A Framework for Canadian Organizations Assessing Privacy Implications of Extra-National Outsourcing[1]

Principal Author: Stephanie Perrin

Contributing Editors: Andrew Clement, Heidi Bohaker

Preamble

Moving to the Cloud? Thinking about moving your organization's electronic communications to servers located outside of Canada? How should your organization assess the implications of doing so? To what extent have ongoing revelations about the extent of state surveillance and its legal basis changed the risk assessment landscape?

Many Canadian companies and organizations have already outsourced electronic communications – or eCommunications – services to vendors based outside of Canada, while others are considering this option to both save money and enhance service.

This framework document, developed as part of a research project funded by the Office of the Privacy Commissioner of Canada's 2014-2015 Contributions programcontains a process, as well as key questions, in order to assist Canadian organizations with the privacy and security implications of their eCommunications outsourcing decisions.

Important in this analysis is the differentiation between the risks inherent in all email and communications systems currently, the risk in outsourcing, and the additional risk in outsourcing in such a way as to place large data holdings outside Canada, subject to foreign control. Once outside the jurisdiction of Canadian Courts and data protection provisions, even when one considers the somewhat limited scrutiny of security and intelligence functions currently within Canada (and its potential further erosion with Bill-C51 as of writing) the risks increase dramatically and in ways that are difficult to predict and control. A framework is required to put these clustered risks in perspective.

---

[1] Stephanie Perrin, with Andrew Clement and Heidi Bohaker, A Framework for Canadian Organizations Assessing Privacy for Extra-National Outsourcing of eCommunications Services," August 2015. This document 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 E of the final report. The complete project findings and recommendations are available at http://ecommoutsourcing.ischool.utoronto.ca/. This project has been funded by the Office of the Privacy Commissioner of Canada (OPC); the views expressed herein are those of the author(s) and do not necessarily reflect those of the OPC.

A Three-Tiered Approach to Understanding eCommunications Risks

1) Privacy Risks Inherent in eCommunications Systems

While one popular meme in wide circulation asserts that “email is fundamentally insecure,” and another that “one should only write in an email that which one would put on a postcard,” the fact is that Canadians increasingly rely on eCommunications systems, including email, instant messaging, Facebook, Twitter, VoIP and other services for private and confidential communication. Saying that “email is fundamentally insecure” obscures the contemporary complexity of our eCommunications practices. Furthermore, there is no need for such services to be insecure at all, especially eCommunications internal to an organization. Business enterprises and government agencies deploy a range of strategies to keep their corporate communications private, including guarding against the basic risk of people using untrusted equipment, or hardware devices brought from home. Here are some of the ways that they do so:

- By strictly controlling the hardware that staff use
- By strictly controlling the applications available to staff on company equipment
- By severely restricting the use of separable media (memory sticks, backup disks, etc.)
- By monitoring for the presence or use of any of the above
- By issuing strict policies about the use of equipment, including during travel, where the devices may be connected to the network, etc.
- By managing their own secure networks
- By operating their own eCommunications services
- By engaging in user training and conducting regular audits of logs to avoid and detect such things as inappropriate external forwarding of private and/or confidential information.
- By insisting on the use of strong end to end encryption, and maintaining tight control of keys and other access points.

Before we leave this section on technical measures, it is worth noting that the UN Special Rapporteur on Freedom of Expression has published a ground breaking report on the use of

encryption and the right to anonymity, in the meeting of the Human Rights Council of June 15 2015[2]. This report eloquently outlines the importance of encryption to uphold a cluster of human rights, and calls on public authorities to promote it:

> Encryption and anonymity, and the security concepts behind them, provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age. Such security may be essential for the exercise of other rights, including economic rights, privacy, due process, freedom of peaceful assembly and association, and the right to life and bodily integrity. Because of their importance to the rights to freedom of opinion and expression, restrictions on encryption and anonymity must be strictly limited according to principles of legality, necessity, proportionality and legitimacy in objective. (p.19)

He goes on to make several recommendations to states, organizations, and civil society , that they undertake measures to promote and protect the right of encryption and of anonymity, and focus on the defence of human rights in the use of these cryptographic rules, rather than the threat of criminality.

