education, Privacy FAQ, Prepared by the Office of the General Counsel, 7 November 2014. http://www.concordia.ca/content/dam/concordia/docs/IITS/office365-privacy-faq.pdf. Email access to students is provided at outlook.com/live.concordia.ca

[32] Arbitration Award between Nova Scotia Government and General Employees Union and Dalhousie Faculty Association. Awarded August 26, 2015. Available online through http://allaboutinformation.ca/2015/09/05/arbitrator-says-outsourcing-e-mail-system-to-the-cloud-lawful/

[33] Zack Whittaker for iGeneration | June 15, 2010 -- 13:28 GMT (06:28 PDT); http://www.zdnet.com/article/why-is-canada-reluctant-to-adopt-cloud-computing/?_escaped_fragment_=#!.

[34] This appears to be changing. In April of 2015, BC-Net entered into an agreement (a "strategic alliance") with Microsoft and its regional reseller, Long View Systems, to provide access to the Microsoft Office 365 product through a sector-wide licensing agreement. Users presumably will have to give "informed consent," referring to the informed consent clause in BC's FIPPA legislation that is necessary to permit out-of-country data storage by publically-funded bodies. See https://www.bc.net/bcnet-higher-education-members-unite-establish-sector-wide-strategic-alliance-microsoft.

Table 1: Universities asked for PIAs and Vendor Contracts[35]

Year [36]	University (bold, italics indicates faculty/staff outsourced as well)	Total Student Enrollment	Province	Vendor
2006	***Lakehead University***	8 610	Ontario	Google
2010	***University of Alberta***	38 930	Alberta	Google
2011	University of New Brunswick	9 980	New Brunswick	Microsoft
2011	University of Prince Edward Island	4 410	Prince Edward Island	Google
2011	University of Toronto	85 900	Ontario	Microsoft
2011	***Carleton University (Faculty, 2014)***	28 440	Ontario	Microsoft
2011	McMaster University	30 680	Ontario	Google
2012	Ontario College of Art and Design University	4 660	Ontario	Google
2012	University of Ottawa	43 300	Ontario	Google
2012	***Ontario University Institute of Technology***	9 990	Ontario	Google
2012	***Ryerson University***	39 430	Ontario	Google
2012	Memorial University	18 280	Newfoundland and Labrador	Google
2012	University of Windsor	15 990	Ontario	Google
2012	***Queen's University (Faculty, 2013)***	25 900	Ontario	Microsoft
2013	***Dalhousie University***	18 810	Nova Scotia	Microsoft
2013	University of Manitoba	29 060	Manitoba	Microsoft
2014	Concordia University	36 250	Quebec	Microsoft
2014	University of Guelph	27 110	Ontario	Google
2014	Western University[37]	30 600	Ontario	Microsoft
2014	York University	53 600	Ontario	Google
2015	Brock University	18 510	Ontario	Microsoft
2015	***McGill University***	37 780	Quebec	Microsoft

[35] Statistics for September 2015 taken from http://www.univcan.ca/canadian-universities/facts-and-stats/enrolment-by-university/

[36] 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.

[37] Formerly the University of Western Ontario.

Rationales for Outsourcing

When Canadian universities finally did decide to outsource their eCommunications, they typically gave three reasons for their decision (the "drivers"): 1) the cost-savings that outsourcing would bring; 2) student expectations for better eCommunications services than the university could or was willing to provide; and 3) failing in-house equipment and/or software no longer supported by the vendor. These rationales were expressed both in the Privacy Impact Assessment documents we studied, and also in the web-accessible information universities prepared to explain to their communities why the outsourcing was occurring.

The offers of free eCommunication services from Microsoft and Google corporations were and remain attractive to University administrators. Lakehead University was the first in Canada to outsource eCommunications extra-nationally in 2006. Michael Pawlowski, then Lakehead University Vice-President (Administration & Finance) who oversaw the transition that began in 2006, later explained (in 2008) that "when Google made the offer that it wouldn't cost us anything, no ads, I couldn't believe the offer…So we took the three-year arrangement which included not only e-mail, but calendaring, instant messaging … word processing – the whole application."[38] In an internal memo released by Lakehead in response to our FIPPA request, the university's internal system prior to outsourcing was described as wholly inadequate to meet the university's current and growing needs, with minimal disk quotas and regular system outages. Google's offer to Lakehead must have indeed seemed providential indeed.

"Free" quickly became a key requirement. Alberta noted in 2009 that contracting to Google's free service "would be of an economic and operational advantage to the University." [39] In their Privacy Risk Assessment, Alberta explained that they had 35 different email systems operating across the university and that to replace them all with one commercial system would be "cost prohibitive" – "several million dollars for start-up and a million dollars annually for ongoing costs."[40] In his February 2010 response to the report from the student consultation process, the CIO of the University of Toronto stressed the expense of constructing and maintaining an in-house system: "We have not pursued a detailed quotation, but it would obviously cost millions of dollars for hardware, software, system porting and ongoing development staff."[41] When the University of Toronto issued a Request for Information later in the spring of 2010 from potential student email vendors it was specifically looking for "free outsourced options." The University received three replies, one each for Microsoft (Live@Edu) and Google Apps,

[38] Phillip Todd, "Switch to Google email saves resources, raises privacy concerns" 10 March 2008, http://www.universityaffairs.ca/news/news-article/switch-to-google-email-saves-resources-raises-privacy-concerns/ .

[39] Privacy and Information Security Impact Assessment Report. University of Alberta Google Applications and Gmail Project, 2009. (henceforth Alberta PIA), Released under FIPPA 2015-001, 3.

[40] Alberta PIA, 1.

[41] Robert D. Cook, CIO's Response to the Report from the Consultation on Student e-Communication Services," http://email.utoronto.ca/wp-content/uploads/2013/09/CIOs-Reponse-to-eCommunications-Report.pdf .

and a third "fee-based solution" from an unidentified vendor that "was consequently set aside."[42]

Curiously, in considering costs, there appears to have been little to no concern expressed about the time limited terms of the contracts (ranging from 2 to 5 years), or the lack of provision in the contracts for the perpetual continuation of the "free" service.[43] In fact, the contracts and/or license agreements contain the opposite provision – the right at renewal to charge for what was previously free, or to change the terms of service. The university is of course free to not renew the agreement if it does not like the terms. What costing we did observe was limited to very high level descriptions of annual operating costs of in-house versus outsourced solutions, and did not include "migration" costs in the event of a change in service provider. Switching eCommunications vendors on an organization-wide basis is a complex process, especially given the proprietary systems used that encourage vendor-lock-in and make it difficult to migrate data seamlessly from one system to another and can take significant time.

The second driver commonly cited (and also related to cost) was the poor state of in-house eCommunications systems. They were "end-of-life," frequently failed and required "annual patchwork replacement"[44] All universities in our sample set reported completely inadequate in-house data storage capacity (account sizes of 50 to 150 MB per user in contrast with 50 GB to now up to ITB on outsourced systems). Other challenges reported included lack of support for open-source software or vendor abandonment of the product line. Queen's noted that its current system was "no longer supported by the vendor," but further, that it lacked the calendaring and other integrated tools of other newer systems.[45]. Larger universities like the University of Alberta were trying to replace multiple on-campus email systems with one outsourced system. Alberta had 35 separate email systems in different divisions and units prior to outsourcing.[46] The University of Toronto has multiple systems in use across departments and divisions with some departments such as computer science, math and chemistry each having their own departmental email server.

The multiplicity of email systems on university campuses should not be interpreted simply as a legacy of past practices. For some academic units, particularly computationally heavy ones like computer science, internal eCommunications systems serve very specific academic needs, and are not infrequently a site of research themselves by faculty and students in those units. Further, the sorry state of hardware and limited storage capacity as described in these documents is not a sudden, unplanned crisis, but reflects a

---

[42] Robert D. Cook, "Report #3 and Recommendations, Student e-Communications Services," http://email.utoronto.ca/wp-content/uploads/2011/03/Report-3-Student-e-Communications-Consultation-w-Appendices.pdf, 1.

[43] Memorial University did discuss this risk and its mitigations, which include bringing the service home and/or paying for the outsourced previously free service. See Memorial University of Newfoundland. Privacy Impact Assessment, Google Apps for Education, "Version 1.0 October 2011, *Released under Access to Information and Protection of Privacy Act* File B-05-01-15 (henceforth Memorial PIA), 21.

[44] Robert D. Cook "Report #2 and Recommendations, Student e-Communications Services." http://email.utoronto.ca/wp-content/uploads/2011/03/Report-2-and-Recommendations-Student-e-Communications-Services-Web.pdf

[45] Telus Security Solutions, "Privacy Risk Assessment: Final Report, Prepared for Queen's," 29 August 2012, Reference #: QU-05022012-PRO002, released under FIPPA Request No. 2015-001 (henceforth Queen's PIA),19.

[46] Alberta Privacy and Information Security Impact Assessment Report. University of Alberta Google Applications and Gmail Project, 2009. (henceforth Alberta PIA), Released under FIPPA 2015-001.

lack of investment in critical infrastructure and support staff over a longer period of time. It is also not a technological failure but of institutional priorities. Smaller schools with smaller budgets face more constrained budgetary realities, but with provincial leadership and an appropriate community cloud model, smaller schools could share services with larger universities.

Student expectations were also cited as the third driver of eCommunications outsourcing. Memorial University conducted a three month pilot study with their Term 4 Commerce students for their planned outsourcing to Google; the university found that in their survey, 100% of students reported being "satisfied" or "very satisfied" with the greatly expanded email storage, document collaboration features, calendar, chat and video-conferencing provided in the new tool.[47] In 2012, the Chief Information Officer at the University of Toronto explained in a Microsoft case study document published on the vendor's website that "we didn't want to continue expending resources on an aging service that didn't meet students' expectations."[48] Western University's 2014 PIA explained "Western has outgrown its own platform, resulting in higher maintenance costs and numerous deficiencies relative to the changing needs of the student."[49] York University noted that moving to Google "will provide students with a vastly improved service."[50] Meeting student expectations for eCommunications technologies as part of supporting and improve the overall student experience was a common theme in both the PIA documents we examined as well as the other sources we consulted such as the information provided to students to explain the reason for the transition to the new system, and in industry-sponsored publications where university IT leadership explained why they chose the new outsourced system.

Vendor-sponsored case studies of successful migrations tout the positive feedback students give the new system. In one Canadian example, the CIO and Associate Vice Principal at Queen's University commented on the positive student response to the Office 365 rollout: "The students were easy: they love that they are working with a business-grade productivity platform. As soon as we offered Exchange Online to the undergrads, the graduate students were knocking at our door. Everyone was ecstatic when we introduced the Office 365 ProPlus benefit that gave all students the latest copy of Office to download on five devices—PCs, Windows-based laptops and tablets, Macs, iPads, Android tablets—whatever students owned."[51] In some cases students were in fact actively campaigning for better email; at Western "a new email service has been major priority of the USC [University Student Council] for the past few years.[52]

In all of the above case, students were always being asked to compare an "aging" in-house system with a state-of-the-art outsourced system, rather than a third option, a privacy protective, improved in-house

[47] Memorial PIA, 7.
[48] Microsoft Canada, "University Improves Student Services, Saves IT Costs with Cloud-Based Email," 9 April 2012, http://www.microsoft.com/canada/casestudies/Case_Study_Detail. (note this case study has been removed from Microsoft's website as of writing).
[49] Paul Eluchok and David Ghantous, "MICROSOFT OFFICE 365 PRIVACY IMPACT ASSESSMENT Western Student E-Communications Outsourcing," 19 August 2014, released under FIPPA 28 May 2015 (henceforth Western PIA),1.
[50] York PIA, 3.
[51] Bo Wandschneider, "Queen's journey to a cloud-connected campus with Office 365," 20 January 2015. https://blogs.office.com/2015/01/20/queens-journey-cloud-connected-campus-office-365/.
[52] http://www.westerngazette.ca/2015/02/western-email-converges-microsoft-office-365/ .

system that would require institutional investment and/or higher fees to fund. The University of Toronto did consider developing a student email system either within Microsoft Exchange or within the Blackboard learning portal, and in the words of the University's CIO report on the student consultation process "student sentiment within the committee tended towards this option."[53] However, as at other universities, cost considerations overrode privacy concerns.

