UNIVERSITY OF TORONTO

Privacy Impact Assessment

Student E-Communications Outsourcing Project

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	December 2, 2010
	Version 2.1	December 8, 2010
	Version 2.2	January 3, 2011
	Version 2.3	January 10, 2011
	Version 2.4	March 22, 2011
	Version 3.0	March 25, 2011
	Version 3.1	May 30, 2011

Table of Contents

Executive Summary

A privacy impact assessment (PIA) is a process for assessing, documenting and addressing privacy risk in the development, implementation and operation of projects which affect personal information. A PIA analyzes data activities and handling of personal information to verify project alignment with privacy standards, legal requirements, including the *Freedom of Information and Protection of Privacy Act* (FIPPA), University policy, practice, and stakeholder privacy expectations. A PIA is an evolving document that elucidates privacy risks as a project progresses helping decision makers understand and address them at the right time.

As a result of consultation on student e-communication, the CIO of the University of Toronto (the University) recommended that "the University actively and aggressively pursue the single course of determining the best features and costs possible in an outsourced solution for student email." After assessing two service providers; Google and Microsoft, a decision was made to pursue negotiations with Microsoft respecting its Live@edu product.

Student participation will be voluntary with the choice to not use Live@edu. Live@edu will provide useful new functionality for students, including larger e-mail inbox quotas, calendaring and several other services not previously available as part of student e-communication at the University. Significant cost savings are projected as the service is free of charge to the University. Live@edu is expected to improve reliability, freeing valuable support staff time for projects better aligned with the core mandate of the University.

Microsoft demonstrated a strong commitment to Privacy and security to the University, in its online materials, and in the design of its services. Microsoft has, and will annually continue to provide the University with the results of its SAS70 Type II external audit. This PIA finds that Microsoft's physical and logical controls and staff training for data center employees evidence an approach to privacy consistent with University standards in the context of student e-communications.

Some minor risks will be introduced by outsourcing student e-communications to Microsoft's cloud-based Live@edu, including:

- The use of a proxy authentication gateway for certain methods of accessing e-mail.
- Inadvertent or malicious disclosure of personal information by (a) Microsoft employee(s).
- Exploitation of shared cloud computing infrastructure by other customers to compromise U of T information or accounts.

Another risk of cloud computing results from data being stored, transported or used in other jurisdictions, rendering University information potentially subject to foreign legislation (such as the USA PATRIOT Act). While foreign governments may be unlikely to request information from Microsoft about a U of T user, such requests and disclosures can occur without notice or recourse. It may not be possible to fully mitigate this privacy risk. Canadian authorities are also legally empowered to access personal information in certain circumstances. Lawful Canadian access is permitted under FIPPA, but access pursuant to foreign legislation generally is not.

Microsoft implemented several features to effectively mitigate privacy risk such as transport layer encryption (protecting data flows between the user and Microsoft) and strictly audited security and privacy controls. In addition to Microsoft privacy measures, the University worked to build reasonable privacy protections into its contract with Microsoft.

In deciding whether to proceed or not, University decision makers must decide to accept or reject the residual privacy risks. (See Summary of Residual Risks Chart at page 55)

Work Units

Relevant University and Microsoft units collaborate on the Privacy Impact Assessment.

The following is a listing of major partners and their role in this PIA.

- University of Toronto
  - Information + Technology Services

Bob Cook	Information + Technology Services, CIO
Martin Loeffler	Information Security, Director, Security Lead
David Auclair	Information Security, PIA Author
Matt Wilks	Information Security, PIA Author
Paul Ruppert	Integrated Client Services, Director
Marden Paul	Planning, Governance and Assessment, Director
Vicki Vokas	Web Services Project Office, Manager
Alex Nishri	Integrated Client Services, Manager -- Email and UTOR Services
Derek Yuen	Integrated Client Services, Project Manager
Peter Ip	Integrated Client Services, Chief Integration Engineer
Paul Fardy	Integrated Client Services, Authentication Specialist
Michael Simms	Integrated Client Services, Network Services Specialist
George Katterloher	Integrated Client Services, Network Services Specialist
Hong Zhu	Integrated Client Services
Stanley Alleyne	Integrated Client Services
Richard Sanford	Integrated Client Services
Chad Holden	Integrated Client Services, Web Architect
Mike Clark	Integrated Client Services, User Experience Designer
Crisan Diaconu,	EASI, Technical Writer
Peter Eden,	Supervisor, Network Administration, Security review
Kevin Howie,	Assistant Dean, Operations, Security review
Wes Robertson,	Director, Information Technology, Security review

  - University of Toronto Lawyers and outside legal counsel
  - Freedom of Information and Protection of Privacy office

Howard Jones	Privacy Lead, FIPP Office
Rafael Eskenazi	Privacy Lead, FIPP Office

- Microsoft

David Fisher	Senior Product Manager, Live@edu Research and Development
Brad Tipp	Education Solution Specialist, Live@edu
Richard Wakeman	Solution Architect, Microsoft Consulting Services
Raj Mukherjee	Senior Product Manager, Online Services
Gabe Long	Release Manager, Live@edu Support
John Weigelt	National Technology Officer, Microsoft Canada
Chris Tardif	Principal Consultant, Microsoft Consulting Services
Karen McGregor	Education Solution Specialist, Microsoft Canada
Shann McGrail	Education Director, Microsoft Canada
Mike Tremblay	Director, Public Sector
Glen Donegan	Account Manager for U of T

Introduction

A privacy impact assessment (PIA) is a process for determining and addressing privacy risk during the development, implementation and operation of projects that involve or affect personal information. A PIA is a living document that develops with the project, aligning with project milestones and decision points. 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 mitigation strategies for identified privacy concerns, provides a tool for decision makers to understand the privacy risk present in the project. The purpose of this document is to delineate the risks along with possible mitigations for each. The remaining residual risks to privacy after possible mitigations have been applied is also set out for decision makers to decide whether residual risks are acceptable to the University or may require further mitigation.

Many methodologies exist for conducting PIAs. The University structured its PIA on the Privacy by Design (PbD) principles developed by the Information and Privacy Commissioner / Ontario (IPC). The assessment is structured around one overarching question about compliance with each of the seven PbD principles and a set of more detailed questions to more closely examine how the principle has been implemented. It is the University's experience that this approach yields a more detailed and complete understanding of privacy implications than older, more traditional PIA approaches, particularly given the inability to obtain detailed, transaction-level data flows from the proposed cloud service provider.

The University is committed to the requirements of FIPPA. Consideration was given to PIPEDA (The Personal Information Protection and Electronic Documents Act) since the University is contracting with a private sector service provider. The website of the Federal Privacy Commissioner states; "...our Office is of the view that, as a general rule, PIPEDA does not apply to the core activities of municipalities, universities, schools, and hospitals."[1] Although Microsoft's commercial activities would normally be covered by PIPEDA, in this instance it is acting as an agent of the University and so relevant privacy requirements are those set out in FIPPA, which applies to the University. PIPEDA legislation is therefore not specifically addressed in this PIA, although Microsoft will comply with legal requirements applicable to it. Protection of privacy is not only a legal requirement, but a reasonable expectation for activities involving personal information. Careful protection of personal information is a necessary, responsible institutional practice, particularly in response to increasing threats to personal privacy. The focus of this assessment is to highlight risks to privacy in order to ensure that:

- personal information is protected against unauthorized collection, use and disclosure in the context of student e-communications;
- all information created or maintained through this project remains accessible to the University for proper institutional purposes;
- the contract signed with the external provider meets or exceeds the requirements of applicable legislation (FIPPA).