Many other institutions in the broader public sector, particularly in the education sector, as well as small businesses, non-profit organizations and the general public, do not typically take the above steps, principally for cost considerations. Nevertheless, the threats remain, and without adequate care, users' private data is at considerable risk of exposure.

Communications over telecom networks are already exposed to a number of risks, notably:

- Accessibility in switching equipment
- Deep packet inspection
- Transit through foreign countries
- Data breach
- Accessibility in servers, or "in the cloud", which really means in servers and back up servers, wherever those are located

While the Snowden revelations have driven recent concern about the mining of this kind of data for security and intelligence purposes, it must be said that the more mundane risks listed

[2] Report of the UN Special Rapporteur on Freedom of Expression David Kaye
A/HRC/29/32, Human Rights Council 29th session.
http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Pages/ListReports.aspx

above will always exist to some degree. We are becoming more aware of data breaches and the extent of insider abuse, as transparency becomes required. The extent to which personal data at rest and data in transit is available to law enforcement and government actors is not well understood, particularly in regimes where there are constitutional protections and data protection law. In other regimes where these protections do not exist, there is often an assumption that secrets should not go over the telecom network/Internet, because they will be accessed by unfriendly government actors.

Potential mitigations for these basic risks inherent in e-communications include the following:

- Full, broadly scoped security threat risk assessments (TRAs) for all aspects of the system, performed on a regular basis, with regular checks of the effectiveness of proposed risk mitigations
- Full, broadly scoped privacy impact assessments (PIAs) for all aspects of the system performed on a regular basis, with regular checks of the effectiveness of proposed risk mitigations
- Scanning of the systems for malware and other software threats
- Traffic analysis and other types of network scanning to determine unusual activity (i.e. intrusion detection systems or IDS)
- Accreditation of e-communications systems to ISO standards
- User training, to reduce exposure to malware, phishing attacks, etc.
- User training, to ensure all parties are aware that they have a role to play in the protection of personal information (through limiting their own risk, respecting the privacy of others, becoming aware of their own liability if they transmit personal information and breach the privacy of others)
- Mandatory breach reporting
- End to end encryption of messaging
- Audits of server farms, help desk functions, data backups, email system management practices, etc.
- Penalties for abuse, particularly for those who are staffing the system management but also including users of the system

There are clearly many cost implications for running a system securely, as described above. Some of these functions may well be better performed by large IT companies who are in the business of designing and operating large systems securely, who are aware of evolving threats, and who have large security teams dedicated to finding solutions to problems on an ongoing basis. However, outsourcing does introduce new risks, as described in the next two sections.

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

There are many risks inherent in outsourcing, which are well documented. The first and most obvious is the loss of control over the data. Even the best drafted and executed contract cannot provide adequate assurances that the contractor is acting in the best interests of the client, because their interests are inevitably somewhat in tension, a phenomenon which everyone who signs a contract realizes at some point. While it is no doubt true that in all organizations, service departments are tempted to put a happy face on their own performance, in outsourced situations the contractor is highly motivated to keep bad news away from the client, and keep the contract renewed. The liability and responsibilities of client and contractor are fundamentally different.

In matters of IT security and the protection of personal information, the reporting of compliance issues can become problematic. Where information is concerned, the actual quality of the management is not always apparent to either end user or client. Quality control with information processing is not as visible as (for instance) the processing and packaging of potato chips. Information can look exactly the same after it has been breached. Furthermore, some actors, notably law enforcement and national security authorities, have the ability to demand secrecy for many types of investigations. Under Canada's own Security of Information Act, which replaced the Official Secrets Act, telecommunications and IT staff might be cleared for life,[3] in order to perform technical functions for security and intelligence purposes. When this happens within an organization which is hosting its own data, there is arguably more likelihood that due process will be adhered to; when it is under contractor control, absent specific instruction, it may not be. Importantly, it is harder to find out if that happens.