Analysis of university Privacy Impact Assessments

Prior to outsourcing, nearly all universities in our sample set undertook some form of a Privacy Impact Analysis exercise. The resulting Privacy Impact Assessment (PIA) documents are intended to present the results of an organization's self-study exercise to ensure that it can live up to its obligations under federal and provincial statutes to protect the privacy of personal information in its custody. Producing such a document requires a commitment of institutional staff time and/or institutional resources in terms of external consultant fees, depending on whether the university in question undertook the process in-house or brought in an outside firm. Done well, and rigorously, PIAs can identify potential privacy risks and help organizations plan risk mitigation strategies. They can also help organizations identify the most privacy-protective course of action in terms of whether, for example, to provide in-house or outsourced eCommunications services.

But a privacy impact assessment can also be undertaken after a choice or action is made, and in that case the risk is that the document simply serves as a checklist to ensure that the decision will not cause the organization to run afoul of existing legislation. In the 2014 report *Transparent Lives: Surveillance in Canada*, editors Colin J. Bennett, Kevin D. Haggerty, David Lyon, Valerie Steeves assessed the role of PIAs in protecting the privacy of personal information across a broad range of sectors and found was that PIAs were more likely to be after-the-decision checklists rather than serving to help organizations make privacy-protective decisions prior to choosing a vendor.[54]

In our examination of university PIA documents, we observed a broad range of quality and thoroughness, ranging from a few pages to much heftier documents running over 50 pages; some were undertaken *after* a vendor had already been selected, while others before the decision was made. In several cases the PIAs indicated that the vendors (in these cases, Microsoft specifically) had contributed advice or information to, or had otherwise participated in the PIA process. Some were fairly rudimentary checklists, while others were far more comprehensive. Particularly notably in the case of Ryerson University and the University of Alberta, the documents reveal that significant efforts were made to reach out and involve the University community in the planning and decision-making process. Several PIAs were still marked draft when we received them or contained unaccepted changes or other markup, suggesting that perhaps these particular institutions did not fully complete the PIA process. Our purpose here however is not to characterize individual documents as weaker or stronger, but rather to assess the set as a whole and to identify widespread but problematic assertions that served to support

[53] http://email.utoronto.ca/wp-content/uploads/2013/09/CIOs-Reponse-to-eCommunications-Report.pdf .
[54] http://www.surveillanceincanada.org/trends/what-can-be-done.

extra-national outsourcing decisions. We also identify lapses – areas not covered – in existing PIAs, and explain the benefits to addressing these areas or expanding on these areas in future PIAs.

Definition of Personal Information

At the most basic level, a privacy impact assessment considers the privacy risk to personal information in the organization's custody, and identifies and proposes mitigation strategies to reduce that risk. The definition of "personal information" for universities must be taken from provincial privacy statutes, if applicable.[55] These legal definitions cover a broad range of information that needs protection from unauthorized disclosure if in the care of an organization or institution such as a university. Ontario's FIPPA legislation, for example, defines personal information as "recorded information about an identifiable individual, including:

> (a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
> (b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,
> (c) any identifying number, symbol or other particular assigned to the individual,
> (d) the address, telephone number, fingerprints or blood type of the individual,
> (e) the personal opinions or views of the individual except where they relate to another individual,
> (f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,
> (g) the views or opinions of another individual about the individual, and
> (h) the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual; ("renseignements personnels")[56]

Universities varied in their approach to defining and describing the types of personal information that the PIAs covered with respect to the service to be outsourced. The University of Alberta, for example, had a broad and comprehensive definition that included draft documents, email attachments and the "substance of all calendar appointments and notations of all staff of the University."[57] However, in their privacy impact assessments, several universities defined the personal information in their custody much more narrowly, confining it to the information that the University (the "Customer") had to provide to the software vendor in question in order to create accounts on the new system, and then defining all other personal information in the new eCommunications system as that created by the end users (the faculty, staff and students who have accounts on the system). In other words, these schools conducted

[55] UPEI says such legislation is not applicable to them.
[56] Ontario. *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F.31. Section 2(1). http://www.ontario.ca/laws/statute/90f31 .
[57] Alberta PIA, page 4.

their privacy impact assessments on the risk of providing only first names, last names, university id or student numbers, an institutional email address to an extra-national vendor, not on the total of information likely to be archived within a university's email or eCommunications system.[58]

Western University's PIA is one such document where personal information was defined in this way. Specifically, the document indicated that what the university was disclosing to Microsoft was the following only: "student name, student enrollment details (group membership) and assigned email address." The PIA explained this by noting "it is the position of Western that student email is not information that is considered to be under the custody or control of Western and therefore FIPPA does not apply to this information. It is not considered information collected by Western for use by Western for its purposes." The authors then went on to note that nonetheless, "the information in the email system is considered the personal information of the student and the system should be designed to protect it to the same security standards that would apply to any other university systems that contains personal information." [59] The University of Manitoba also did the same, noting that "the content of student email is not information considered under the custody or control of the University and therefore the *Freedom of Information and Protection of Privacy Act* (FIPPA) does not apply to this information."[60] Memorial University took the same line, arguing that "the vast volume of records generated through the use of the services will be records generated by student users and will not be considered to be in the University's custody and/or control in accordance with ATIPPA."[61]

Such a technical approach to what personal information is in the custody and control of the University does not seem to meet the spirit and intent of statutory requirements for public bodies to protect the privacy of personal information even if it meets the minimum required by the law. But this also raises a crucial question: how much information is a University responsible for? Surely eCommunications exchanges between faculty and students should be considered under the custody and control of the institution, as these exchanges are a necessary part of the overall teaching mission, as are communications between staff and students about grades and other matters, and findings of University disciplinary bodies when they are communicated to students via email. But what role and/or responsibility does the University have to protect the private correspondence between two or more students about personal matters that have nothing to do with their status as a student or their respective relationship with the University? We need answers to these questions.

By taking different approaches to defining personal information without a broad debate on these issues, University IT administrators and internal privacy officers are making determinations about the institution's responsibility towards personal information. Such determinations may be correct in terms

---

[58] University of Ontario Institute of Technology (UOIT), "Google Apps for Education: Student Email Service Privacy and Risk Assessment", released under FIPPA 10-001-2015 (henceforth UOIT PIA), 8. See also OCAD University, Google Aps for Education Privacy and Risk Assessment. 27 July 2011 (henceforth OCAD PIA). Released under FOI 2015-01, 5.

[59] Western PIA, 5

[60] University of Manitoba, "Privacy Impact Assessment: Microsoft Office 365 Implementation: Student email project," Released under the *Freedom of Information and Protection of Privacy* Act, UM2015-10, (henceforth Manitoba PIA), undated, 3.

[61] Memorial PIA, 13.

of strict interpretation of the relevant privacy statutes as they affect the university's potential liability for disclosure of that information, but may be at odds with how the broader university community defines what should be considered personal information. It should be noted that other universities such as the University of Alberta and the University of Windsor, took a broader approach. Windsor argued that "all email must be regarded as being as sensitive as the most confidential of these communications."[62] Nevertheless, Windsor too outsourced its eCommunications to the cloud. In the digital age we urgently need a robust discussion about what is considered information that the University has a responsibility to protect. We turn now to a discussion of the arguments used to date to support outsourcing decisions.

The Similar Risk Argument

The "similar risk" argument is the logical underpinning of all the university outsourcing decisions that we investigated and has been the principal argument used to assuage privacy concerns about extra-national outsourcing. Similar risk is the idea, as colleagues Lisa Austin and Daniel Carens-Nedelsky describe in their legal analysis, that the risk of disclosure to third parties, particularly government agencies, is roughly the same regardless of where in the world the data are stored. This idea has been in wide circulation for more than a decade and has been accepted uncritically by those Canadian university administrations and senior IT staff who have chosen to outsource. While the PIAs we examined all recognized that when University data were stored in foreign jurisdictions it would be subject to the laws of those jurisdictions, all concluded that this was ultimately not relevant because such data faced similar risks of state access in Canada.

To give just one representative example, here is the short explanation given on the University of Manitoba's "Frequently Asked Questions page about their Office 365 email deployment. The question: "is my email subject to US government laws? The answer: "Yes. However, the move to Office 365 results in no appreciable difference to what currently exists with our email. US and Canadian laws regarding email are very similar in nature.[63]. In making such claims, we noticed that the authors of PIAs and University "FAQ" documents were drawing on conclusions also 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.[64]Canadian jurisdiction offers significantly better privacy protection to Canadians and residents than US jurisdiction does, for example.

Several other examples are included here to show the range of variations in circulation under the umbrella of the "similar risk" argument. When references were made in these PIA documents to any foreign statute potentially posing a risk to privacy, the *USA PATRIOT* Act of 2001 (often written simply as

---

[62] University of Windsor, "Privacy Impact Assessment: University of Windsor Considerations in Moving Student Email to the Cloud," April 7, 2011, 10, fn 5. Released under FIPPA File 2508 (henceforth Windsor PIA), 3.

[63] http://umanitoba.ca/computing/ist/email/studentemailfaqs.html .