This PIA comprises a description of the student e-communications project; stakeholder expectations; similar experiences of other universities and; a list of resources consulted. Particular attention has been given to the SAS70 Type II audit provided by Microsoft.

[1] Municipalities, Universities, Schools, and Hospitals, 2006 http://www.priv.gc.ca/fs-fi/02_05_d_25_e.cfm (December 2010)

The PIA considers the use of a cloud platform for University e-communications. A critical focus of the PIA is the IPC's foundational privacy principle that the privacy of the University's students not be an afterthought to the external service provider, but rather has been built into the project from the beginning. The PIA delineates flows of personal information, examines privacy risks at identified critical points and transactions, including analysis of FIPPA-specific risk. These analyses are compiled into a summary of residual risk remaining after possible mitigations are applied, to be accepted or rejected by University decision makers. The PIA considers, and must be read in conjunction with, the Live@edu contract with Microsoft.

Project Description

Reports from I+TS staff demonstrate that UTORmail (the University's legacy institutional email service) is near end-of-life and requires significant investment to bring up to current industry standards. Ubiquitous use of and dependence on email in daily life is a necessary feature and expectation of the student experience. I+TS (Information + Technology Services) conducted a consultation on student e-communications with a representative sample of students and pertinent staff around the University. From this consultation came a recommendation by the University's Chief Information Officer (CIO) "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." Two external service providers were considered: Google Inc. and Microsoft. A Request for Assistance (RFA) was issued to the two companies and after careful assessment of responses, a decision was made to pursue a contract with Microsoft using its Live@edu service.

The suite of tools offered through Live@edu represents a "significant improvement to the University's status quo as well as support for some of the calendaring, document management and other communications integration aspirations discussed during the consultation." In addition to providing an email service with a significantly larger storage potential, the users of Live@edu are given access to calendaring and online file storage features previously not offered to students. Students of universities that switched to hosted email services have been satisfied with the additional storage capacity and features, which are available at significant cost savings over services offered "in house".

This project represents a major shift in the way that the University provides its email service to students. Student email will be stored off-campus in data centers that are not located in Canada, raising the issue of applicability of foreign legislation to this data and loss of local control. With this shift away from internally managed email comes the need to establish a level of trust with Microsoft appropriate to the sensitivity of the personal information that will be stored in email and the other tools offered. Although Microsoft ensures the security and privacy of student personal information on its systems, the University will oversee the continuing privacy protection of students in this process.

Other Jurisdictions

In addition to key stakeholder input, experiences of universities that outsourced email services was examined. Thousands of universities worldwide have outsourced email services, including several in Canada, such as University of Alberta (U of A), which outsourced student, staff and faculty email to Google Inc. At this early stage in adoption of cloud e-communications, other universities' experiences provided useful context for the University of Toronto exercise.

a. **University of Alberta**

U of A recently announced its contract with Google to outsource student, faculty and staff email to Google's *Apps for Education* platform. Vice Provost Jonathan Schaeffer stated; "moving to Google will ultimately have a positive and transformative effect on teaching and learning on campus." The University of Alberta conducted a detailed Privacy Impact Assessment which was reviewed by the Alberta Privacy Commissioner. Other Canadian Universities followed U of A's Google negotiations with great interest and provided support. "More than 20 Canadian universities and the Canadian University Council of Chief Information Officers sent Google letters of support during a low point in negotiations last July, indicating interest in accepting Gmail if a legal framework like the one the U of A wanted was in place."[2] U of A's success in negotiating a contract that prohibits Google from mining user data or sharing personal information with third parties is expected to support the inclusion of similar terms in similar contracts at other universities, including the U of T contract with its service provider.

b. **Lakehead University**
Lakehead University (Lakehead) has used Google for faculty, staff and student email since 2007. A grievance was filed by the Lakehead University Faculty Association, stating that Lakehead was violating privacy and academic freedom by outsourcing faculty email to a US company (subject to the USA PATRIOT act). The arbitrator found for Lakehead and dismissed the Faculty Association's grievance[3].

c. **US peers (Washington, Arizona State, USC)**
USC, ASU and U Washington shared many details of their Google experience:

- Few uptime issues; if there is downtime, people seem to understand and accept more readily than when local systems go down.
- Students self-migrate and adopt services readily
- "Students thrilled!" – Kari Barlow, AVP University Technology Office, ASU
- "Our experience has been positive. Each of the moves [they have other outsourcing arrangements as well] has decreased our costs, improved our reliability, and made our services more predictable. This is a core element of our information technology strategy, and it has accelerated our advancement." Dr. Adrian Sannier, VP and University Technology Office, ASU
- USC annual IT survey for students has had Google Apps as the favourite service since it was introduced.

d. **alumni.utoronto.ca**
The Division of University Advancement has offered alumni accounts in partnership with Google for some years. They report:

- Alumni experience has been good. Alumni respond well to the offer.
- Close to 15,000 active accounts although more are on the system.
- Of affinity services, Google Mail is most popular, helping drive alumni to other offerings and communities.
- Graduating students are eager to take advantage of service. They appreciate the storage and the service levels. They have not experienced problems with email forwarding as with other services.

e. Nipissing University (Google)
f. Concordia University (Microsoft)
g. University of Lethbridge (Google)

[2] http://www.edmontonjournal.com/technology/inks+Gmail+deal+with+Google/3949065/story.html
[3] http://www.canlii.org/en/on/onla/doc/2009/2009canlii24632/2009canlii24632.pdf

While most of these examples are from universities who chose to use Google's email services, the fundamental questions of privacy and cross-border relations remain the same with Microsoft's *Live@edu*.