Here are a few risks that arise when the management of eCommunications is outsourced:

[3] Security of Information Act, RSC 1985, c O-5, <http://canlii.ca/t/52cjw> retrieved on 2015-03-04, s. 10.

- Quality control for the management of information is outside the control of the organization
- The contract must set out all policies and legal requirements to which the contractor must adhere, in specific terms and language, which is a formidable task in a contract
- Incentives to report breaches, improve performance, and maintain continuous service improvement may be replaced by a focus on the bottom line, and profit taking. Those outsourcing to “free” services should be especially careful, and consider what incentives are there for the vendor to actually report breaches to the customer.
- When e-communications services are being offered at no charge, as a loss leader for other goals, the client has little to no leverage on the contractor. The question must be asked, what precisely is the value proposition for the contractor in these circumstances?
- Loyalty to end users using the systems becomes mediated by loyalty to contracting clients, and therefore service goals are somewhat different
- Changes in the management, staff and marketing goals of the contractor may influence service performance
- Training may be necessary for contractor staff because of unfamiliarity with the policy and legal environment of the organization (see for example in the case of universities), but contractor may be unwilling to keep this up as required.
- Focus on provision of security services, while necessary, may substitute for the broader goals of the organization. For example**, universities** need to have first class information systems that serve their interests in innovation and knowledge seeking, and that clearly protects academic freedom.
- Auditing is most likely to be outsourced as well, and loyalty to end users may again be attenuated.

Many of these risks are inherent to the outsourcing of the provision of goods and services generally, but some are uniquely exacerbated in the context of information services that involve personal information. Potential mitigations include the following:

- Contracts must to a maximum extent cover all policy and legal requirements that the organization would be addressing if it were managing the communications.
- Scrutiny (oversight) and audit must, in order to replace the due diligence that the organization would take if the service were kept in-house, be rigorous, preferably including some audit and verification performed by the organization itself, or independent auditors acting on behalf of the organization, not the contractor. Contracts or subcontracts for oversight and control should be closely supervised, to avoid potential conflicts of interest.
- Organizations need to be alert to the risks of 'V**endor lock-in' which are widespread in the IT industry**, in which a service provider "makes a customer dependent on the vendor for products and services, unable to use another vendor without substantial switching costs"[4]. Robust measures must be included in the contract to provide the organization an exit strategy in the event of changes in the management of the contractor, or in the event of sale or takeover of the division. How will the data come home in this case? Will all the data, including change logs, version history, and metadata be returned, or just the content? Will the data be in proprietary format or will it be in an open format? Will end users have access to their data and metadata when the outsourcing agreement ends?
- Ownership of the information, and rights of the end users (eg. access to their own personal information under data protection law of the jurisdiction of the organization, keeping in mind that this right must be accorded to the data subjects of personal information contained in the system, not just users or account holders) must be guaranteed in the contract.

[4] Vendor lock-in is a well known problem. The European Commission, as part of its Digital Agenda for Europe, published a guide for public authorities to avoid Vendor lock-in https://ec.europa.eu/digital-agenda/en/news/against-lock-building-open-ict-systems-making-better-use-standards-public. While more relevant to other IT systems, particularly those which do not rely on open standards, the same principles apply to the provision of email systems. See also Wikipedia at en.wikipedia.org/wiki/Vendor_lock-in

- Although certain functions can be assured in the contract, it is not a given that every legal right and redress mechanism will be available in a contracted situation, particularly if it is one dependent on local Courts.

3. Risks of Foreign Control of Outsourced Communications

What changes when personal and sensitive data is transferred offshore, to other countries? Despite the friendly language of "the cloud", the current paradigm of moving data to foreign jurisdictions, where it resides in servers and equipment just like it always has, introduces new risks that sound remarkably like the risks we discussed in transborder dataflow discussions back in the 1970s and 1980s, amplified by the new cyberthreats that have come with the Internet (as opposed to mainframe computers). The kinds of issues discussed in the previous section, notably the attenuation of the relationship with the contracting organization and its users, the lack of familiarity that the contractor's staff have with the legal and policy regime that is the environment which dictates the organization's goals, obligations, and liabilities, and the remoteness of the operations from an oversight perspective, are amplified as we move further from home. This becomes more problematic if there are multiple sites and backup storage facilities, and accountability becomes therefore more difficult to track.