[64] 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/ .

the "Patriot Act" with no citation) was often the only one discussed.[65] Very few PIAs mentioned the important *Foreign Intelligence Surveillance Act* (FISA) Amendments Act of 2008, which enabled bulk surveillance in the first place[66] or other relevant US statutes identified by Lisa Austin and Daniel Carens-Nedelsky in their report "Why Jurisdiction Still Matters."[67]

At its most basic, the "similar risk" argument makes a false equivalency. In University of Alberta's 2010 PIA for example, the authors "acknowledge that the Patriot Act is consistent with the laws in the US and Canada and elsewhere that allow government to seek information about individuals in connection with intelligence activities."[68] While on the surface this statement is accurate, what is missing, as Lisa Austin and Daniel Carens-Nedelsky show, is the fact that the tests that must be met to seek that information are different in each jurisdiction, and that in the US the data of "non-US persons" is subject to an even lower standard for access than for US persons, and importantly on a standard that would be unconstitutional in Canada. Carleton University's PIA report asserts a variation on this false equivalency: that "the requirements of the PATRIOT Act can also be found in Canadian law (See, for example, *Anti-Terrorism Act*, S.C. 2001, c. 41)" But its authors go on to make several unfounded assertions as further "evidence" in support of the similar risk argument: "… extensive data sharing occurs between Canadian and American law enforcement authorities. There is no border when it comes to anti-terrorism cooperation and if American (or any other country's) authorities want information about Canadians they are more likely to ask their Canadian counterparts for it than sort through databases of American service providers located in the United States… whatever concerns about law enforcement access triggered by the Patriot Act equally exist with a Canadian service provider in Canada." Again, these sorts of claims are incorrect and ignore the fact that under Mutual Legal Assistance Treaties (MLATs), it is the constitutional norms of the sharing state that apply.[69]

The University of Ottawa's detailed report also makes a similar risk argument, that it

> "should be noted that given that Canadian search and seizure laws are fairly similar to United States law (to the extent of the powers provided to government), the close collaboration and ongoing sharing of information between Canadian and US agencies, and the ability of Canadian authorities to obtain warrants for US authorities through mechanisms such as mutual legal assistance treaties, it is possible that data managed in Canada by a Canadian company could in theory end up in the hands of US authorities, which highlights that an agreement with any service provider, regardless of location,

[65] The USA PATRIOT Act is an acronym for the full title of the legislation: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism. See https://www.congress.gov/bill/107th-congress/house-bill/3162 .
[66] See Foreign Intelligence Surveillance Act. Amendments of 2008 (FISA) 50 USC Ch 36., PL 110-261. http://www.gpo.gov/fdsys/pkg/STATUTE-122/pdf/STATUTE-122-Pg2436.pdf
[67] Austin and Carens-Nedelsky, "Why Jurisdiction Still Matters," http://ecommoutsourcing.ischool.utoronto.ca/.
[68] University of Alberta "Privacy Risk Analysis: Google Inc. Project," 2009. Released under FIPPA 2015-01, 10.
[69] Austin and Carens-Nedelsky, "Why Jurisdiction Still Matters," http://ecommoutsourcing.ischool.utoronto.ca/.

> should consider the privacy risks/implications of the relationship, and that a transfer of data across borders should not necessarily cause grave concern in and of itself." [70]

Again, these assertions rest on faulty legal analysis. Not only do these PIAs consistently rely upon the similar risk argument that our project calls into question, they give the impression that these risks are more focused on terrorism-prevention related intelligence gathering. But the 2013 Snowden documents provided clear evidence not only of bulk surveillance but of surveillance targeting a much broader range of interests than "terrorism" or "homeland security," as well as evidence of the broad powers granted under the *FISA Amendments Act* of 2008 with respect to the collection of "foreign intelligence information" from the data of non-US persons. We were therefore surprised to see that universities did not reassess their outsourcing decisions in light of new information and that PIAs written after June 2013 did not reflect upon the implications of the documents released by Snowden.

Another version of the "similar risk" argument asserts that bulk warrantless surveillance is occurring even within Canada against Canadian persons and that Canadians and Canadian organizations have no power to do anything about it. The University of Toronto's 2014 PIA/IRRM document, for example, asserts that: "The University recognizes that beyond itself and its commercial partners exists external governmental agencies –both within and external to Canada –whose mandate is to surveil electronic communications, and with whom the University has no means of negotiating terms, conditions, or any sort of standard of notice or behaviour."[71] It is not clear what this statement is meant to establish. Universities have the ability to choose in which jurisdiction to place their digital institutional archives, and also have the ability to assess the scope of the legal authority that underpins the mandate of any government agency acting within that jurisdiction. Universities can also influence law reform within their own jurisdiction. Certainly within Canada one can point to the ways in which Canadians, including university faculty, have a direct impact on both law-making and judicial interpretations related to the protection of privacy rights. If these are deemed to be inadequate, they can be strengthened through the electoral process and law reform. Canadian citizens and residents can draw on their constitutional and statutory rights to improve privacy protections within Canada. Canadians have far less leverage or influence extra-nationally.

Email is "like a postcard," lowering expectations of privacy.

In addition to the similar risk argument, all PIAs made some version of the "email is like a postcard" or "email is inherently insecure" argument as a further justification in support of extra-national outsourcing. Instead of considering ways in which eCommunications systems can be deployed to enhance the privacy and security of user data and metadata, these documents defines email as a fundamentally insecure form of communication for which there could be no guarantee or expectation of privacy.

---

[70] "University of Ottawa Cloud Computing Initiative Privacy Impact Assessment," prepared by Deloitte LLP. June 2013 (henceforth Ottawa PIA), Released under FIPPA A-15-1, 3.

[71] University of Toronto Information Risk and Risk Management, "Staff and Faculty e-Communications Outsourcing Project," August 7, 2014. Online at http://main.its.utoronto.ca/wp-content/uploads/2014/08/Office365-Staff-Faculty-IRRM-2014_0807-v2-0-9a.pdf, 7.

There are many examples of this assertion in the PIA documents. The University of Windsor's PIA points out "it is important to understand that any email communication has a low expectation of privacy."[72] Memorial University's PIA asserted that "Email is, by nature, an inherently insecure form of communication... A user should always assume that email is not private, and this is true for all email services."[73] The University of Manitoba's PIA asserted that "Students be notified in advance of claiming their email that their information will reside in a foreign jurisdiction and will be subject to the laws of that jurisdiction, and that the University cannot guarantee protection against possible disclosure of personal information that is held in foreign jurisdiction…Students will be notified to not use the email system to send or receive sensitive personal health information."[74] The PIA for Queen's University contained a contradictory statement about the privacy expectations for email: "Emails are considered private information and therefore should only be disclosed to authorized users on a need-to-know basis. It is critical that emails containing sensitive information be stored protected." And yet in the same section, its authors pointed out that: "It is important to implement a policy outlining that sensitive information including personal information should not be transferred by email."[75]

This approach of lowering University eCommunications privacy expectations is in contrast to the Canadian Supreme Court's clear statements that Canadians do have the right to expect privacy with their eCommunications and despite the acknowledgement within the PIAs themselves of the many types of confidential and/or personal information transmitted by and stored on University systems. If the solution was to effectively educate all users to not send any personal or confidential information through a University's eCommunication system (as one PIA recommended), one wonders how the University would conduct any internal business at all.

Furthermore, by repeating the assertion that email is "like a postcard," these authors used a false analogy. Email is not a postcard and we do not think of it as such. Indeed, the icon for "email" is an envelope. Sending an email message either within an organization's internal system or across the Internet does not automatically mean that it is open to all to read as a postcard actually is. To be sure, an email sent as packets of plain text across the Internet is much more vulnerable to exposure and could be captured and/or read by third parties via the various computers the message travels *en route* to its final destination. But that is not at all equivalent to using a modern enterprise in-house eCommunications software platform that requires a secured encrypted virtual private network access in order to access messages remotely over the public Internet or other security provisions. It is technically true that those working with system administration privileges have access in theory to all of the data on the systems, but the risk of system administrators or those with physical access to the machine reading email can be mitigated within organizations by now well-established control procedures that include software that logs all the actions of users with administrator level privileges working on systems and with proper physical security for server rooms. Organizations considering outsourcing their eCommunications to the Cloud should think carefully about how much of their e-Correspondence are

[72] Windsor PIA, 4.
[73] Memorial PIA, 11.
[74] Manitoba PIA, 3.
[75] Queen's PIA, 34.

really external to their organization. The fact that some email messages may traverse the Internet and may therefore be intercepted and read by others does not logically support the hosting of one's entire institutional digital archive outside of Canadian jurisdiction.

The "Email is fundamentally insecure" argument seems especially problematic given that many universities now use email as their sole official means of communication with students, and many have policies that require students the use the account provided by the university for such official correspondence. Furthermore, although it is true that students are free to choose what information to send via email, they are often the recipient of confidential or personal information about themselves from others, including correspondence from university officials and from faculty members, including, but not limited to, findings of academic discipline panels. How are students to protect themselves if the university chooses to send confidential, internal communications about them to an email account hosted extra-nationally? What about such exchanges between faculty and staff?

Several university PIAs point to the need to educate users to employ alternate means of communication (including telephone calls) when exchanging confidential or personal information rather than email. But ironically these new eCommunications suites include voice and video capabilities that University faculty, staff and students will use, such as Skype (embedded within Microsoft Office 365) or Google's audio and video conferencing tools. Such advice is therefore logically incoherent. Where and through what channels then should private and/or confidential communications within the University take place if all internal communication services are to be routed through the same cloud provider, with all data stored extra-nationally?

The fact is that eCommunication internal to an organization can be made very secure, whether users are working on systems located physically within the organization's premises or accessing servers remotely. Many organizations can and do achieve high degrees of information security and privacy protection by requiring the use of encryption technologies, access to servers via virtual private networks, and other well-documented best practices. Organizations of course have less control over communications that circulate outside of their walls, physical or virtual, but this is true of paper mail as well. Internal communications within universities, especially those between faculty and students, student services and students, faculty and research services, senior administration, etc., can be accorded a much higher degree of privacy protection with the appropriate investment in both technology and user training under institutional control. Moreover, university community members would not be required to waive their constitutional rights and statutory protection of their digital privacy if the data were housed in servers on Canadian soil.

Conflating privacy and security: the "incremental risk" argument.

This argument asserts that even factoring in the risk of disclosures to foreign governments, outsourcing eCommunications is still a good idea because the data will have better protection overall from risk of disclosure due to the purportedly better data security measures that major cloud vendors are able to provide. 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.

Security of information is a necessary requirement to protect the privacy of information, and so the quality of information security is crucial when selecting an eCommunications system. The University PIAs we examined all acknowledged that outsourcing would provide better security from attacks by hackers than any in-house solution they could provide, while simultaneously agreeing that data stored on such a system would be exposed to lawful access of international jurisdictions. The authors argued that on balance, the risk of a privacy breach is lower overall because arguably illegal hacker access would be reduced in frequency, because vendor data centres meet an impressive set of security standards and are subject to regular audits. If one accepts both the similar risk argument and the email is inherently insecure argument, then the apparent protection offered against hackers by these vendors appears to provide a more secure eCommunications environment overall. But this line of thinking rests on unstable ground. As Austin and Carens-Nedelsky have shown, the key question is not if your data could ever be accessed lawfully or illegally by any third party, but who could have access to the data, and under what conditions or standards?

This "incremental risk" argument suggests that expectations of privacy are just one factor of several to be weighed when considering extra-national outsourcing, rather than understanding that privacy expectations are constitutionally protected within Canada and therefore must form the overarching constitutional framework from within which we should assess the other risks. To be sure, compliance and regulatory requirements are increasingly driving institutional practices. No university (nor any organization) wants to face the necessity of alerting users that their data has been breached. T staff time required to deal with breaches and respond to concerned users can be a significant drain on resources depending on the number of people affected. And certainly universities face both reputational and financial implications from data breaches. Outsourcing to large established vendors such as Microsoft and Google, both of whom meet industry-standard external audit compliance requirements for information security, appear on the surface to reduce the risk that a university could be held liable for a data breach of personal information in its control caused by hackers with malicious intent.

While such thinking appears logical on the surface, they are assertions made without evidence or by offering anecdotal evidence along the lines of eye-witness descriptions of physical visits to vendor server facilities. As one Canadian University CIO explained: his visit to Microsoft's datacentre in Quincy, Washington was "a real eye-opener for us …I could prove that we didn't have the resources necessary to handle security threats the way I saw them being handled at Quincy."[76] But, physical security of servers is one small part of the overall information security picture. Equally important is the integrity of the software on the system, including the firewall rules that regulate access to the servers, and ensuring that the people who use the system are adequately trained in the processes necessary to protect personal and confidential information in their custody. A physical "site visit" by potential customers to a vendor's data centre proves very little.