Resources Consulted

Some of the key resources consulted in the creation of this PIA are:

- *Privacy by Design: The 7 Foundational Principles*[4] (Ann Cavoukian, Ph.D.)
- *Modelling Cloud Computing Architecture Without Compromising Privacy*[5] (NEC Company and Information Privacy Commissioner Ontario, Canada)
- *Operationalizing Privacy By Design: The Ontario Smart Grid Case Study*[6]
- *Privacy in the Clouds*[7] (Ann Cavoukian, Ph.D.)
- *7 Laws of Identity: The Case for Privacy-Embedded Laws of Identity in the Digital Age*[8] (Ann Cavoukian, Ph.D)
- Microsoft's RFA response (provided by Microsoft under NDA)
- SAS70 Type II Attestation (provided by Microsoft under NDA)
- Online Services Information Security Policy (provided by Microsoft under NDA)
- *Microsoft and Data Privacy – Helping to Protect Personal Information in the Digital Age*[9] (Microsoft)
- *Microsoft and Data Retention*[10] (Microsoft)
- *Privacy Guidelines for Developing Software Products and Services*[11] (Microsoft)
- *Privacy in the Cloud Computing Era – A Microsoft Perspective*[12] (Microsoft)
- *Securing Microsoft's Cloud Infrastructure*[13] (Microsoft)
- *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1*[14] (Cloud Security Alliance)
- *University of Alberta PIA For Outsourcing Email* (provided by UofA under NDA)

[4] http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf
[5] http://www.ipc.on.ca/images/Resources/pbd-NEC-cloud.pdf
[6] http://www.privacybydesign.ca/content/uploads/2011/02/pbd-ont-smartgrid-casestudy.pdf
[7] http://www.privacybydesign.ca/content/uploads/2008/05/privacyintheclouds.pdf
[8] http://www.privacybydesign.ca/content/uploads/2006/10/7laws_whitepaper.pdf
[9] http://download.microsoft.com/download/B/C/A/BCAD4354-99E8-4A80-BCE3-210A74ECFA6C/Microsoft_and_Data_Privacy_final.pdf
[10] http://download.microsoft.com/download/7/9/8/7988DF4C-142E-4A29-96BE-2384C524AB68/TwC-Enterprise-CTZ3-Data Governance-Data Retention-BackgrounderFS.docx
[11] http://download.microsoft.com/download/3/8/5/385BEAE9-72E9-4F7F-A798-9D54F896351A/privacy_guidelines_for_developers.pdf
[12] http://download.microsoft.com/download/3/9/1/3912E37E-5D7A-4775-B677-B7C2BAF10807/cloud_privacy_wp_102809.pdf
[13] http://www.globalfoundationservices.com/security/documents/SecuringtheMSCloudMay09.pdf
[14] http://www.cloudsecurityalliance.org/csaguide.pdf

Privacy by Design Analysis

Given the nature of cloud computing, the University must ascertain that Microsoft facilities, datacenters and technology resources around the world provide a secure, privacy-protective environment. As a reasonable baseline, this environment should be at least as sound as the U of T resources that it will replace.

Ontario Information and Privacy Commissioner Dr. Ann Cavoukian developed a set of design principles for privacy protective service and systems development, called *Privacy By Design (PbD)*[15], which can be used to address the systemic effects of information technologies and large-scale networked data systems by assessing compliance with seven overarching privacy principles.

One key principle is "Privacy by default" -- privacy assurance and verification, with full commitment from leadership - must be an organization's default mode of operation.

A positive sum approach must also be taken (security, functionality and privacy optimally implemented to support system goals and each other) for IT systems, business practices and physical design and networked infrastructure.

The broadest objectives of *PbD* -- ensuring optimal privacy with effective individual control over personal information can be accomplished by following the seven foundational principles. The principles, set out in Appendix E, are used in this PIA to analyze, establish and demonstrate whether this project meets or exceeds IPC, legal, and community privacy expectations.

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

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.[4]

Does the Project take proactive and preventive measures?

Is there clear commitment at the highest levels to set and enforce high privacy standards?

Yes. *How?*

Microsoft

In a recent speech at the University of Washington, Microsoft CEO Steve Ballmer observed that Microsoft and other online service providers have a responsibility to lead in privacy protection:

> "As a big company, we've got to lead on privacy.... We have a responsibility, all of us, not just to socially respect the user, but to build the technology that will protect the anonymity, the privacy, the security of what I say, who I say it to, where I go, what's important to me."[16]

Microsoft has a comprehensive suite of forward-looking privacy actions and commitments, intended to proactively secure their infrastructure and client data[17]. Microsoft's approach starts with people; more than 40 Microsoft employees focus full time on privacy. Microsoft appointed a Chief Privacy Officer very early. Microsoft's central privacy team develops and implements programs for every aspect of the Microsoft ecosystem, from products, services and processes through physical systems and infrastructure. All new Microsoft employees receive privacy training, and to date more than 52,000 people have taken "Privacy 101", an interactive course that provides guidance on how to handle basic privacy scenarios.

Microsoft has thorough privacy reviews to help ensure that privacy is systematically incorporated into the development of products and services. The "Microsoft Privacy Standard for Development" is incorporated into baseline development guidelines (the Security Development Lifecycle or SDL). This approach helps ensure that privacy is incorporated into development from project genesis. After development, products and services undergo privacy review designed to ensure ongoing compliance with privacy policies and standards.

In addition to these fundamental privacy commitments, Microsoft also engages in cutting edge digital privacy tech research. Current projects include a Cryptographic Cloud Structure. The Microsoft privacy website details the importance of projects like this (emphasis added):

> "Researchers are working on cryptographic tools that will enable an individual or organization to help secure data stored in the cloud, *even if the data resides on a computer infrastructure that is not controlled or trusted by the user*. Potential outcomes of this project include tools that enable patients to generate and store keys to encrypt their information and give them full control over which organizations can access which portions of their health information."[18]

[16] http://www.microsoft.com/presspass/exec/steve/2010/03-04Cloud.mspx
[17] http://www.microsoft.com/privacy/bydesign.aspx
[18] http://www.microsoft.com/privacy/research.aspx

University of Toronto

University of Toronto leadership values privacy and endorses the seven Foundational Privacy by Design Principles. The University supports a culture of privacy and recognizes the work of Ontario's Information and Privacy Commissioner, in developing the PbD principles.

The University is officially committed to the principles of FIPPA, conducts faculty and staff privacy training, and operates under privacy guidelines, policies and comprehensive data protection guidelines, including a security baseline, designed to support a security culture where systems and procedures are crafted to prevent and address emerging security challenges[19]. These resources incorporate and detail core privacy principles including data minimization, need-to-know, record schedules and secure destruction. The University recognizes and follows Privacy by Design principles, the highest security standards, and conducts TRAs and PIAs for projects involving personal and confidential information.

One way that the University demonstrates its strong commitment to privacy and security is by maintaining full time director level positions and active programs to oversee protection of privacy and of information security.

Does the project anticipate and prevent privacy invasive incidents before they happen?

Yes. *How?*

Microsoft

Microsoft uses risk management processes[20] such as asset management, physical and logical access controls, change management and security surveillance to identify and mitigate risks before they become problems. In addition to proactive and preventive privacy measures, Microsoft monitors its infrastructure closely to ensure its security and privacy controls are effective. While Microsoft security controls and management processes are designed to reduce the risk of security incidents, it would be naïve to expect problems and attacks to not happen. Microsoft employs a Security Incident Management (SIM) team to respond to attacks, 24 hours a day, 7 days a week. The SIM has a comprehensive 6 phase incident response process including training, identification, containment, mitigation, recovery and analysis of lessons learned.

University of Toronto

The University undertook this PIA to anticipate and prevent privacy issues before they happen. This PIA developed over more than one year. Prior to the expected implementation date a working group was established specifically to anticipate potential incidents. Key stakeholder feedback was solicited in various ways, including a special committee, formed to address student expectations; an anonymous web form advertised through RSS Feeds, Facebook, notices distributed through Student Life and emails sent to students. More than 20 staff across 7 departments participated in the project. The University benchmarked other jurisdictions' and institutions' projects and experiences.