Here are a few of the additional risks:

- Contractor staff, operating in different or multiple jurisdictions, will be less familiar with the legal and policy regime in which the organization operates.
- Increased distance from the organization and its personnel may decrease the sense of loyalty and fiduciary responsibility to the client.
- Government actors who are interested in the data for many reasons, not necessarily criminal law enforcement, have reduced responsibilities under their law to respect the rights of "aliens" or non-citizens. In some jurisdictions, all data and metadata is fair game. If you are outsourcing to a foreign jurisdiction, you must ask what privacy protection is provided in law (if any) to the data of foreign nationals.
- Data protection law and intellectual property law may not be enforceable in foreign courts, and the investigation of even major infringements is much more problematic in

foreign jurisdictions, involving MLATs (mutual legal assistance treaties) and the cooperation of the foreign state actors. Given the lack of criminal sanctions available in Canadian data protection law, it is most unlikely that foreign authorities would bother helping with an investigation. Many other kinds of breach and criminal behaviour may also fail to get the attention of foreign law enforcement officials who are likely the only ones able to investigate on their soil.

- Intelligence and some law enforcement authorities are not obliged to get a warrant to access personal information of non-citizens in some jurisdictions, notably the United States, and they are also not bound to the same transparency requirements as they would be for citizens. The organization is unlikely to be informed of routine access requests.
- All service providers have disincentives to insist on human interactions when serving information requests, they all prefer to have automated systems with trusted requestors, where the requestor is free to access the data themselves. In a routine situation where foreign data is being held for years, this kind of access could lead to wholesale abuse that could go unreported.
- One of the features of cloud computing is the ability to move data from server to server fluidly. Courts have recently taken the position that a company can bring the data home for the purposes of law enforcement access, since they have the ability to move it about at will. Although some companies are fighting these orders in Court, this could be a new risk[5].

Potential mitigations:

- Contractor staff training could be instituted, and maintained on a routine basis as staff come and go (a best practice also for domestic outsourcing)

[5] https://blogs.microsoft.com/eupolicy/2014/12/18/privacy-law-enforcement-matter-principle/
In this case, a US Court has demanded that Microsoft bring home data that is held in Dublin. Microsoft is fighting the case in a high profile manner, but other companies may not be doing so.

- The organization could insist contractually on keeping up to date lists of contractor staff who have access to the information, and regular webinars and meetings with these staff could help establish relationships with the client to improve loyalty and awareness of legal and policy issues (a best practice also for domestic outsourcing)
- Transparency reports on the rate of access to data, and notification of data subjects where relevant, should form part of the contractual requirements to the extent possible.
- Prior to issuing a contract, the organization should investigate whether there is a possibility of enforcing Intellectual Property (IP) and Data Protection (DP) rights in the foreign court. If not, end users should be made aware of this fact when they decide to use the system. Some kind of remedy to replace these rights should be specified in the contract.

This simple, three tiered approach to some of the risks inherent in the management of eCommunications systems shows how the risks compound when the information management is not just outsourced, but held outside the country for any period of time. The following questions will help administrators determine where on this continuum of risk their eCommunications project sits, with respect to each facet of the data and systems management.

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

This framework is applicable to Canadian provinces that permit or do not prohibit by statute the extra-national outsourcing of personal information.

Step 1: Consider the full of range of data and metadata generated by your organization that is to reside outside of Canada.