Universities also refer in their PIAs to the security compliance certificates that both Microsoft and Google provide as clear evidence of their ability to protect customer data against illegal intrusions. Such

[76] Bo Wandschneider, "Queen's journey to a cloud-connected campus with Office 365," 20 January 2015. https://blogs.office.com/2015/01/20/queens-journey-cloud-connected-campus-office-365/.

measures cannot be taken as guarantees that data will not be disclosed. Indeed the contracts of both these vendors contain specific language that the vendor will notify the customer promptly about unauthorized breaches when they detect them. And as recent news events of major data breaches indicate, large data stores and large multinationals are attractive targets for criminals.

This is not to suggest that Microsoft or Google do not take security seriously or that their compliance programs are not sufficiently rigorous. Rather, the reality is that both major information security standards (COBIT, ISO 270002) and the National Institute for Standards and Technology CyberSecurity framework ALL acknowledge in their control standards not the possibility, but the near certainty that data breaches will occur no matter the level of security provided. The standards and controls for information security management are about mitigating and reducing risk, but all recognize the near impossibility to impossibility of eliminating risk of data breaches. What is vitally important in these standards is classifying data appropriately, investing the resources to ensure that confidential data is protected to the highest standards possible, detecting that a breach has occurred, identifying the factors that lead to the breach, and minimizing the damage from the breach.[77]

On the surface, outsourcing appears to reduce certain kinds of risks to information security that universities must deal with. However, accepting this argument as a justification for outsourcing introduces other privacy risks, while asking Canadians to forgo their constitutional rights. While outsourcing removes the responsibility for day-to-day operational security of data protection, it does not remove the institution's accountability for the breach. Organizations cannot outsource accountability.

On the other hand, by outsourcing eCommunications systems extra-nationally, universities place their data in jurisdictions where we know not only that bulk surveillance is occurring, but that customers will only ever find out if there has been a lawful request from a government agency if the law permits. When data are outsourced to the United States, for example, provisions in the *USA PATRIOT Act* and the *FISA Amendments* Act of 2008 prohibit US headquartered multi-nationals from even revealing the existence of a request for the data of a non-US person. By conflating privacy with security, this argument asks Canadian customers to accept better (without guarantees) possibly protection from criminal data breeches, at the expense of the broader societal importance of their privacy rights within a democracy, and specifically, for universities, at the expense of the important role that privacy plays in ensuring the academic freedom necessary for universities to carry out their mission and purpose.

[77] ISO 27002 is an internationally recognized "code of practice for information security." See http://www.27000.org/iso-27002.htm. COBIT is an information security framework (Control Objectives for Information and related Technology) offered by ISACA, an information security and governance professional association. See http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx. The United States National Institute of Standards and Technology's Cybersecurity Framework is a lightweight "meta" framework that simplifies the highly prescriptive and detailed ISO and COBIT controls, but still references them underneath its framework umbrella. See http://www.nist.gov/cyberframework/index.cfm.

PIAs that focused on email only or nearly exclusively

The PIAs we examined talk nearly exclusively about the privacy risks to email. But 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 as if they were almost "add-ons" rather than part of an integral, bundled, eCommunications system.

One university explicitly excluded discussion of the privacy implications of what it perceived as other, separate "cloud-based, value-added products" noting that its PIA process "to-date has considered privacy compliance solely with the migration of student email to Microsoft Office 365." It noted that students may access calendaring or collaboration tools such as SharePoint, but that "students must ensure that they have read and are familiar with these terms of use prior to making use of these products." [78]

It is hard to see how students would not come to see these tools not as options but as essential parts of their university experience. In the paragraph following the above statements, the authors of the PIA noted that the university, for example, may choose to "automatically populate student calendars with dates from the academic calendar,"[79] further integrating the calendar functionality into the students' daily lives and encouraging students to enter other personal information into one integrated calendar system.

Defining eCommunications as separate from the teaching and research missions of universities.

This assertion, which occurs in many PIAs, justifies outsourcing on the grounds that doing so frees up university IT resources to focus on the "teaching and research mission" and frees up IT staff to "work on projects that add value to the university community."[80] For example, in 2013, the Executive Director of the University of Alberta's central information technology department pointed out that by outsourcing eCommunications, IT could now "stay focused on our university's mission of teaching and research, and how the IT services we provide can support that 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.

Vendors argue that eCommunications or email systems are a "commodity service" and therefore are a good choice for outsourcing. The problem here is while the system itself can be thought of as a "commodity" (i.e. all organizations can purchase the same system for internal use, in much the same way that photocopiers or paper is purchased), the *content* that is created and stored on the system is something else entirely. The *content* – the data and metadata – are what is really important, and what are unique to each organization, and are deserving of the highest levels of privacy protection. The *content* is not a commodity, and should not be treated as such. The contents of the digital archive reflect the unique way each university carries out its teaching and research mission.

---

[78] Western PIA, 7.
[79] Ibid.
[80] Bo Wandschneider, "Queen's journey to a cloud-connected campus with Office 365," 20 January 2015. https://blogs.office.com/2015/01/20/queens-journey-cloud-connected-campus-office-365/.

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.

This is an unfortunate lapse, because universities are not, like other public bodies, filling only a custodial role with respect to the privacy of the personal information of their users. Privacy is also a necessity to support the principle of academic freedom, which is a necessity for universities to fill their broader social mandate. Threats to the privacy of information do more than expose the university to potential liability; they erode the ability of university faculty to engage in research for the broader social good.

While most PIAs at least acknowledged that faculty in particular were raising concerns about the impact of outsourcing on academic freedom, none significantly engaged with the broader issues or with the moral obligations of universities to protect the ability of their faculty and students to engage in research. While faculty are certainly concerned about protecting their personal privacy, they are far more concerned about threats to academic freedom, which requires, in order to be meaningful, "control and confidentiality of [our] professional information."[81] The privilege of academic freedom is granted to tenured faculty so that they can conduct their research and teaching activities, protected "from dismissal without just cause and rigorous due process."[82]The University of Toronto's mission and purpose statement, passed by its Governing Council in 1992, explains the significance of academic freedom well:

> "Within the unique university context, the most crucial of all human rights are the rights of freedom of speech, academic freedom, and freedom of research. And we affirm that these rights are meaningless unless they entail the right to raise deeply disturbing questions and provocative challenges to the cherished beliefs of society at large and of the university itself."[83]

The extra-national outsourcing of eCommunications presents more than theoretical concerns to academic freedom. As Professor James Turk, former executive director of the Canadian Association of University Teachers explains: "It's about the likelihood that a professor whose research touches on a subject that could be deemed of interest to U.S. security agencies can't write an e-mail about his work without wondering if it will land him on a terrorist watch list – even by accident."[84] Certainly university

---

[81] James Turk, executive director of the Canadian Association of University Teachers, quoted in Dan Michaluk, "Commissioner Cavoukian Says the Patriot Act is 'Nothing," 26 February, 2011. *Slaw*. http://www.slaw.ca.
[82] The Canadian Association of University Teachers, definition of Academic Freedom. http://www.caut.ca/issues-and-campaigns/academic-freedom .
[83] http://www.utoronto.ca/about-uoft/mission-and-purpose
[84] Phillip Todd, "Switch to Google email saves resources, raises privacy concerns" 10 March 2008, http://www.universityaffairs.ca/news/news-article/switch-to-google-email-saves-resources-raises-privacy-concerns/.

faculty internationally also face ongoing challenges to academic freedom. American academics, for example, found themselves increasingly under pressure from governments, corporations and private interest groups following the September 11, 2001 attacks.[85]

Concerns about threats to academic freedom pre-date the eCommunications era. To give just one example, during the 1950s in the United States, the Red Scare saw the wide-spread suspension of civil liberties, when academics, as well as journalists and others were targeted for their political views, including the Holberg-prize winning and internationally lauded historian of the early modern world: Natalie Zemon Davis.[86] As a result of being targeted as a graduate student for challenging the legality and constitutionality of the House Committee on Un-American Activities (HUAC), in 1952 she and her husband lost their passports. She was unable to complete her research in France, and her passport was not returned until 1960.[87] Her husband, mathematician Chandler Davis, lost his faculty position at the University of Michigan for refusing to name names to HUAC; he ultimately served six months in jail from 1959-1960.[88] Even in Canada, left-wing academics and prominent activists have been the subject of RCMP surveillance and harassment before CSIS was created, when "national security" was part of the RCMP's mandate. The list includes Tommy Douglas, now regarded as a principal architect of publically-funded health care in Canada, who also served as Saskatchewan's premier (1944-1961) and later as national leader of the New Democratic Party from 1961-1971, as well as prominent left-wing academics at Canadian universities.[89]

Justifiable concerns about academic freedom are not limited to the past. Not only are there ongoing concerns about the impact of state surveillance, there are also examples of the private sector

---

[85] Beshara Doumani, ed., *Academic Freedom after September 11*, (New York : Zone Books, 2006).

[86] The Holberg International Memorial Prize is the most prestigious award given for outstanding research in the humanities. Awarded by Norway, the prize is worth roughly $750,000 CDN. (http://www.holbergprisen.no/en). Zemon Davis received the prize in 2010 reflecting her lifetime achievement as a social historian of the early modern world.

[87] Natalie Zemon Davis, How the FBI Turned Me On to Rare Books," 30 July 2013 http://www.nybooks.com/blogs/nyrblog/2013/jul/30/fbi-turned-me-on-to-rare-books/.

[88] He served 6 months in jail because, in defending himself he (and two others) did not invoke their Fifth Amendment protection against self-incrimination (for what crime had they committed?), instead relying solely on their First Amendment right to free speech in order to challenge the unconstitutionality of HUAC. They eventually lost their cases in a Supreme Court split decision. Chandler Davis, "The Purge," in Peter Duren, ed. *A Century of Mathematics in America: Part 1*, (Ann Arbor: American Mathematical Society/ University of Michigan, 1988), 412-428. http://www.ams.org/samplings/math-history/math-history .