Privacy and security staff attended a symposium at Ryerson University on the future of e-mail, privacy and cloud computing and a comprehensive PIA workshop at Brock University.

Is there a methodology to recognize and correct poor privacy design, practices and outcomes well before they occur? *Yes.* *How?*

[19] http://www.its.utoronto.ca/rules-and-regulations/regulations_guidelines/Information_Security_Guidelines.htm
[20] http://www.globalfoundationservices.com/security/documents/SecuringtheMSCloudMay09.pdf, page 11

Microsoft

As described, Microsoft uses a dedicated team of individuals to monitor its infrastructure and services for security and privacy incidents. This Security Incident Management team responds to issues 24 hours per day, every day. The team's mission is to:

> "… quickly and accurately assess and mitigate computer security incidents involving Microsoft's Online Services, while clearly communicating relevant information to senior management and other concerned parties within Microsoft."[21]

In addition, Microsoft conducts many types of internal risk assessments to understand and mitigate the possibility of privacy and security incidents.

University of Toronto

The University Information Security team takes an active role to identify and remedy potential privacy breaches. Penetration testing is performed regularly and results given to departments to enable them to better secure resources. The University also uses Intrusion Detection and Prevention Systems (IDS and IPS) to actively monitor the network to detect and prevent threats to critical resources. The Information Security team regularly reviews authentication logs to look for aberrant behaviour that might indicate accounts that have been compromised.

What gaps remain?

Both Microsoft and the University of Toronto take a proactive approach to protection of privacy. From top leadership to operations, both demonstrate a clear and consistent commitment to the privacy and protection of data that they steward. All reasonable efforts are made to discover, assess, and mitigate potential risks and threats as early as possible.

[21] http://www.globalfoundationservices.com/security/documents/SecuringtheMSCloudMay09.pdf, page 11

2. Privacy as the Default setting

> We can all be certain of one thing – the default rules! *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*.[4]

Is Privacy the Default setting?

Is personal information automatically protected in IT system, business practice and physical design? Yes. How?

Microsoft

Microsoft makes privacy its default by employing a deny-by-default design in its physical and logical operations, with policies that deny access by default, following a least privilege principle and reviewing access privileges on a periodic basis.

University of Toronto

The University takes a strong stance on protecting data and minimizing access to data by default. The University's Data Protection Guidelines state:

> "Data must be protected from unauthorized access or alteration while the data are in use, in physical or electronic storage, in physical transport or electronic communication, or under administrative access. Access to confidential information must be on a need-to-know basis only; need-to-know requirements must be documented as a requirement of job duties or contractual obligations."[22]

The Guideline states that access controls for confidential or personal information must be "… proportionate to the risk to the University due to unauthorized disclosure, deletion, modification or duplication of data."

Is the purpose for the collection, use, retention and disclosure of personal information clearly communicated to the individual at or before the collection? Yes. How?

The University uses a notice of collection:

> The University of Toronto respects your privacy.
>
> Personal information that you provide to the University is collected pursuant to section 2(14) of the University of Toronto Act, 1971.
> It is collected for the purpose of administering admissions, registration, academic programs, university-related student activities, activities of student societies, safety, financial assistance and awards, graduation and university advancement, and reporting to government agencies for statistical purposes.
> At all times it will be protected in accordance with the *Freedom of Information and Protection of Privacy Act*. If you have questions, please refer to www.utoronto.ca/privacy or contact the University Freedom of Information and Protection of Privacy Coordinator at McMurrich Building, room 104, 12 Queen's Park Crescent West, Toronto, ON, M5S 1A8.

[22] http://www.its.utoronto.ca/rules-and-regulations/regulations_guidelines/informationsecurity/Data_Protection_Guidelines.htm

In addition, a detailed notice will clearly inform students of purposes of the collection of personal information, uses and disclosures if they choose to use Live@edu. The notice will make the service transparent and understandable to students, supporting privacy by giving students knowledge and control.

Supplementary to core Live@edu service, Microsoft offers additional services like its SkyDrive online storage. Microsoft will provide students who choose to use extra services with a detailed notice of collection explaining if additional personal information will be required and for what purposes. Students who wish to use those services can agree with Microsoft for their use.

Students will be given the option to use the Live@edu service or provide a forwarding address for email. Students will be provided clear and persistent choices for opting out of Live@edu.

Is the collection, use, retention and disclosure of personal information limited to the strict minimum necessary, and consistent with individual consent, including secure destruction?

Yes. *How?*

Microsoft

The agreement with Microsoft states:

> "Microsoft shall not collect, use or disclose any Personal Information of End Users, or any derivatives of such Personal Information, except to provide the E-Mail Service to End Users and perform its obligations under this Agreement or except as otherwise permitted under this Agreement."

Microsoft encourages data minimization wherever possible, which reduces the risk to personal information. In its document "Privacy Guidelines for Developers", Microsoft advises:

> "One of the best ways to protect a customer's privacy is to not collect his or her User Data in the first place. The questions that should constantly be asked by architects, developers, and administrators of data collection systems include:
>
> - Do I need to collect this data?
> - Do I have a valid business purpose?
> - Will customers support my business purpose?" [23]

The document instructs developers to consider all possible uses of data, including secondary uses such as marketing analyses and recommends that data only be collected as necessary for immediate planned uses. It also suggests that wherever possible, data be aggregated and removed entirely if no longer needed.

The SAS 70 report provided to the University demonstrates secure destruction of data which has reached the end of its lifecycle.

University of Toronto

The University is committed to the principle of data minimization as noted. The University's Data Protection Guidelines state: "Access to confidential information must be on a need-to-know basis only; need-to-know requirements must be documented as a requirement of job duties or contractual obligations."

University privacy practices also require that no more personal information be collected than is needed for official University purposes.

[23] http://go.microsoft.com/?linkid=9746120, page 9

Does the project meet or exceed the requirements of FIPPA? *Yes.* *How?*

FIPPA Risk

Consistent with its commitment to the principles of FIPPA, the University analyzed how well Live@edu meets FIPPA privacy requirements and explored mitigation strategies to best reduce privacy risk. The details are in Appendix H. It is divided into six sections: collection, use, disclosure, retention, disposal of data and security. Many mitigations are contractual and excerpts of the agreement with Microsoft have been included in the analysis. Although the agreement does not state that Microsoft will comply with FIPPA, the University is satisfied that Microsoft's contractual commitments support privacy protection consistent with FIPPA standards.

What gaps remain?

Global Address List

The Global Address List (GAL) in *Live@edu* is a central directory of information about users in a domain. At the University of Toronto, this will include students who opt to use the *Live@edu* service. To be functional, the GAL must at least contain user name and email address, which would be visible to all other users. It would be simple to turn off the GAL by default, however some functionality is lost when the GAL is not available, including:

- Cannot use Outlook 2007 & 2010 in "native" mode (MAPI, OutlookAnywhere)
- Cannot create distribution groups

It is expected that the primary method of connecting to *Live@edu* will be through the web client (OWA), so users are not expected to be in the GAL. If an opt-in is provided for individuals interested in GAL dependent functions, an appropriate notice will be provided, explaining the consequences of being listed in the GAL, i.e., being globally[24] searchable.