Data

Some examples of data communicated using a university eCommunications system:

- Instructional correspondence, including assignments, draft and completed work, questions, group discussions, marks, etc.
- Library research, including catalogue search terms, documents and books downloaded, page viewing order, time spent on each page, bookmarks, etc. (in short, the reading habits of users)
- Research work, including results of studies and trials, new breakthroughs, draft articles, trademark and patent applications, etc.
- Discussions of an inherently personal nature such as personal circumstances, health issues, stress and psychological matters which interfere with work, etc.
- Personal email between students/faculty and others, including those of a social or romantic nature, personal opinions of others, descriptions of social or political events, etc.
- Personal email associated with the individual's participation in activities entitled to protection under freedom of association, such as list sign-ups including those of a political or religious nature, notifications of blog postings, interests entitled to protection under the Charter such as sexual orientation, etc.
- Pictures, images, videos, scans of documents, documents downloaded for scholarly or other use, etc. Some pictures and videos could contain information that is personal, non-consensual, political, etc.
- Personal email used for routine life on the Internet, such as banking, credit card information, travel, purchase information, etc. Given the reality that commerce is pushing overwhelmingly to conduct business and billing electronically, this could include all kinds of transactions, from fuel orders to pension payments and telephone bills (including the numbers of everyone the individual called)

It is important to note that the information an end user is putting on the network via his/her own access to it is often considered to be his/her own, so we sometimes slide into talking about the privacy of the end user alone. This is often not the case, however, since the research notes could include other's data, pictures could be of others, the financial information may include

that of others, the marks and grades and feedback could be of others, etc. From the perspective of the university, its liability, and its fiduciary responsibilities, it is important to understand that the personal information at risk is not just that pertaining to the owner of the access or email. They can perhaps consent to putting their own data at risk, but they cannot do so for others.

Metadata

Metadata is structured data *about* the content or data. A few examples:

- Date and timestamps of content creation and modification which over time reveal work habits and daily rhythms
- To/from email addresses which reveal social networks
- IP addresses which can reveal user location
- System used to access the data
- Pages viewed when reading data
- Servers traversed during email delivery

It should be noted that IP addresses are considered to be personal information by most data protection authorities.[6]

Step 2: Assess whether any data or metadata categories identified in Step 1 meet the definition of personal information with respect to your provincial jurisdiction's privacy legislation.

[6] See the opinion of the Article 29 working party on geolocation data, for a detailed discussion of unique identifiers: 881/11/EN WP 185 *Opinion 13/2011 on Geolocation services on smart mobile devices* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf.

Does this range of data contain personal information? Here is the definition from Ontario’s Freedom of Information and Protection of Privacy Act: Use the applicable privacy legislation from your own jurisdiction:

“personal information” means 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”)

In the example above, a University’s eCommunications system contains a rich treasure trove of both data and metadata that falls under the definition of “personal information” given in FIPPA.

Note the issue here is not whether a user transmits emails internationally containing their personal information as there is no statutory prohibition on a person doing so with their own information. The test here relates to the overall archive of data and metadata for which the organization has responsibility, including the internal communication within the organization itself.

If there is no personal information in the proposed data/metadata to be outsourced then there are no privacy implications for extra-national outsourcing. There is no need to proceed further with this assessment.

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

For most organizations, end users in Canada will be Canadian citizens and permanent residents. Many Canadian universities will have a significant percentage of foreign nationals either on student visas or visiting/new faculty on work visas. Not only are the legal rights of these individuals often different with respect to their information, their risks may be much higher, particularly when the data is not under the direct control of the organization.

Note that automated collection and analysis tools mean that data needn’t be identified as interesting before it is harvested (as in a targeted effort). Data can be collected, undergo preliminary analysis, and retained for ongoing analysis as related data is harvested.

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

The list of potential data types described in Step 1 might be of interest to:

- Market competitors both of the mundane variety, looking for market information, or those representing more serious threats of economic espionage and copyright/patent violation, looking to access and steal IP
- Law enforcement authorities
- Tax authorities
- Casual friends/enemies of the individuals in question, or hackers in general looking for personal information of interest
- Criminal enterprises looking for data or metadata for any number of purposes.
- Security and intelligence authorities, particularly in the case of foreign students from certain countries, who are looking for environmental or social activists, political dissidents, etc.
- Businesses looking to mine personal information collections or metadata for profit

Step 5: Identify the ways in which your organization can protect the personal information of all of your end users (identified in Step 4) in the face of lawful requests or illegal access attempts by the above actors identified in Step 3.