[89] Douglas was spied on through most of his career. As Whitaker *et al* write of Douglas, who was voted 'the greatest Canadian of all time' in a 2004 national poll," that he was also "the subject of an apparently voluminous RCMP dossier. The declassified security service file on him shows that the Mounties surreptitiously attended his speeches, analyzed his words for evidence of subversion, and even eavesdropped on private conversations." See Reginald Whitaker, Gregory S. Kealey and Andrew Parnaby, *Secret Service: Political Policing in Canada from the Fenians to Fortress America*, (Toronto: University of Toronto Press, 2012), 336. See also the excellent essays in Gary Kinsman, Dieter K. Buse, Mercedes Steedman, eds. *Whose National Security?: Canadian State Surveillance and the Creation of Enemies* (Toronto: Between the Lines Press, 2000) for histories of ordinary individuals who became targets of state surveillance for their political associations. See also Ray Argyle, Steve Hewitt," 'Information believed true': RCMP security intelligence activities on Canadian university campuses and the controversy surrounding them, 1961-71, *The Canadian Historical Review,* 81.2 (Jun 2000): 191-228

attempting to muzzle the findings of researchers, or university administrations attempting the same. Noted cases in Canada include Dr. Nancy Olivieri of the University of Toronto, who found that her research co-sponsor Apotex Inc., abruptly cancelled the drug trial she was conducting and warned of legal consequences should she publish, or "inform patients or anyone else of the risk" the medication posed that she had discovered.[90]

The Canadian Association of University Teachers (CAUT) has expressed concern about the implications of collaborations with private corporations, and found in its own review of twelve major donor agreements, that only two – "the partnership between the University of Toronto and Pierre Lassonde/Goldcorp Inc., and the Balsillie School of International Affairs – are, for the most part, structured in a way so as to preserve academic integrity, protect academic freedom, and encourage the unfettered practice of teaching and learning." In the other ten agreements, the CAUT found that the universities "agreed to various violations of their own academic integrity," including "allowing direct and indirect restrictions on the creation and dissemination of knowledge."[91]

Outsourcing eCommunications to vendors such as Microsoft and Google is equally problematic, as the terms of use for both vendors allow them the right to suspend end user accounts of Customers for a variety of reasons, including actions deemed harmful to the corporations themselves, thus introducing the vendor as an arbiter of what is considered appropriate behaviour for tenured faculty. To give just one example, UNB's initial contract with Live@Edu (the precursor to Microsoft Office 365) gives the corporation the right to "suspend or discontinue the provision of the Live@edu Core Service to any End User" if it believes the End User has engaged in any of the following: "engaged in, facilitated or furthered unlawful conduct" "used the Microsoft Services in any way that harms Microsoft or Microsoft's advertisers, affiliates, resellers, distributors and/or vendors, or any customer of Microsoft or Microsoft's advertisers, affiliates, resellers, distributors, and/or vendors;" in addition to clauses relating to account suspension for hacking, spamming, or disabling the services.[92] The statement granting account suspension privileges for users who have "engaged in, facilitated or furthered unlawful conduct" does not indicate if the user must be charged or convicted of an offense, nor does in indicate which country's laws apply to the interpretation of this clause.

The ability of cloud providers to sub-contract the storage of data outside the United States to third countries such as China about students in Canada's universities should give university administrators particular cause for pause. Canada now hosts an increasing number of international students and international faculty from many countries where intellectual and personal freedom is severely restricted by law.. Vendor service contracts suggest that Microsoft and Google could well be legally obligated upon

---

[90] Jon Thompson, Patricia Baird, Jocelyn Downie, "Report of the Committee of Inquiry on the Case Involving Dr. Nancy Olivieri, the Hospital for Sick Children, the University of Toronto, and Apotex Inc., October 2001 http://www.caut.ca/docs/af-reports-indepedent-committees-of-inquiry/the-olivieri-report.pdf?sfvrsn=0. See the Canadian Association of University Teachers collection of reports of their independent commissions of inquiries into academic freedom cases.

[91] CAUT, *Open for business on what terms? : An analysis of 12 collaborations between Canadian universities and corporations, donors and governments*, 183.

[92] "Microsoft Live@Edu Terms of Use (Organizational NonStandard University of New Brunswick Section 2iii (a), Released under RTIPPA 2015-001, 4.

request to make data stored in third countries available to local authorities, potentially exposing foreign students in Canada to sanctions at home - especially students of the humanities and social sciences should they research or write papers about political, social or religious topics that are taboo at home. In the Chinese example, these might include the 1989 Tiananmen massacre, China's occupation of Tibet or Falun Gong. Student emails to one another might well contain personal information concerning relationships, sexuality, politics or religion that might be frowned upon in their home countries. The privacy assessments and documentation reviewed for this study offer scant, it any, evidence that those Canadian universities who had outsourced considered how third country data storage might compromise the intellectual freedom, or potentially the human rights, of students and international faculty on their campuses – values Canada's learning institutions hold to be essential - even though from the vendor contracts the universities were clearly made aware that the former are allowed to store data outside of the United States, without any qualifications concerning comparable rights or freedoms, save for countries on the US embargo list such as Cuba, North Korea or Iran. [93]

University administrations that have permitted extra-national outsourcing have to date sidestepped the opportunity to meaningfully consider the chilling impact that such outsourcing can have on the academic freedom necessary for faculty and students under their supervision to do their research, and for students to learn, which includes analysis and critique of actions taken today by governments and corporations around the world. Instead, faculty concerns have been minimized in PIAs and in public writings by senior university IT staff about extra-national outsourcing. Well-founded, evidence-based concerns expressed by faculty, including by those expert in the fields of law and privacy, have not been heard, but rather have been characterized as a problem to work around. In these publications, the "similar risk" argument and the "red herring" metaphor also reoccur. For example, in February of 2013, the Associate Vice President of Information Technology Services at the University of New Brunswick observed that "Faculty members in particular are quite sensitive about current jurisdictional issues…We understand that fear, and we also understand that there are facts with which to fight that fear. For instance, Canada and the US exchange information all the time – there are treaties enabling this and groups like CSIS help facilitate it." In the same article, the Associate Vice President of Information Technology at Trent explained that "The Ontario Privacy Commissioner has identified the risks associated with cloud services as a red herring…And even if you do get opposition, it's usually a very small population – maybe 1-2%. It's about how you get around that that's important, and that's by doing your work ahead of time."[94] On a Microsoft sponsored blog in January of 2015, Queen's University's CIO explained that "Having a dialogue with faculty is one of the most important components on the journey to the cloud…everyone has their notions around privacy and confidentiality and it was important to have answers ready to address possible concerns."[95]

[93] The prohibited countries under US Foreign Assets Control legislation are listed in Agreement between Google Apps for Education and the University of Alberta, December 2010, section 1.2. Released under FIPPA 2015-01. This list includes Cuba, Iran, Myanmar, North Korea, Syria and Sudan. Note it is US law applying here. Canada has for example maintained normal relations with Cuba.

[94] http://cuccio.net/news/life-in-the-cloud.php .

[95] https://blogs.office.com/2015/01/20/queens-journey-cloud-connected-campus-office-365/

While the principle of academic freedom is at the foundation of a university's teaching and research mission, in their Privacy Impact Assessments, universities who have outsourced the eCommunications systems have failed to make the connection between the two. Without academic freedom, the mission cannot be fulfilled. As the University of Toronto's Mission and Purpose continues: "It is this human right to radical, critical teaching and research with which the University has a duty above all to be concerned; for there is no one else, no other institution and no other office, in our modern liberal democracy, which is the custodian of this most precious and vulnerable right of the liberated human spirit."[96] "Outsourcing" university IT and senior administrators may have had the best of intentions to provide improved eCommunications services at a lower cost than they could do so themselves. They relied upon the opinions and findings of the Office of the Privacy Commissioner of Canada and their respective Provincial counterparts for their reassurances that extra-national outsourcing, while posing some risks to personal privacy, was compliant with applicable legislation.[97] But a much more important conversation about the importance of academic freedom and the need for Information Technology to support that principle has not yet occurred.

Carleton University's PIA on outsourcing and staff email had perhaps the most pragmatic analysis of the "risk" of faculty concerns about outsourcing, and is worth quoting in full:

> "It may be viewed as an understatement but the use of a service resulting in the storage of email in the United States, especially in a "post-Snowden" world of widespread data collection and surveillance by government, will attract attention from faculty and staff who may have justifiable concerns if stated views attract attention from American authorities. Having said that, this may be characterized as a political risk as opposed to a legal one since the IPC has expressly opined on the subject of FIPPA and the storage of personal information in the United States is permissible provided security measures are adequate."[98]

Carlton's PIA for this project was prepared by a third-party consultant. This analysis indicates the deep gap between University faculty prioritizing and upholding the mission and purpose of the organization while the administration prioritize minimizing costs and legal risks to the organization.

---

[96] http://www.utoronto.ca/about-uoft/mission-and-purpose,

[97] See for example, the Office of the Privacy Commissioner of Canada's publication "Reaching for the Cloud(s): Privacy Issues related to Cloud Computing. https://www.priv.gc.ca/information/research-recherche/2010/cc_201003_e.pdf. This article was cited in the Memorial University PIA, 17. Windsor's PIA quoted Ann Cavoukian's findings regarding Lakehead University in the Jackson article cited in note 13. See Windsor PIA, 10, fn 5.

[98] Raymond Chabot and Grant Thorton, Cygnos Information Security, "Carleton University: Cloud Based E-mail Services (MS Exchange) Privacy Impact Assessment, 2 January 2014. Released Under FIPPA Appeal No. P.A.15-72.

Contract/License Agreement Discussion

Microsoft and Google offer access to their educational SaaS offerings through contracts or license agreements signed between the institution and the vendor. The following charts draw attention to key clauses in current contracts which relate to the privacy implications of extra-national outsourcing. For this comparison, we selected Manitoba's contract with Microsoft and Guelph's contract with Google as being broadly representative of the relevant clauses in each. These contracts are based upon the standard North American contracts used for all educational customers, and they include both the signed agreement between the university and the vendor as well as online documents that form part of the larger agreement. Note that in contracts from both vendors, the "Customer" is the university. Staff, students and faculty are defined as "end users." We did not always receive fully disclosed contracts. Some details, including a least one definition and information about security incident notifications on Microsoft's Volume Licensing Enrollment for Education Solutions were redacted during the FIPPA review process, invoking sections of the legislation covering so-called "third party" information, protecting the confidentiality of the vendor's internal data from disclosure. The Enrollment for Education Solutions document was further amended by terms added [as Section 6], but all of those terms were redacted as well.

Where Data Are Stored

Microsoft Office 365 for Education[99] University of Manitoba: Term 3 years	Google Apps for Education[100] Guelph University
Section 2 c) Transfer of Customer Data. "Customer Data that Microsoft processes on Institution's behalf may be transferred to, or stored and processed in, the United States or any other country in which Microsoft or its Affiliates or subcontractors maintain facilities. Institution appoints Microsoft to perform any such transfer of Customer Data in order to provide Microsoft Online Services." Section 5a v) 2) b. "Microsoft stores copies of Customer Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data is located."	Section 1.1 "As part of providing the Services, Google may transfer, store and process Customer Data in the United States or any other country in which Google or its agents maintain facilities." (p.1) Google includes "end use data" in its definition of Customer data.(p7)

The implications of these sections are clear. Both Microsoft and Google are able to store and move university data in any country in the world in which they or their affiliates do business. The laws of whatever jurisdiction the data are stored in or transited through apply, and in the context of that foreign jurisdiction, the data of Canadians are viewed as belonging to non-citizens, with typically less privacy

[99] For purposes of comparison, we selected the University of Manitoba Contact dated 27 February 2013 as representative of the Microsoft Office 365 for Education contracts. Released via FIPPA UM2015-10.

[100] For purposes of comparison, we selected the University of Guelph Contract dated 9 July 2014 as representative of the Google Apps for Education contract. Released via FIPPA 2015-001.

protection than that given to citizens. The PIAs we reviewed dismissed or minimized this risk with the flawed similar risk argument and a near exclusive focus on the *USA PATRIOT* Act.

Furthermore, the PIAs we reviewed focused nearly exclusively on data storage within the US, even though the contracts indicate otherwise. Data could be exposed to multiple foreign jurisdictions, unnamed and unknown beyond the USA save those countries on the list of embargoed countries such as Iran, Sudan, Cuba and North Korea. The risk is not simply exposure to a single foreign jurisdiction, but to multiple (and unnamed and unknown) foreign jurisdictions in the global cloud.