[24] "Global" in this context refers to the users that the University of Toronto creates in their own instance of *Live@edu,* not all users of the *Live@edu* service worldwide.

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]

Is Privacy Embedded into the Design?

Is privacy embedded into the architecture of IT systems and operations in a holistic, integrative and creative way? Yes. How?

Microsoft

Microsoft has an extensive document detailing guidelines that developers should follow when developing software products and services.[25] The document makes developers aware of such privacy-protecting practices as:

Data Minimization

- "One of the best ways to protect a customer's privacy is to not collect his or her User Data in the first place."
- "Employee access to User Data should be limited to those who have a legitimate business purpose for accessing the data."
- "The risk of data exposure can be further minimized by reducing the sensitivity of stored data wherever possible."
- "The longer data is retained, the higher the likelihood of accidental disclosure, data theft, and/or data growing stale. User Data should be retained for the minimum amount of time necessary to support the business purpose or to meet legal requirements."

Notice, Choice, and Consent

> "All products and services that collect User Data and transfer it must provide an explanation ("give notice") to the customer. The customer must be presented with a choice of whether to provide the information, and consent must be obtained from the customer before PII can be transferred from the customer's system."

Security

> "Security is an essential element of privacy. Reasonable steps should be taken to protect PII from loss, misuse, unauthorized access, disclosure, alteration, and destruction."

Access

> "Customers must be able to access and update PII that is stored remotely. When customer contact preferences are collected, customers must be able to view and update their preferences."

Data Integrity

> "Reasonable steps must be taken to ensure that PII is accurate, complete, and relevant for its intended use."

[25] http://download.microsoft.com/download/3/8/5/385BEAE9-72E9-4F7F-A798-9D54F896351A/privacy_guidelines_for_developers.pdf

Each of these is a core privacy or security principle. It is encouraging to see them built into the design of Microsoft products and services through the education of developers.

University of Toronto

The University of Toronto embedded privacy design into the infrastructure that will be interfacing with the Live@edu system.

Encryption of mail flowing between the University's mail routers and Microsoft's is provided by a service called Forefront Online Protection for Exchange (FOPE). The functioning of this service is reinforced through firewall rules, managed by the University of Toronto, that block traffic on unencrypted ports, and through the configuration of the U of T Message Router to only accept encrypted traffic, regardless of network port.

The University will provide authentication services for Live@edu, to retain control of user names and passwords, and for the most part, to avoid passwords flowing through Microsoft's servers. This is described in more detail in principle 5, Data Flows section.

Has a systemic, principled approach to embedding privacy been adopted, relying upon accepted standards and frameworks, which are amenable to external reviews and audits? Yes. How?

Stakeholder Expectations[26]

An extensive stakeholder consultation preceded and informed the selection of the vendor and negotiations regarding features, security, privacy and functionality. The consultation elicited and incorporated views of experts, users and University communities, to ensure that all stakeholder expectations including privacy and security were embedded from the start and optimally implemented in a positive-sum way. This process ensured visibility and transparency of design and implementation in a meaningful user-centric manner.

A committee was formed to solicit input from students about e-communications. The committee met four times between November 2009 and January 2010 and also provided an anonymous web form available on the I+TS website along with full information about the consultation. Various media were used to direct interested parties to the form including RSS feeds, Facebook, notices distributed by Student Life staff and email sent to students.

Security and privacy were the most commonly raised concerns about outsourcing email to an external provider. Students who participated in the consultation expect the University to protect their information. They expressed concern about the misuse of information (e.g. data mining) and advertising by an external provider. Concerns about the USA PATRIOT Act were 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. While discussion made it clear that the University should ask tougher security and privacy questions of all its systems and practices, it was agreed that consideration of outsourcing would have to thoroughly investigate and clarify risk to security and privacy. Concerns raised by faculty and staff focused on issues surrounding trans-border information flow and intellectual property ownership.

Stakeholder consultation has continued since the committee was formed. The CIO's third report on the Student e-Communications project details some further consultation:[27]

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

> *A 34 question survey on email use and future services was developed with the assistance of Student Life and delivered to 6000 undergraduate, graduate and professional students. The survey received 429 responses that closely paralleled the feedback received earlier from student members of the committee. A summary of the responses is on the I+TS website.*[28]
>
> *With the assistance of Student Life, invitations to meet with project staff were sent to student organizations on all three campuses. A drop-in session was held July 12th, and the Engineering Society executive arranged a follow-up consultation on July 26th. Feedback received aligned with survey and earlier consultation results. A meeting with members of the UTSU Executive took place September 3rd.*
>
> *I+TS staff met with UTFA Council on May 20th. A meeting with three faculty members from Arts & Science and OISE was held June 10th to consider their security and privacy concerns, including trans-border information flow and intellectual property ownership. They asked that care be taken with respect to data storage, security and personal information privacy. They supported the proposed opt-out provision for students.*

While not all risks raised by students, staff and faculty can be fully eliminated, this PIA explores reasonable mitigations to reduce privacy risk associated with the project.

SAS70 Type II Attestation

The SAS70 Type II report referenced in the Resources Consulted section contains highly detailed information provided about Microsoft's internal systems. Since this was an essential verification for Microsoft security assurances, the following specifics are set out in detail.

SAS70 defines the standards that an auditor must follow when carrying out an audit of the internal controls in a service organization. That is, SAS70 is an audit standard, not a security or privacy standard. There are a few things to keep in mind about this report:

1. A SAS70 Type II Attestation is a measure of a company's adherence to their defined controls; whether they are doing what they say they are. Since SAS70 does not define the security controls, it is not necessarily a good indication of the security of an organization. It is therefore important to understand what standard of security they have committed themselves to. In Microsoft's case, they asked to be evaluated by the "ISO 27001: Specification for an Information Security Management System" standard.
2. It is important that the standard being audited be broad enough in scope to cover all of the infrastructure and software that the University's personal information will be stored on. "ISO 27001 specifies requirements for the establishment, implementation, monitoring and review, maintenance and improvement of a management system **-** an overall management and control framework - for managing an organization's information security risks. It does *not* mandate specific information security controls but stops at the level of the management system."[29] The SAS70 Type II audit provided by Microsoft covers their management system, not specific controls that have been put in place. Understanding Microsoft's overall management strategy for managing risk is as important as having a good grasp of the specific security controls in place.
3. A SAS70 Type II attestation is not a tool to monitor the ongoing state of security at an organization, but a review of past events, and the effectiveness of the controls in place to prevent security incidents. A Type II attestation will cover a specified length of time.

[27] http://www.its.utoronto.ca/Assets/ITS+Digital+Assets/Report+3+-+Student+e-Communications+Consultation.pdf
[28] http://www.its.utoronto.ca/Assets/ITS+Digital+Assets/Appendix+3+Student+Survey+Summary.pdf
[29] *ISO/IEC 27001 Certification Standard*, http://www.iso27001security.com/html/27001.html (Novemember 2010).

