UNIVERSITY OF TORONTO

Interim Privacy Impact Assessment

Student E-Communications Outsourcing Project

Matthew Wilks, David Auclair — Information Security, I+TS

Howard Jones, Rafael Eskenazi — FIPP Office

Creation Date:	Version	1.0	April 16, 2010
Last Updated:	Version	1.02	April 19, 2010
	Version	1.03	June 11, 2010
	Version	1.1	June 21, 2010
	Version	1.11	June 22, 2010
	Version	1.12	June 23, 2010
	Version	1.13	July 7, 2010
	Version	2.0	Sept 22, 2010

Table of Contents

Executive Summary

A privacy impact assessment (PIA) is a process for determining and addressing privacy risk during the development and implementation of projects that involve or affect personal information. The PIA is an analysis of how project data flows align with legal, policy, practice and stakeholder privacy expectations. The PIA is a tool for executives to understand and address privacy risk in the project. This PIA is a living document that will continue to develop as the project develops. Future versions will align with milestones as the project develops.

As a result of a consultation on student e-communication, the CIO of the University has recommended "that at this point the University actively and aggressively pursue the single course of determining the best features and costs possible in an outsourced solution for student email." The two external service providers being considered are U.S. based: Google Inc. and Microsoft. The products under consideration are Google's *Apps for Education* and Microsoft's *Live@EDU*.

Both organizations attempt to relieve concerns surrounding what is perhaps the most talked about aspect of outsourcing email to an external provider: foreign legislation such as the Patriot Act in the United States. While the probability of such a request for information remains low, the risk to privacy it imposes – especially since Google or Microsoft might be forbidden from informing the user of such a request – is significant, with no possible mitigation.

While both organizations exhibit a high degree of attention to the privacy of their users, one possible area of concern lies in Google's statement that if they propose to use personal information "for any other purpose other than those described in this Privacy Policy", an effective opt-out would be provided[1]. It should be pursued whether the University could contractually bind Google to take an "opt-in" approach with the University's users. Both the respondents indicated that aggregate, non-personally identifying, statistical information would be collected and shared with third parties about the users of their services.

Once the service provider has been selected, the next step for the PIA is to perform a transactional level information flow analysis. Additional input from the service providers will be required in order to accomplish this. However, there is a high probability that the detailed interactions between the service providers systems will never be revealed to us.

[1] It should be noted that this "opt-out" only applies to Google's use of personal information. If Google wishes to share personal information with a third party, they state that they would require opt-in consent from the user.

Introduction

A privacy impact assessment (PIA) is a process for determining and addressing privacy risk during the development and implementation of projects that involve or affect personal information. A PIA typically contains a description of the project, a detailed transaction-level examination of data flows, and an assessment of how those data flows align with legal, policy, practice and stakeholder expectations. This analysis, together with possible mitigation strategies for identified privacy concerns, provides a tool for executives to understand and address privacy risk in the project. This PIA is a living document that will continue to develop as the project develops. Future versions will align with milestones as the project develops. The level of granularity will increase as we learn more about the detailed personal information transaction flows and will align with necessary decisions and risks associated with each milestone.

The University is committed to the requirements of the *Freedom of Information and Protection of Privacy Act* (FIPPA). In addition, since the third party contractor considered in this PIA is a private sector entity, adherence to *The Personal Information Protection and Electronic Documents Act* (PIPEDA) is necessary. Protection of privacy is not only a legal requirement but an integral element of projects involving personal information. Privacy protection is a necessary, responsible institutional practice in response to increasing threats to personal privacy.

Project Description

As a result of a consultation on student e-communication, the CIO of the University has recommended "that at this point the University actively and aggressively pursue the single course of determining the best features and costs possible in an outsourced solution for student email." The two external service providers being considered are U.S. based: Google Inc. and Microsoft. The products under consideration are Google's *Apps for Education* and Microsoft's *Live@EDU*.

Both of these companies offer a suite of tools that represent a "significant improvement to our status quo as well as support for some of the calendaring, document management and other communications integration aspirations discussed during the consultation." Since email has become an expected service at any institution, our email services are no longer a factor that differentiates the University. Students of universities that have switched to hosted email services have been happy with the additional storage capacity and features, while at the same time universities that have switched have been happy with the significant cost savings.