Data Mining, Targeted Advertising and Metadata Analysis.

Section 1. Definitions of Enrollment for Education Solutions "Customer Data" means all data, including all text, sound, or image files that are provided to Microsoft by or on behalf of Institution through Institutions' use of the Office 365 Services. Specific reference to advertising is in the Microsoft Volume Licensing Online Service Terms April 2015. "Microsoft will not use Customer Data or derive information from it for any advertising or similar commercial purposes," 7.[101]	Definitions: Customer Data "means data, including email, provided, generated, transmitted or displayed via the Services by Customer or End Users "End Users" means the individuals Customer permits to use the services "Customer" is the institution. Section 1.4 "1.4 Ads. (a) Default. The default setting for the Services is one that does not allow Google to serve Ads. Customer may change this setting in the Admin Console, which constitutes Customer's authorization for Google to serve Ads. If Customer enables the serving of Ads, it may revert to the default setting at any time and Google will cease serving Ads "

Another particular concern regarding university outsourcing decisions is the prevention of "mining" email content for keywords that would permit targeted ads to be directed particularly at students. Both Microsoft and Google assert that they do not target ads to students in their educational products and neither have "pop up" ads that appear when students are using their respective services. However, Google has been the subject of lawsuits alleging violation of this principle. The lawsuits allege that data is collected through Google Apps for Education about users, not with the intention of targeting ads when the user is working within the Google Apps for Education environment, but for adding to the user's Google database profile so when the user moves off to another site a targeted ad will appear.[102]

[101] http://www.microsoft.com/en-ca/Licensing/product-licensing/products.aspx. This document forms part of the agreement with universities.

[102] "Google: don't expect privacy when sending to Gmail "14 August 2013, http://www.theguardian.com/technology/2013/aug/14/google-gmail-users-privacy-email-lawsuit; "Google faces lawsuit over email scanning and student data," The Guardian, http://www.theguardian.com/technology/2014/mar/19/google-lawsuit-email-scanning-student-data-apps-

Both agreements do permit the mining of alumni email for the purpose of serving targeted advertisements.

In addition, a closer reading of the contract wording of both vendors raises the crucial question of whether the restrictions on data mining are specifically limited to data, or also include metadata. Metadata is the data about the data, and is anything that can be defined algorithmically from the content of the message, for example, how many times person A wrote an email to person B, when they did so, etc. (i.e. the patterns of communication). In the context of email, for example, metadata is also the to/from/date/subject information. In the context of a document, metadata can be the title of the document, stored keywords, date of creation, editing history, etc. Metadata, because it is structured data, is easily mined and can be used for all sorts of purposes. Metadata can be analyzed to reveal patterns and habits of work. But is metadata created by the Software-as-a-Service provided by an outsourcing vendor covered under the definition of "customer Data?" While more research is clearly needed, it does not appear from the contract language to be the case. And is traffic data – the log files which reveal the paths information took—also Customer data? Contract reading suggests not. As Google's own terms of use on Intellectual property Section 6.1 states, "As between the parties, Customer owns all Intellectual Property Rights in Customer Data, and Google owns all intellectual property rights in the Services"[103] which appears to include data *about* customer data that is in fact created by the software and not by the end user.

In short, the contracts are not clear about the important distinctions between data and metadata, and who owns what. These questions about metadata use are beyond the scope of this current project, but need to be addressed. It is important to note that Microsoft and Google both sell Business Intelligence solutions so that organizations can analyze such data themselves; unless contract language expressly prohibits the use and/or disclosure of metadata or traffic data, Microsoft or Google would be free to do so, either to disclose or sell access to the metadata to third parties. Furthermore, as Lisa Austin and Daniel Carens-Nedelsky note in their report (Appendix B), while the Canadian courts have protected the privacy of metadata in the context of lawful access requests, the US courts have said that the Constitutional 4th amendment protections do not apply to metadata.[104] And as noted Princeton University Computer Science professor Edward Felten made clear in is his testimony to the US Congress on the dangers of metadata mining posed by the FISA Amendments Act of 2008, metadata, which is highly structured data, is actually far more useful for analysis purposes than content data, and easily used by automated systems, for a whole range of purposes, including bulk surveillance.[105]

---

education; Benjamin Harold, Google Under Fire For Data-Mining Student Email Messages," *Education Week,* 13 March 2014, http://www.edweek.org/ew/articles/2014/03/13/26google.h33.html.

[103] OCAD Google Apps for Education Contract. Released under FOI 2015-01, 3.

[104] Lisa Austin and Daniel Carens-Nedelsky, "Why Jurisdiction Still Matters," "Appendix B, Seeing Through The Cloud", 6-8.

[105] United States Senate. Committee on the Judiciary Hearing on the Continued Oversight of the Foreign Intelligence Surveillance Act. Written Testimony of Edward W. Felten, Professor of Computer Science and Public Affairs, Princeton University. October 2, 2013. http://www.cs.princeton.edu/~felten/testimony-2013-10-02.pdf

Third Party Requests, Law Enforcement Requests

Microsoft Office 365 for Education	Google Apps for Education
Section 2 b iii). P. 1 "Microsoft will not disclose Customer Data to law enforcement unless required by law. Should law enforcement contact Microsoft with a demand for Customer Data, it will attempt to redirect the law enforcement agency to request it directly from Institution. As part of this effort, Microsoft may provide Institution's basic contact information to the agency. If compelled to disclose Customer Data to law enforcement, Microsoft will use commercially reasonable efforts to notify the institution in advance of a disclosure unless legally prohibited."p1-2.	Section 2.7. Third Party Requests. Customer is responsible for responding to Third Party Requests. Google will, to the extent allowed by law and by the terms of the Third Party Request: (a) promptly notify Customer of its receipt of a Third Party Request; (b) comply with Customer's reasonable requests regarding its efforts to oppose a Third Party Request; and (c) provide Customer with the information or tools required for Customer to respond to the Third Party Request. Customer will first seek to obtain the information required to respond to the Third Party Request on its own, and will contact Google only if it cannot reasonably obtain such information."

These clauses indicate the terms under which Microsoft and Google will respond to requests for information. Microsoft uses the term "law enforcement" but neither defines the term nor defines which country's law enforcement agencies apply. Google uses the even broader term "Third Party Requests." Both indicate that they will inform the customer of the request, but only if permitted by law. If the law of the requesting country prohibits even disclosing the request (as is the case with some US requests, such as security letters) then the university customer will never know about whose data was requested. Carleton University's PIA warned that this contract language with respect to "law enforcement" is "broad, vague and provides Microsoft with much discretion." The PIA authors suggested that "Carleton may wish to clarify the contract language to better specify the circumstances where Microsoft should 'respond to lawful requests or legal processes."[106] However, Microsoft and Google customers using the "free" educational offerings are provided with the standard volume licenses for the North American educational market. Neither corporation appears to be, from the contracts we have seen, tailoring the wording to suit the particular needs of those using its service free of charge. There were redacted portions in the Microsoft agreements that could possibly have contained such amendments but this is speculation only.

[106] Carleton PIA, 5.

How did outsourcing to the cloud come to seem like a sensible option?

University outsourcing decisions did not occur in a vacuum. As we examined the PIA documents in the context of the timeline of outsourcing decisions, it became clear that multiple factors reinforced the decision to outsource eCommunications. Lakehead University's experiences were pivotal, not only because Lakehead was the first Canadian University (in 2006) to outsource their eCommunications to either Microsoft or Google (in their case, Google), but also because the faculty association lost its challenge to the decision in mediation. The mediation decision, widely referenced in the PIA documents, asserted both the similar risk analysis and the "email is like a postcard" analogy.

Federal and provincial privacy commissioners and privacy experts also played a key role. While most privacy commissioners were not actively endorsing outsourcing, findings in particular cases where outsourcing of some personal information was acceptable, were generalized to more privacy-sensitive systems such as email and eCommunications over time. In addition, presentations and writing by privacy experts (that also repeated the similar risk argument) further reassured universities that the benefits of extra-national outsourcing outweighed the risks. Finally, the experiences of other universities were frequently cited, and there is ample evidence that universities were sharing information with each other that served to reinforce, rather than encourage critical interrogation of, key assumptions.

The Lakehead Case

Lakehead University was an early and influential adopter, launching its Google service late in 2006[107] Lakehead's Faculty Association initially did not appear overly concerned about the migration, as they had negotiated language respecting privacy of their electronic data as part of their collective agreement.[108] They became concerned however, following the roll-out of the service, when faculty were required to consent to Google's terms of service, which included the following clause:

> "*By using Google services, you acknowledge and agree that Google may access, preserve, and disclose your account information and any Content associated with that account if required to do so by law or in a good faith belief that such access preservation or disclosure is reasonably necessary to: (a) satisfy any applicable law, regulation, legal process or enforceable governmental request, (b) enforce the Terms, including investigation of potential violations hereof, (c) detect, prevent, or otherwise address fraud, security or technical issues (including, without limitation, the filtering of spam), or (d) protect against imminent harm to the rights, property or safety of Google, its users or the public as required or permitted by law.*"

The union then filed a grievance on grounds of concern about privacy violations and the threat such violations posed to the principle of academic freedom. The Association noted that members were now exposed to surveillance activities under the *Foreign Intelligence Surveillance Act*, the *USA PATRIOT Act* and the *Protect America Act*. In order to use the service, faculty would have to accept Google's "terms of

---

[107] Phillip Todd, "Switch to Google email saves resources, raises privacy concerns" 10 March 2008, http://www.universityaffairs.ca/news/news-article/switch-to-google-email-saves-resources-raises-privacy-concerns/.

[108] Article 16.01.03 of the Lakehead University Collective Agreement acknowledges that faculty members "*have the right to privacy in their personal and professional communications and files, whether on paper or in electronic form.*"

use" which both "allowed access to their e-mail pursuant to U.S. laws and subjected them to potential prosecution pursuant to that legislation."[109]

The case went to arbitration, and the mediator, Toronto lawyer Joseph Carrier, ruled against the union, in favour of outsourcing. Mr. Carrier acknowledged the legitimacy of faculty concerns, but concluded in favour of the University because according to the terms of the collective agreement with the Union, the University was not technically obligated to provide "an email service or system." Although it was required to provide a computer and a "computer connection," a specific application such as "email" was not itemized. With respect to the question of privacy and academic freedom, the arbiter further accepted the argument of the University as presented by Michael Pawlowski (Lakehead Vice-President, Administration & Finance) "that e-mail messages were no more private than a postcard." In other words, faculty could have no expectation of privacy with email.

The arbiter further noted that no evidence had been presented to show that "comprehensive email privacy is technologically achievable".[110] The arbiter also accepted the "similar risk" argument provided by Ottawa University professor Michael Geist. In the end however, his ruling centred not on the larger questions of privacy or the principles of academic freedom, but on the wording of the collective agreement, which did not explicitly include email. Furthermore, the entire discussion focused on the question of email, even though the services that Google provided also included document storage and online collaboration tools.

In other words, Google offered an entire suite of software that fundamentally changed the ways in which people at Lakehead would work and in what legal jurisdiction the records of that work would be archived, but the arbitration decision focused exclusively on email.