On the basis of the usefulness of the SAS70 Type II attestation, the following wording is included in the draft agreement with Microsoft:

> "Microsoft shall cause its external auditors to provide to Institution a SAS 70 Type II report (or equivalent) annually throughout the term of the Agreement on the design, existence, effective operation and continuity of Microsoft's control procedures in respect of the data centers used to provide the E-Mail Service. Where the SAS 70 Type II report identifies material deficiencies in the data centers used in the performance of the E-Mail Service, Microsoft shall provide to Institution a remedial plan to address such deficiencies and shall report to Institution on the progress made in executing such plan."

Has a detailed privacy impact and risk assessment been carried out and published, documenting the privacy risks and measures taken to mitigate those risks? Yes. How?

The University conducted a detailed Privacy by Design Privacy Impact Assessment process to thoroughly address risk assessment and document privacy risks and measures taken to mitigate those risks. Data flows were documented and analyzed for privacy impact and risk assessment, both in-house and at Microsoft (detailed analysis of these data flows is found under principle 5 below). The University published an early version of the PIA and intends to publish an implementation version on the University website. The PIA will continue to develop and guide the Live@edu project through its lifetime.

What gaps remain?

Some residual risks have been identified in Appendix A, "Analysis of Residual Risks".

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.[4]

Is there Full Functionality in a Positive Sum manner?

Are all system requirements optimized to include full functionality, privacy and security?

Yes. *How?*

The relationship between Microsoft and the University is a positive sum exercise in which each party seeks an optimal mix of ingredients. For the University, these include full functionality, privacy and security, features, low cost and flexibility. Through its agreement with a cloud vendor, the University seeks to provide a world-class email service for students, to enhance their University experience, complete their coursework, build and maintain relationships with their professors and fellow students. Providing this enhanced email service will improve the student experience and the relationship between the University and its students.

Microsoft has integrated both security and privacy into its Security Development Lifecycle (SDL)[30] [31], the Microsoft methodology for developing all software and services. This appears to be a highly effective approach for developing software that respects privacy in a positive-sum way.

Are all legitimate non-privacy objectives embraced and accommodated in an innovative, positive-sum manner? Yes. *How?*

Live@edu provides a level of service that it would be prohibitively expensive for the University to duplicate. Some of the benefits of Live@edu include:

- Increasing mailbox storage from 120 MB to 10 GB, an increase of some 85 times
- Addition of student calendaring, instant messaging solution
- Increased availability, redundancy of services
- Modern, usable web-based interface
- Leveraging the multi-billions of dollars of investment by Microsoft in their infrastructure, and their full time security staff
- Updates applied to infrastructure at no cost to the University
- Optional availability of online document storage

These features are key benefits to users and to the University, which in a positive sum context will be delivered together with strong privacy protections and sound security.

Is creativity and innovation used to achieve all objectives including privacy? Yes. *How?*

The University uses Shibboleth technology (described in Appendix G “Technology Overview”) to implement a federated identity system that allows the University to protect the privacy of usernames and passwords by processing them at the University without providing them to

[30] http://msdn.microsoft.com/en-us/library/ms995349
[31] http://go.microsoft.com/?linkid=9746120

external service providers. This is discussed in more detail in the Data Flows section referenced in principle 5 below.

Cloud Computing

Considerable effort was made to analyze the cloud computing model used by Microsoft to provide the *Live@edu* service. As the Internet has evolved, companies have increasingly leveraged economies of scale by centralizing computation resources in data centers and relying on the Internet to transfer information to and from these data centers and clients.

Given the relative novelty and rapid change of cloud computing models, it is important that the University understand the implications of using such a service.

Traditional computing models focus on establishing a secure perimeter around a set of "trusted" machines that comprise the (University) network, with appropriate attention to endpoints of communication as information leaves the trusted environment.

In a Cloud computing context, the secure perimeter must be expanded around resources under control of the external provider (and beyond direct control of the University). This represents a significant risk to the University and care must be taken to ensure that this extension of trust is both reasonable and prudent. The general types of cloud computing services and modalities are described in Appendix B "Cloud Computing Models".

Live@edu is offered as a Software as a Service model and is run in a public, off-premises cloud wholly owned and operated by Microsoft. A key implication of this is that the University is effectively outsourcing the security of its email platform to Microsoft, from the network infrastructure all the way up to the application. It is essential that the University assess the reliability and trustworthiness of Microsoft's reputation 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 to the external provider at every stage of the development of its services and infrastructure. A recent privacy breach[32] in a Microsoft cloud computing environment illustrates the potential risk of SaaS contexts, with a system vulnerability enabling users to access each other's information. While this breach was, according to Microsoft, minor and brief, it is not unique and the existence of problems of this type is a significant factor in the decision to adopt cloud based services. Microsoft's SAS70 Type II audited compliance with the ISO 27001 standard for an information security management system will be integral to establishing trust.

A recent paper released by NEC and the Office of the Information and Privacy Commissioner entitled *Modelling Cloud Computing Architecture Without Compromising Privacy* served as an ideal against which *Live@edu* was measured. While *Live@edu* did not achieve every single standard set out in the paper, Microsoft privacy solutions exhibit a well tuned sense of privacy issues. The IPC/NEC paper states:

> "there is, of course, further work to be done in the research and engineering disciplines. ... As such we call to action the research and engineering domains for provision of security and privacy-enhancing technologies, and those in the operational domain to deploy these technologies."[33]

The University is committed to the vision of privacy set out in this paper and will continue to monitor the industry for developments in this direction. No currently available email providers

[32] http://www.pcworld.com/article/214591/microsoft_bpos_cloud_service_hit_with_data_breach.html?tk=mod_rel

[33] *Modelling Cloud Computing Architecture Without Compromising Privacy*, 2010 http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=961 (July 2010), p. 18

offer the level of security and privacy defined by the paper's cloud computing model. In the absence of such technology however, the architecture Microsoft has pursued -- transport layer encryption (protecting the data as it flows between the end-user and Microsoft) and strict, audited security controls -- provides a next best alternative.

Data Residency

Given the nature of cloud-based services, there is a degree of uncertainty as to the exact location of the University's data at any given time. Microsoft stated that the University's data will reside within two datacenters, and in three locations within each datacenter. Under a non-disclosure agreement, Microsoft revealed to the University the approximate locations of its currently operating datacenters and their expected use for U of T Live@edu service.

What gaps remain?

Foreign Legislation

In cloud environments, it is increasingly common for service providers to use globally distributed resources, which, by virtue of such distribution, are beyond geographic reach, and may be subject to the laws of foreign jurisdictions. The Ontario government publication, "*Guidelines for the Protection of Information when Contracting for Services*" attributes high risk to storage of sensitive information outside Canada. This risk must be addressed in every project or activity. This type of risk is usually addressed through contractual security and privacy assurances by the service provider to protect data in all contexts, at all times and in all locations. These assurances are provided by Microsoft in its agreement with the University.

Microsoft is a U.S. based corporation subject to U.S. legislation, including the USA PATRIOT Act. Information about the USA PATRIOT Act is set out in Appendix C.