1. Consider the extent of your organization’s ability to act in:

- Your own location (i.e. “in house”)
- Within your jurisdiction (outsourced in Canada) [but note that this does not necessarily imply protection as foreign-owned corporations may be compelled to hand data over to their home country.]
- Each foreign jurisdiction in which your outsourced data may be stored or deposited for the purposes of the convenience of cloud services (extra-national outsourcing and cloud services). Despite the haziness of the expression “cloud services,” when data is available in the cloud it means that is has been housed in a server in a jurisdiction, and is available to authorities in the event there is a request or warrant for it.

3. A Questionnaire for eCommunications Outsourcing by Universities and Other Public Institutions

Data Protection Law

1. Do you know which data protection law(s) apply to the e-communications systems and associated information?
2. Does the responsible data protection authority have existing guidance on how the law applies to e-communications systems and associated data?
3. Does the responsible data protection authority have existing guidance on outsourcing, particularly outsourcing outside Canada?
4. Have you sought legal advice from a privacy expert on these matters?

Existing Policies in Your Institution

1. Have you consulted your data protection officer about this project?
2. Have you examined existing policies and procedures to see if they cover the project?

Data Covered by the Project

1. Have you obtained or created a complete list of all systems affected by the proposed project?
2. Have you obtained or created a complete list of all types of data that could be accessed on each system, and possibly placed in storage?
3. Do you have a complete data map of all data and systems with their likely geographic locations (i.e. avoid using the cloud metaphor; jurisdiction matters so destinations matter!)

Risk Management

1. Is there a comprehensive, annual risk management plan for your institution?
2. Are personal data protection and security risks identified in the annual plan if it exists?
3. Are there existing privacy impact assessments for your eCommunications systems?
4. Are there existing threat risk assessments for your eCommunications systems?
5. Have you considered/discussed having a comprehensive risk assessment workshop to update any of the preceding items in the context of this project?
6. If the answer to 5 is yes, have you considered the following key elements in such a workshop:
    - Neutral facilitation with a trained risk manager
    - Identification of all potential stakeholders, including representatives of end users
    - Cost benefit analysis for all aspects of the system
    - Metrics for existing risk mitigations (i.e. Are they working? When did you last measure them?)
    - Scope of the risk management framework
    - Management buy-in for real risk mitigations
    - Likely ownership of risks and their mitigations
    - Ongoing risk assessment requirements
    - Whether or not potential contractors should be involved in the exercise

7. If you have a robust risk management system in place, how are you rating your privacy risks? Some risks are too irremediable to effectively rate….once some types of personal information has been stolen, you cannot get the data back and fix it. It is worthwhile recalling, when evaluating risk scores dealing with personal information, that we are not dealing with money, we are dealing with data which cannot be unknown, and cannot be replaced. If your Social Insurance Number is being used by somebody else, Service Canada will help you to get a new one, but they will never take the old one out of the system, it is lost and gone but in all likelihood, alive with your name on it. While Identity theft is one example of catastrophic loss, there are many others, such as deeply personal health information (abortion, STDs, mental breakdown) which can have life altering effect when released. We advise against trying to rate these risks, they are high impact even if low likelihood. Another outlier to consider in the catastrophic loss category is celebrity data…hospitals have a constant problem stopping staff from inspecting celebrity health data, and there is a market for the data. The same applies to celebrity students (eg. children of rock stars or politicians).