The Role of Vendors

While the education market in Canada is a tiny fraction of this global sector, vendors see it as an important one. Vendors offer services to universities free of charge or at low cost with the intention of influencing that important consumer sector: the student. As one Microsoft Account executive explains "At Microsoft, we invest heavily in Canadian education and it is one of our most strategic verticals[111]" From the PIAs we examined, it is clear that the senior Academic and IT leadership within Canadian universities moved more cautiously to outsource than many of their US and International counterparts, but in the end they were satisfied that the "similar risk" argument nullified privacy concerns raised by faculty. It is also clear that vendors are well aware of differing provincial privacy laws around

[109] See Arbitration Award between the Board of Governors of Lakehead University and the Lakehead Faculty Association in the Matter of the Grievance Respecting the Right of Privacy and Academic Freedom of Faculty Members in their Electronic Communications. http://www.canlii.org/en/on/onla/doc/2009/2009canlii24632/2009canlii24632.pdf. 11 May 2009, 2.

[110] See Arbitration Award between the Board of Governors of Lakehead University and the Lakehead Faculty Association in the Matter of the Grievance Respecting the Right of Privacy and Academic Freedom of Faculty Members in their Electronic Communications. http://www.canlii.org/en/on/onla/doc/2009/2009canlii24632/2009canlii24632.pdf. 11 May 2009.

[111] Mat Burke, Account Executive, Microsoft; https://www.bc.net/bcnet-members-unite-establish-sector-wide-strategic-alliance-microsoft.

outsourcing. As one vendor selling to the Canadian market (a reseller for Salesforce.com, another cloud SaaS offering) noted in a company-sponsored blog, "except for a couple of special cases imposed on provincial public sector agencies, there is no fundamental impediment to storing data in the cloud, regardless of where the data centres supporting that cloud physically reside. Privacy commissions have published a large body of supporting information that reinforces this point, and offer a strong set of resources to help have this conversation internally."[112]

Both Google and Microsoft produce "resources" or "white papers", often cited in PIAs, to help customers provide answers to their user communities about the new service. Vendor assertions in what are effectively marketing materials were thus used to construct arguments in support of the acquisition of the new service. This is not a strategy limited to vendors and universities but is practiced in the private sector as well. For example, cloud providers claim in their marketing materials that they can provide better protection against hacker attacks and therefore reduce an organization's potential financial liability. These assertions find their way into privacy impact assessments as facts. As the Salesforce reseller quoted above asserted in respect to this issue: "for the vast, vast majority of organizations the cloud offers a much higher degree of security as compared to the limited resources and capabilities that most organizations have to support their own infrastructure." That this is part of the marketing argument, the reseller went on to explain how "First-tier cloud service providers have well-rehearsed and practiced dialogues for having these conversations during the sales cycle."[113] In other words, the vendor sales team are prepared to help your organization address concerns about privacy and security issues, and may even help with the writing of the organization's PIA or threat risk assessment in order to acquire your business.[114]

Vendors deploy other marketing strategies to encourage adoption of their services. As the University of Toronto was considering whether to migrate faculty and staff to Office 365 in the fall of 2013, a full page ad from Microsoft in the Business Section of the Globe and Mail, announcing "Queen's is now on Office 365: Your complete office in the cloud.[115]" But a more common practice is the publication of "case studies" on vendor websites which tout the ease of migration and the benefits to be gained from contracting with the vendor's services. [116] There are even a few YouTube videos featuring customers

[112] Tim Hopkins, Managing Director, NTT Centerstance Canada, "Approaching Data Residency for Canadian Organizations," 20 June 2013. https://centerstance.wordpress.com/2013/06/20/approaching-data-residency-for-canadian-organizations/.
[113] Ibid.
[114] This was the case with U of T's IRRM, which listed Microsoft staff as contributors to the document. University of Toronto Information Risk and Risk Management, "Staff and Faculty e-Communications Outsourcing Project," August 7, 2014. Online at http://main.its.utoronto.ca/wp-content/uploads/2014/08/Office365-Staff-Faculty-IRRM-2014_0807-v2-0-9a.pdf
[115] The complete (and short, but large font advertisement) reads "When managing 45,000 users, having a fully collaborative work environment is a prerequisite. That's why Queen's University is now on Office 365. Its cloud based environment helps students, faculty and staff communicate better across the devices of their choice, be it PCs, laptops or mobile phones. With the help of Office 365 exceptional service is a guarantee for the people at Queen's. Nowonoffice365.ca." 20 November 2013, *The Globe and* Mail, B7.
[116] Microsoft Canada, "University Improves Student Services, Saves IT Costs with Cloud-Based Email," 9 April 2012, http://www.microsoft.com/canada/casestudies/Case_Study_Detail. (note this case study has been removed from Microsoft's website as of writing). Andrew Perchaluk and Lia De Cicco-Remu, "The University of Manitoba

describing their eCommunications adoption successes, one produced by Microsoft in particular featuring Queen's University's experiences. [117] Google also uses case studies, but does not appear to do so to the same extent that Microsoft does.[118] Microsoft has sponsored "Partners in Learning" which produces what looks like an independent "newsletter" of case use stories, and is now the Microsoft Educator Network. Google sponsors Learning Communities. In both cases the vendors provide places for customers to share their experiences and successes with the products. In these "booster" marketing materials one can find similar arguments to the ones described above in the rationalization for outsourcing, that in-house solutions were end of life, and that millennial students' technology expectations would be met with the vendor's solutions. The materials also tout the cost-savings to be realized, the productivity gains to be made, and the better security that will be provided. What such materials do not provide of course is independent, arms-length, critical assessments of the strengths and weaknesses of the product. They are instead sales pitches and/or endorsements of the products in question.

Leading by Example and Drawing on the Experiences of Peers

Vendor sales pitches and marketing materials may have been persuasive, but not exclusively so. Universities could look to the experiences of US universities, many of whom began outsourcing as soon as the services became available. After Lakehead outsourced successfully, other Canadian universities began to consider the option, and their leadership could share their own experiences of improved services and cost-efficiencies with each other. One important venue where such conversations occur is the Canadian University Council of CIOs (CUCCIO), which incorporated in 2006, including at its annual conference, CANHEIT (Canadian Higher Education Information Technology). The successful roll-out of Lakehead's new Google Apps for Education eCommunications service, the positive response of students, the mediation decision, and the reported cost savings prompted many universities across Canada to take a closer look at the new possibilities. CUCCCIO's website has featured news-type articles from other universities who have also outsourced, and more recent PIAs typically include statements citing the success of Canadian peer institutions that had already made the transition.[119]

Presentations at CANHEIT and to CUCCIO members can also influence IT decision makers or support IT decision making. One in particular which addressed the privacy implications of extra-national outsourcing was given in 2010 by David Fraser, a privacy lawyer with McInnes Cooper. While careful to say that his presentation did not comprise legal advice, verbatim and near verbatim excerpts from this presentation's slide deck occur in at least one PIA, including the assertion that "Canadian authorities can

---

Leverages Microsoft Office 365: Replacing an Outdated Email Solution," *PiL Best Practices Newsletter*, 1 May 2014, Bo Wandschneider, "Queen's journey to a cloud-connected campus with Office 365," 20 January 2015. https://blogs.office.com/2015/01/20/queens-journey-cloud-connected-campus-office-365/.

[117] Queens. https://www.youtube.com/watch?v=fnXYZvNHAZo. U of T https://www.youtube.com/watch?v=Pk_dVTYQe00.

[118] http://www.google.ca/edu/case-studies/.

[119] "Is life better in the cloud? These three universities think so," 31 March 2014, http://cuccio.net/news/life-in-the-cloud.php

get information in the US without a warrant and American authorities can get information in Canada without a warrant."[120]

The PIAs themselves also reveal the importance of inter-university information exchange about eCommunications Outsourcing. The University of New Brunswick, for example, informed us that instead of writing its own PIA, UNB "instead relied upon the PIAs produced by many other schools to inform our decision-makers about the process around Live@edu and Office365 (the next generation of Live@edu).[121] OCAD noted in its PIA that its decision to agree with Google about the terms of the contract being covered by New York state law "was based on the University of Alberta's legal assessment that New York State privacy laws are considered to be similar to Canadian privacy legislation."[122] For smaller schools in particular, consulting with and relying on the expertise of larger Canadian universities seems an understandable and cost-effective option.

Larger schools also took this route, and referenced the experience of other Canadian universities in their PIAs. The University of Toronto, for example, followed Alberta's experiences closely when outsourcing student email, and referenced Alberta, Ryerson, Dalhousie, Queen's and Lakehead's successes in the Risk Management document for the planned faculty/staff outsourcing.[123] Queen's consulted with the University of Toronto's CIO about how to manage conversations with faculty, and "colleagues at Dalhousie in Halifax to see how they dealt with security and privacy issues in a province that has stricter privacy rules than Ontario."[124] Western University looked globally, noting that "thousands of Universities worldwide have outsourced email services" but it also pointed specifically to other Canadian universities, naming Queens, U of T, Dalhousie, Lakehead, Carleton and the University of Alberta, citing the fact that " a majority of Canadian universities are either moving or are considering a move to the cloud based email for students." Western could have confidence that these other schools had "assessed the privacy implications to the students and deemed the solutions to be acceptable for delivering the service. Being a late entrant in the cloud email space affords western the opportunity benefit from the experiences of others through consultation at both the technical and legal level."[125] York provided an appendix listing all Ontario universities who had outsourced and to whom, and also noted that "the vast majority of American universities and colleges have moved to third-party email providers."[126]

In short, the PIAs reveal a great deal about the extent of cooperation and collaboration between senior IT staff at the universities in our sample set. Such shared expertise can be highly beneficial, but it can

---

[120] http://www.unb.ca/its/_resources/pdf/about-its/privacy-cloud-davidfraser.pdf, see especially slide 49.
[121] Email from Sarah DeVarenne, University Secretary and Head under the Right to Information and Protection of Privacy Act, University of New Brunswick to Heidi Bohaker, 3 February 2015.
[122] OCAD PIA, 9.
[123] University of Toronto, "Privacy Impact Assessment: Student e-Communications Outsourcing Project," 30 May 2011, 7, http://main.its.utoronto.ca/wp-content/uploads/2013/09/E-mail-Privacy-Impact-Assessment-v3.1.pdf. University of Toronto Information Risk and Risk Management, "Staff and Faculty e-Communications Outsourcing Project," August 7, 2014, 10. http://main.its.utoronto.ca/wp-content/uploads/2014/08/Office365-Staff-Faculty-IRRM-2014_0807-v2-0-9a.pdf
[124] Bo Wandschneider, "Queen's journey to a cloud-connected campus with Office 365," 20 January 2015. https://blogs.office.com/2015/01/20/queens-journey-cloud-connected-campus-office-365/.
[125] Western PIA page 2.
[126] York PIA, page27.

also lead to the spread and acceptance of unexamined assertions. Reinforcing these assertions though were privacy experts who also accepted the similar risk argument, and privacy commissioners who also shared these beliefs.