Under its agreement with Microsoft, U of T will be given prior notice of disclosures by Microsoft when legally possible. This is the soundest assurance that can be provided by Microsoft. Users will be notified that their information will reside outside Canada before signing up for Live@edu.

5. End-to-End Security - Full 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.[4]

Does the Project Apply End-to-End Security, achieving Full Lifecycle Protection?

Are there strong security measures in place throughout the lifecycle of the data so that the data is retained securely? Yes. How?

Data Flows Analysis

A fundamental PIA component is a description and analysis of information flows. This section comprises a high level overview of information at risk and key actors, and an analysis of personal information transactions within the system. Due to the closed nature of the *Live@edu* system, these transactions can only be examined at a relatively high level of granularity.

Information at Risk

This PIA uses the FIPPA definition of personal information (see Appendix D). Email and other communication/collaboration tools involve the collection and exchange of personal information.

Email is used to communicate personal information and other Live@edu services may be usable to store or communicate information including (but not limited to):

- assignments or notes
- official communications with the University transmitted by email
- calendar appointments
- information stored in *SkyDrive*, an optional online storage service

An overview of Live@edu service dataflows and processes, including, major parties, migration processes, email flow, protection, encryption, web/non-web access, backups and termination of service, is set out in Appendix E.

Summary

Transport encryption, which is used throughout the Live@edu system, protects information (including student personal information) in transit, as it flows over the Internet from U of T to the Microsoft data centers and back.

Offering an opt-out to students before they sign up for *Live@edu* gives them the option to use other email services if they are not satisfied with the privacy afforded by *Live@edu*.

Most large email providers (Google, Yahoo, etc.) are U.S. based/international so opting out of Live@edu is unlikely to solve problems of data being stored, transported or used in other jurisdictions.

Are the security measures consistent with standards developed by recognized bodies? Yes. How?

Microsoft maintains a SAS70 Type II Audit certifying compliance with the ISO 27001 standard for Information Security Management Systems.[34] [35]

Microsoft recently achieved the Federal Information Security Management Act (FISMA) certification & accreditation for its data centres.[36] This certifies that the security of Microsoft's cloud computing infrastructure is sufficient for obtaining U.S. government contracts.[37] [38]

Industry standard transport layer encryption (SSL/TLS) has been required during transmission of all data across all life-cycle stages of this project.

Do the security standards assure the confidentiality, integrity and availability of the personal information including secure destruction, appropriate encryption and strong access controls and logging methods? Yes. How?

The SAS70 report provided to the University by Microsoft indicates a comprehensive approach to infrastructure security. Starting at the highest levels, the company conducts risk assessments, implements security controls and regularly monitors the success of those controls to protect its valuable resources. The document shows how in each of the three cornerstones of PbD (information technology, accountable business practices and physical design & infrastructure) Microsoft maintains a high level of security. The ISO 27001 and FISMA certifications indicate a security standard greater than that currently maintained by the University of Toronto.

In addition to the security standard outlined above, the agreement with Microsoft includes a number of contract points that ensure:

- Information confidentiality to the extent consistent with law and best efforts to give notice of disclosures;
- Information integrity consistent with reasonable standards;
- Return or destruction of confidential information and;
- Access controls, including security and confidentiality and on request return or destruction of confidential information.

What gaps remain?

This project considered the full life-cycle of the personal information that is to be protected and achieves a level of security that is appropriate to the sensitivity of the information that is going to be collected / used / disclosed.

[34] http://en.wikipedia.org/wiki/ISO/IEC_27001

[35] Microsoft ISO 27001 Certifications

[36] http://blogs.technet.com/b/gfs/archive/2010/12/01/microsoft-s-cloud-infrastructure-receives-fisma-approval.aspx

[37] http://en.wikipedia.org/wiki/FISMA

[38] http://csrc.nist.gov/groups/SMA/fisma/index.html

6. Visibility and Transparency – Keep it Open

> *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.[4]

Does the project operate with visibility, transparency and openness?

Is responsibility for privacy-related policies and procedures documented, communicated and assigned to a specific individual? Yes. How?

Privacy is a shared responsibility at the University. The FIPP Office takes the lead in providing training and advice to University units that interact with personal information.

Both Microsoft and the University will be provided with critical communication contacts and a process to address privacy questions and concerns.

Is there trust of the vendor and is privacy protection assured by the vendor through contractual or other means, e.g. no data mining, no ads? Yes. How?

A detailed analysis of the agreement was performed, comparing it against the FIPPA legislation. It was found that the agreement gives the University the assurance that Microsoft is operating within the bounds of FIPPA. [Redacted]

Is information about the policies and procedures relating to the management of personal information readily available to individuals? Yes. How?

The University conducted extensive stakeholder consultation throughout this project (see section on Stakeholder Expectations). An earlier version of this PIA has been made available on the I+TS website for public review and comment.

The FIPP website provides information on the legislation and policies governing the management of personal information at the University,[39] and the website of the Provost details University privacy and personal information practices.[40]

Microsoft has detailed documentation about its security and privacy practices on its website. [41] The SAS70 Type II report and FISMA certifications were shared with the University.

Have complaint and redress mechanisms been established and communicated to individuals? Yes. How?

There are two redress mechanisms in place at the University of Toronto:

1. The University's FIPP Office addresses questions or concerns about personal information and looks into privacy concerns.

[39] http://www.fippa.utoronto.ca/Page4.aspx

[40] http://www.provost.utoronto.ca/Assets/Provost+Digital+Assets/Provost/fippa.pdf

[41] http://www.microsoft.com/privacy/default.aspx

2. For technical support questions, the University has an established Help Desk available on the web and on the telephone. Help Desk personnel will receive specific training with respect to the Live@edu service and the technical issues that may arise.

A privacy fundamental at Microsoft is the "monitoring and enforcement of compliance with their privacy policies, both internally and with our vendors and partners, along with established processes to address inquiries, complaints and disputes."[42]

Have steps been taken to monitor, evaluate and verify compliance with privacy policies and procedures? Yes. How?

Verification of Privacy Policies and Commitments

It is critical that the University can verify the commitments Microsoft has made about the privacy and security of their systems and procedures. The SAS 70 audit that the University obtained contains a third-party analysis of the claims that Microsoft makes. While this audit is an excellent first step, the University will go further to confirm that Microsoft's service and actions are privacy protective and appropriately secure. Much of this verification will necessarily leverage relationships between the University and Microsoft.

These relationships have been developed across key areas including decision makers, legal practitioners, privacy officials, and technical staff dealing with the functional and security aspects of the project. Negotiations and understandings of University and Microsoft decision makers are reflected in the agreement between the two organizations. The agreement delineates the operational relationship, which enables the University to abandon the service if it does not continue to meet its needs on a positive-sum basis, including function, security and privacy.

While the contract does not explicitly detail all security and privacy actions, University technical staff are working with leading Microsoft technical experts to develop and define system parameters to meet University functional, security and privacy requirements, guided by Privacy by Design. As the system is rolled out and later through its operational life, Microsoft and University staff will continue to work together to ensure functionality, security and privacy.