Special consideration must be given to the fact that in this case both of the external service providers are U.S. based corporations. The Ontario government publication, "*Guidelines for the Protection of Information when Contracting for Services*" attributes a very high risk to storage of sensitive information outside Canada, and a fundamental question of this assessment is how the University can meet privacy obligations and guarantee information security, privacy and control through contractual agreements. Equally central (if not more important) is the question of the reliability and trustworthiness of the external provider's reputation in the industry as well as the robustness and security of its hardware and software infrastructure. Care must be taken to ensure that the privacy of information is not an afterthought, but rather that privacy has been of central concern – with specific reference to the legislation governing the University – to the external provider at every stage of the development of its services and infrastructure.

In summary, the focus of this assessment will be to highlight risks to privacy in order to:

- Ensure that information that has been collected by the University is protected against unauthorized collection, use and disclosure in its exposure to an external service provider;
- Ensure that all information created or maintained through this project remains under the custody and control of the University; and
- Ensure that the external provider meets the requirements of the acts mentioned in the introduction to this document (FIPPA, PIPEDA), where / if applicable.

Bodies Involved

At this stage, the following bodies (corporate entities) are involved in this project:

- University of Toronto
  - Information + Technology Services
  - Freedom of Information and Protection of Privacy office
- Google Inc. or Microsoft, depending on the procurement process
  - Any and all sub-contractors to Google or Microsoft involved in the provision of the contracted services and who may have direct or incidental access to the personal information or records deemed to be under the control of the University

As this project develops, more entities may be added to this list.

Stakeholder Expectations

A committee was formed to solicit input from students about e-communications[2]. The committee met in person four times between November 2009 and January 2010. In addition to this there was an anonymous web form available on the I+TS website along with full information about the consultation. Many mediums were used to direct interested parties to the form including RSS feeds, Facebook, notices distributed by Student Life staff and email sent to the students at UTM.

Security and privacy were the most commonly raised concerns about outsourcing email to an external provider. Students who participated in the consultation expect and trust the University to appropriately protect their information. They did express concern about the misuse of information (e.g. data mining) and the communications channel (e.g. advertising) by an external provider. Concerns about the USA Patriot Act were also voiced. It was agreed that institutional negotiations with external providers would clarify and likely enhance security of data over that provided by the personal arrangements being made by individuals with these same providers.

[2] http://www.its.utoronto.ca/tri-campus_it/its_info/ITS_Comm_and_Consult/studentecomm.htm

Privacy by Design

Dr. Ann Cavoukian has developed a set of best principles surrounding the development of services that respect privacy called *Privacy By Design*[3]. We include these principles here as a reference point for discussions with vendors:

1. **Proactive** not Reactive; **Preventative** not Remedial

   The *Privacy by Design* (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events *before* they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to *prevent* them from occurring. In short, *Privacy by Design* comes before-the-fact, not after.

2. Privacy as the **Default**

   Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy – it is built into the system, by *default*.

3. Privacy **Embedded** into Design

   Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

4. **Full** Functionality – Positive-Sum, not Zero-Sum

   Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. *Privacy by Design* avoids the pretence of false dichotomies, such as privacy *vs*. security, demonstrating that it *is* possible to have both.

5. End-to-End Lifecycle Protection

   Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved, from start to finish. This ensures that at the end of the process, all data are securely destroyed, in a timely fashion. Thus, *Privacy by Design* ensures cradle to grave, lifecycle management of information, end-to-end.

[3] http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

6. Visibility and Transparency

   Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

7. Respect for User Privacy

   Above all, *Privacy by Design* requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

Recommendation

Based on our analysis, we recommend that future discussions with possible student e-communications service providers take into account the following considerations:

Google

We should inquire if the University could contractually bind Google to take an "opt-in" approach for changes in the way they use our users' information, rather than "opt-out".

Microsoft

We should pursue talks with Microsoft under an additional NDA in order to supplement their RFA response with additional details.

It is necessary that notice be given to the end users of whichever system is chosen stating at least the following:

- User-supplied information will be stored on servers outside of the University's network, and may be subject to the US Patriot Act.
- That some products offered through the external provider (for example, Google Gadgets) may be offered with their own privacy policies. It would be up to the user to read those policies to make sure that they agree to the terms.
- And any additional terms as determined by the FIPP office, or I+TS.

The contract that is entered into by the University should address at least the following points:

- The external provider does not own the user data stored in its systems.
- The external provider cannot conduct data-mining on the user data.
- The external provider will not release any personal information to third parties unless required by law and where possible notify the University of any requests/demands for personal information.
- The external provider must support transport encryption for all communications between their data centres and users of their service.
- The external provider must perform audits regularly to ensure that they meet industry standard information security requirements.
- The external provider must notify us in advance of any changes to their privacy policy.
- The external provider should have an audited hardware disposal process.