Consultations

1. Once you have a project plan and risk management plan, are you going to do a request for proposals? If so, what do you need to put in it?
2. Have you consulted your legal team concerning contractual requirements? Have you ensured that anything mandatory is in the RFP?
3. Have you consulted with your financial and legal teams to estimate the cost to mitigate your financial risks with respect to data protection and security?
4. Have you consulted your security team to ensure that they have a comprehensive security plan in place and are adequately resourced to deliver it? Do they have a partner role in this project, and if not, why not?
5. Have you consulted end users to seek their views and identify any concerns?
6. Have you consulted management to brief them on risks and responsibilities?
7. Have you identified any outside partners who could be implicated in your project, and if so how do you plan to consult them?
8. Is it advisable to consult your data protection authority, and if so do you have a plan for that?
9. Have you consulted your communications branch to discuss the project with them? If so, do you have a communications plan ready? Did you invite them to the risk assessment workshop?
10. Have you consulted with your research ethics branch experts to determine whether additional steps need to be taken to protect research subjects?

Audit and Controls

1. Audits of a number of functions will be part of your security and risk mitigations plan. Who is going to do them? Is that audit function fully independent?
2. Do you control the contract for audit if it is outsourced, or does the contractor?
3. Do you have the ability to audit any remote sites specified in the contract?
4. What systems controls reporting will you receive?

5. Who is responsible for ensuring that any anomalies are corrected? Is there a reporting mechanism for those remedies?
6. Do you have the authority to audit privacy compliance (in addition to security)?
7. Does your data protection authority have the authority to audit, and if so, what resources will be accessible in his/her jurisdiction?
8. Have you developed a set of metrics to measure the success of failure of this project, and if so, who is responsible for measurement?
9. Is the measurement or evaluation sufficiently independent? Do you have a program evaluation branch that can independently assess the project when it is complete?

Access to Information and Other End User Rights

1. Have you allowed for the full suite of privacy rights of end users and other data subjects, and not just security and mitigations to the risk of data breach? This could include:
   - The right to access personal information, have it corrected, or removed
   - The right to damages in the event of a breach, and the right to speedy notification of that breach
   - The right to know who has accessed the information
   - The right to complain to the data protection authority, and or the Courts

2. Have you discussed the risk of civil litigation and tort law with your legal counsel? What is the risk?
3. Have you discussed the risk of certain types of information being found on the system that could give rise to criminal investigations, in the context of the changes expected through this project? This includes child pornography, drug trafficking, terrorism, cyberbullying, trademark and copyright infringement, etc.
4. Have you ensured that the information affected by the project will not be available for data mining for any purpose, not just for marketing?

Surveillance and Law Enforcement Issues

In the wake of the Snowden revelations of widespread capture of Internet traffic for intelligence purposes, many Canadians are concerned about who is reading their e-communications. In the post-secondary sector, institutions must be mindful that many foreign students, faculty and partners do not enjoy the same Charter protected freedoms as Canadians, so the issue of widespread capture is of particular concern. Given that for communications outside the university, any number of individuals anywhere around the globe could be swept up in surveillance of the institution's systems, you will be unable to predict risk for those individuals. What precautions have you taken to protect against the following risks:

1. Examination of eCommunications by unfriendly government actors looking for religious, political, sexual, or social behaviour that they consider unacceptable or that is illegal in that jurisdiction?
2. Insider or other abuse (e.g. corrupt government officials) looking for research or business information, trade secrets, or material to blackmail individuals
3. Parents, relatives or other individuals demanding access to information that would be protected by privacy legislation in this country but may not be elsewhere
4. What steps have you taken to ensure that you will be able to detect this kind of abuse?
5. Have you discussed with legal counsel, your data protection officer, and/ or your data protection commissioner, the recourse and notification rights that the institution and its end users will have with respect to surveillance activity, whether legitimate or not?

Training and Communications

1. Have you developed a training plan for staff, including (where applicable) contractor staff, to familiarize them with security and privacy rights and risks?
2. Have you costed your plans and ensured that even with change over time, they will be implemented on a regular basis?
3. Have you developed a communications strategy and package of materials to brief users of the e-communications system on your policies and procedures, their rights or lack thereof, expected behaviours, including their own management of the personal information of others, etc.?

4. Have you developed complaints mechanisms and opt-out arrangements?
5. Do you have a crisis communications plan, or the ability to respond quickly if required, should you experience a catastrophic loss or breach of sensitive data? Have you briefed your senior management about this kind of risk?

- end framework.