The Role of Privacy Commissioners

Privacy Commissioners also contributed to the widespread acceptance of the similar risk argument. Certainly the Lakehead decision was pivotal, and was subsequently cited by other Canadian universities in support of their outsourcing decisions. But universities also found support for their plans in decisions of the federal and various provincial privacy commissioners; University of Alberta formally sought the advice of its commissioner before outsourcing. At the federal level, in a review of complaints concerning transborder data flows for CIBC (2005) and Canada.com (2008), the Office of the Privacy Commission also accepted the similar risk argument.[127]

Ann Cavoukian, Ontario's provincial privacy commissioner from 1997-2014, was particularly influential in subsequent university decisions. She publically concluded that extra-national outsourcing was not necessarily in conflict with Ontario's provincial privacy statute, and that concerns about the USA PATRIOT ACT were unfounded.[128] Commissioner Cavoukian explicitly supported the Lakehead decision, noting in 2008 that "there's no problem with Lakehead outsourcing to Google so long as they did their due diligence on the contractual agreement made regarding usage of the data." She went on in the same interview to assert that "Fears associated with the [US] Patriot Act are grossly exaggerated… It's like this big bogeyman in the room…This is a theoretical situation that might happen to your data residing in the U.S."[129]

In 2012, she confirmed this formally in her report on the outsourcing of the Ontario Ministry of Natural Resources Hunting and Fishing Licensing system to a US-based provider.[130] In so doing she drew on the earlier findings of the federal Privacy Commissioner cited above and privacy experts such as Michael Geist, Canada Research Chair in Internet and eCommerce law at the University of Ottawa, and Canadian privacy lawyer David T. Fraser. Commissioner Cavoukian then went further. At a 2011 symposium titled "Exploring the Future of E-mail, Privacy, and Cloud Computing at Ryerson University," she noted that outsourcing "is your decision. But don't let things like the Patriot Act...I mean, it's just such a red herring. It's nothing…Whether you have the Patriot Act or not it doesn't matter. There will always be law

---

[127] Office of the Privacy Commissioner of Canada, PIPEDA Case Summary #2005-313. "Bank's notification to customers triggers PATRIOT Act concerns." Issued October 19, 2005; PIPEDA Case Summary #2008-394. "Outsourcing of canada.com e-mail services to U.S.-based firm raises questions for subscribers." Issued August 7, 2008. https://www.priv.gc.ca/cf-dc/2008/394_20080807_e.asp .

[128] Dan Michaluk, "Commissioner Cavoukian Says the Patriot Act is 'Nothing," 26 February, 2011. Slaw. http://www.slaw.ca. Commissioner Cavoukian was widely quoted during her tenure supporting outsourcing decisions as long as the institution or organization recognized that it retained accountability for personal information.

[129] Brian Jackson, "Privacy controversy mars Google Apps rollout at Canadian university," 7 November 2008, http://www.itbusiness.ca/news/privacy-controversy-mars-google-apps-rollout-at-canadian-university/4999. Dr. Cavoukian was widely quoted during her tenure supporting outsourcing decisions as long as the institution or organization recognized that it retained accountability.

[130] *Reviewing the Licensing Automation System of the Ministry of Natural Resources: A Special Investigation Report* (27 June 2012), PC12-39, https://www.ipc.on.ca/images/Findings/2012-06-28-MNR_report.pdf .

enforcement methods and techniques that will access certain types of information here, there and everywhere. What you should concern yourself with is the kind of accountability that you will be able to maintain if your e-mail systems go into the cloud. That's what would concern me."[131] As Lisa Austin and Daniel Carens-Nedelsky convincingly demonstrate, in the post Snowden world such ideas, and the outsourcing decisions they supported, must be thoroughly examined.[132]

Commissioner Cavoukian's words have carried significant weight, evident particularly in Ontario PIAs. Queen's University's PIA, also prepared by an outside consultant, referred to Commissioner Cavoukian's influence, noting that "The Privacy Commission of Ontario has conducted significant research in the area of cloud computing, supported and commented on the work of others in his field. She believes that optimized system functionality available in the cloud and privacy can be delivered in unison by employing Privacy By Design," referring here to Commissioner Cavoukian's own publication on the subject. [133] York, Ryerson and the University of Toronto all followed the Privacy By Design (PbD) model developed by Commissioner Cavoukian in their Privacy Impact Assessments.[134] The PbD model contains a fine set of privacy protective principles, and is used as a privacy protective standard internationally, but unfortunately does not address the crucial jurisdiction issue identified by Lisa Austin and Daniel Carens-Nedelsky.[135]

Alberta's Privacy Commissioner was also consulted by the University of Alberta prior to its decision to outsource to Gmail. In a series of letters exchanged in 2010 between the University and Alberta's Office of the Information and Privacy Commission (volunteered by the University in addition to the materials requested under the FIPPA request), not only did the University undertake a thorough Privacy Impact Assessment, but they had their assessment reviewed by the Commission to ensure that "the University has made reasonable efforts to protect the privacy and ensure compliance with access to information provisions of the Act."[136] While the Commission in its response reminded the University that it could not "contract out" of its obligations under the FOIP Act and that the outsourcing organization bears both the

---

[131] Dan Michaluk, "Commissioner Cavoukian Says the Patriot Act is 'Nothing," 26 February, 2011. *Slaw*. http://www.slaw.ca. Ryerson's conference was also influential on outsourcing decisions, as attendees included representatives from other universities also exploring outsourcing. Other speakers included Fred Carter of Ontario's Information and Privacy Commission (IPC), James Turk, Executive Director of the Canadian Association of University Teachers, and David Fraser, a privacy lawyer who speaks regularly on the risks of outsourcing. At the Ryerson event, according to Michaluk, Fraser "made the argument that there is no significant incremental risk associated with exposing e-mail to American domestic intelligence laws given our own laws."

[132] Austin and Carens-Nedelsky, "Why Jurisdiction Still Matters," http://ecommoutsourcing.ischool.utoronto.ca/.

[133] Queen's PIA, 53.

[134] York PIA; University of Toronto Information Risk and Risk Management. "Staff and Faculty eCommunications Outsourcing Project," August 7, 2014. Appendix B. http://main.its.utoronto.ca/wp-content/uploads/2014/08/Office365-Staff-Faculty-IRRM-2014_0807-v2-0-9a.pdf For Ryerson see Jim Buchanan, "Email and Collaboration Tools Privacy Impact Assessment," April 2, 2015. http://email.blog.ryerson.ca/2015/04/02/email-and-collaboration-tools-privacy-impact-assessment/.

[135] See Ke Zengand Ann Cavoukian. *Modelling Cloud Computing Architecture Without Compromising Privacy: A Privacy by Design Approach.* Toronto: Information and Privacy Commissioner of Ontario, 2010, and the *Privacy By Design* website for additional resources: https://privacybydesign.ca/.

[136] Letter from Harry Davis, Access and Privacy Advisor, University of Alberta, to the Alberta Privacy Commssioner, 8 January 2010, Released under FIPPA 2015-01, 1.

responsibility for the decision and any consequences of the decision, it did not advise against extra-national outsourcing. Rather, the Commission's letter repeated the assertion that email "is not a very secure form of communication" and recommended that the University take steps to train staff about how to protect personal information when it is stored extra nationally, and advise users when they sign up for the service that the University cannot "guarantee protection against possible secret disclosures of information to a foreign authority as a consequence of foreign laws."[137]

Alberta's OPC's response to the University of Alberta's plan was more much conservative that Ontario's Commissioner Cavoukian's statement's about Lakehead's plan, and her assertion that the *USA PATRIOT ACT* "was nothing." Nonetheless Alberta's Privacy Commissioner reviewed the University of Alberta's Privacy Risk Analysis, which contained the following reassuring sentence: "Both the Privacy Commissioner of Canada and Alberta has issued guidance on the implication of the *USA PATRIOT ACT* on outsourcing. They acknowledge that the Patriot Act is consistent with the laws in the United States and Canada and elsewhere that allow governments to seek information about individuals in connection with intelligence activities." [138]

In these cases where the universities pointed to the Privacy Commissioners as having issued guidance, the Privacy Commissioners in turn reminded the Universities that they could not outsource their obligations. In Alberta's case, the Privacy Commissioner did not endorse the decision to outsource, but did not oppose it either. But without a statutory bar, how could Privacy Commissioners prohibit outsourcing? Furthermore, with the exception of British Columbia, the similar risk argument seemed persuasive and was accepted widely.[139] Given that Alberta and Ontario's provincial privacy commissioners found outsourcing to the "public cloud" as consistent with meeting statutory requirements for the privacy protection of personal information under their respective provincial legislation, the choice for outsourcing, and its purported financial savings, seemed a clear and pragmatic decision.

Upon review it appears that the conversations between privacy commissioners and universities about outsourcing occupied a fuzzy borderland of their own between technology and law. Universities appear to have been doing due diligence by seeking advice, and privacy commissioners appear likewise to have been acting in good faith in accordance with the law. But a widely accepted and unchallenged set of assertions, coupled with the attractive cost savings to be realized by the new technologies, appears to lie behind the choice of extra-national outsourcing as a sensible one for Canadian universities. The release of classified documents by Edward Snowden in June of 2013 *should* have forced a re-examination of those assertions, and yet curiously this has not occurred.

---

[137] Letter from Alberta Privacy Commissioner to University of Alberta Provost and VP Academic (Carl G. Amhrein), 2 March 2010, Released under FIPPA 2015-01, 4-5.
[138] Alberta PIA, 10.
[139] See the findings in 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.

The PIAs we reviewed gave limited or no consideration to the privacy and security implications of mass surveillance activities by the United States National Security Agency (NSA) that was clearly laid out in US law well before 2013. We now know from the Snowden documents, that far from being a theoretical risk, the NSA's PRISM program is engaged in the bulk and warrantless collection of data stored by Internet service providers. Furthermore, mention of Canada's own surveillance apparatus, the Communications Security Establishment (CSE) was typically brought up only in support of the "similar risk" argument, (as in "look, Canada is undertaking electronic surveillance too") rather than in any substantive engagement with the different statutory terms under which the data of Canadians can be collected under Canadian law, even including the newly passed C-51. 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. This seems an especially curious lapse.

Conclusion

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 have looked to the outsourcing on offer as a 'win' on multiple levels: a decision that reduces risk to the institution, provides significantly enhanced services and redirects cost savings towards other badly needed services. However, with the findings of our research, and particularly in light of Austin and Carens-Nedelsky' s refutation of the "similar risk" argument, Canadian Universities who have outsourced need to reconsider their decisions. Privacy impact assessments should no longer rely upon the Lakehead arbitration ruling, the similar risk argument, or the assertion that email is fundamentally insecure.

Universities must not seek to lower the privacy expectations of their users below the standard upheld by Canada's Supreme Court. Universities should instead look to research other models, and consider whether approaches such as non-profit cloud consortia, such as BC-Net, which provides cloud computing services to British Columbia's provincial institutions, are a cost-effective way to provide the benefits of cloud technology to Canadian universities while keeping data within Canada. Provinces will also need to review their own privacy legislation, and consider changes to funding models that would permit universities to provide secure and private eCommunications services to their faculty, staff and students.

Universities should also reconsider the long-term impact of extra-national outsourcing on their mission and purpose, and the principle of academic freedom. Canada's leading universities should not be trying to play "catch up" with corporate IT trends, but rather should be leading, drawing from their internal strengths in the sciences, law, humanities and social sciences to ensure that in this new digital age, technology continues to serve the public good and our democratic institutions and does not contribute to the loss of hard-won and constitutionally-protected rights.

While the focus of this study 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 outsourcing. 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.