Through this ongoing relationship, the University will continue to confirm that Microsoft continues to meet privacy and security expectations. It is expected that operational staff at both organizations will communicate clearly and completely to create an environment of mutually verifiable assurances in system design, configuration, implementation and operation. This speaks to accountable business practices, with the University and Microsoft relationship fostering a culture in which the right privacy actions are demonstrably taken and supported.

During the development of this PIA, Microsoft was sensitive to University privacy concerns, responding efficiently and quickly, and providing requested documentation. The University was assigned a Microsoft client representative, Karen McGregor, who provided useful access to other Microsoft resources. Microsoft consultants; Richard Wakeman and Dimtry Kazantsev, have assisted the U of T implementation team. In addition, U of T worked with David Fischer of Microsoft who is Senior Product Manager of Live@edu Research and Development.

As the project progressed, the University realized that encryption of mail between the University's mail routers and Microsoft's is provided by a service called Forefront Online Protection for Exchange (FOPE). This service is not enabled by default, and the University

[42] http://go.microsoft.com/?linkid=9741061

requested that it be turned on for its test users. FOPE has now been tested by the University and is active.

The University worked to enable federated authentication through the SAML technology implemented by Shibboleth. Although Microsoft has a preference for its own ADFS authentication, it has nevertheless delivered on its commitment to provide this functionality to the University via Shibboleth.

Once Live@edu is implemented, the University will work with Microsoft to ensure an appropriate level of support, concomitant with Microsoft's current commitments and actions. In anticipation of future issues, the University will work to ensure that its relationship with Microsoft will ensure effective, timely resolution of problems, sound security and strong privacy protection. While operational details are yet to be determined, the University will vigilantly pursue a constructive and useful working relationship with Microsoft in support of these goals.

What gaps remain?

Although the contract supports privacy protection, and the Microsoft website features privacy design, the contract does not specifically state that Microsoft will support Privacy by Design principles. This is not expected to be an issue in the context of the expected mutually supportive relationship between the University and Microsoft, in which excellent and visible protection of privacy is essential to the University's commitment to its communities and to Microsoft's ongoing credibility as a world-class cloud service provider.

7. Respect for User Privacy – Keep it User-centric

> 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.[4]

Is there a user-centric respect for User Privacy?

Are data subjects empowered to play an active role in the management of their own data? Yes. How?

Microsoft has a commitment to empowering users in their *Privacy Guidelines for Developing Software Products and Services*[43]: "Customers will be empowered to control the collection, use, and distribution of their personal information." The University will provide an opt-in approach for all new students using the Live@edu service, giving them the choice to forward their email elsewhere if they so choose. Students will have the opportunity to use additional services (such as SkyDrive) from Microsoft, but these services will be provisioned only by the student's request.

For those students who choose to use the Live@edu service, it is important to keep in mind that it is fundamentally in the nature of email to be user-driven. Each person using the service decides what emails they will send, and the content of those emails.

Has free and specific consent been established for the collection, use or disclosure of personal information and can consent be withdrawn? Yes. How?

As indicated above, the service will be opt-in for new students of the University. An appropriate notice will be developed informing the user how their information is going to be collected, used and disclosed within the Live@edu service. If at any time the student does not wish to use the Live@edu service anymore, they will be free to copy the contents of their email out of the service and begin forwarding their University email to a different email address.

Are individuals given a clear Notice of the uses and disclosures or their personal information? Yes. How?

A detailed notice of collection will be prepared by the University for students to read and accept before beginning to use the Live@edu service. Microsoft terms of use and privacy conditions will be made available for students in their interactions with Microsoft itself.

Summary

Microsoft appears to have a fundamental commitment to the privacy of the users of its products. Microsoft communicates an understanding that privacy must be built into a system at the very beginning, it provides extensive guidelines to its developers to enable them to incorporate privacy into their design. External audit documentation attests that Microsoft's commitment to privacy extends through all levels of the organization, and shows that a comprehensive approach to protecting customer personal information has been implemented.

[43] http://go.microsoft.com/?linkid=9746120, page 6

Appendix A: Analysis of Residual Risks

This appendix sets out the residual risks that remain for the executives of the University of Toronto to accept or reject. The University performed detailed analysis of the data flows in order to identify all potential risks. Systems that interact with user information and staff who have administrative system control were considered. Network communications were also considered, but were excluded from detailed analysis here because properly implemented encryption reduces their risk to negligible levels. While careful analysis was performed, it is possible that unknown risks remain.

Several components of the U of T infrastructure will be leveraged to integrate *Live@edu* into the U of T email ecosystem. Possible risks affecting these infrastructure components were identified. Briefly, these previously existing risks include:

- Hacker attack of U of T infrastructure including email routing and identity management systems
- Errors of U of T staff responsible for managing or supporting email that lead to personal information exposure
- Inadvertent or malicious access or use of personal information by U of T systems staff.
- User password compromise through use of infected computers.

Proxy Server Compromise

Description of risk:

Microsoft implemented a proxy server that allows non Shibboleth-enabled clients to use Shibboleth authentication. This allows them to integrate with the University's identity management system for authentication and authorization. The user credentials will be sent to the proxy server, which will then communicate with the University's identity system to authenticate the user. The authentication proxy will be used by email clients (such as Outlook or Thunderbird) and mobile devices to authenticate users to the *Live@edu* service. If an attacker (or unauthorized malicious Microsoft employee) was able to compromise (or 'hack') the proxy server, they might be able to collect user credentials as they flow through the server.

Impact:

UTORid credential theft, which could lead to user accounts being used for spam or fraud. There is also the risk of the theft of personal information.

Existing Mitigations:

- Microsoft already uses encrypted communications to and from the proxy server.
- Microsoft assures us that the credentials are not permanently stored on the proxy server. However, the passwords are briefly stored in the memory of the proxy server during the authentication process.
- The server is located in Microsoft's physically secure data center (which can prevent physical tampering).
- Microsoft monitors all of their servers for signs of compromise or suspicious activity.

Potential Mitigations:

The University can optionally disable this method of authentication for its users, which would force users to use the web interface.

Residual Risk:

University of Toronto student's UTORids and passwords could potentially be harvested from a compromised Microsoft authentication proxy server.

Probability: Low, Impact: High.

Global Address List

Description of risk:

Live@edu has a feature called the Global Address List (GAL). The GAL is a listing of the names and email addresses of all users[44] that have the feature enabled.

Impact:

Exposing names and email addresses of users within U of T's *Live@edu* service could go against the idea of privacy by default. Enabling the GAL would provide an opportunity for users to harvest email addresses for bulk unsolicited email or other unauthorized purposes. This could result in complaints against the University and harm to the University's reputation.

Potential Mitigations:

Given the risk to privacy the University should not enable the GAL by default. It should be acknowledged by the University that this is the only reasonable privacy-respecting course of action. Provision could be made for users to opt-in to the feature once they indicate that they are willing to accept the risk of their name and email address being available to other users.

Residual Risk:

If the above mitigation was applied, the user would assume the risks and there would be virtually no remaining risk to the University.

Probability: Medium, Impact: Low

Unknown Software Vulnerabilities

Description of risk:

All complex software systems contain unknown vulnerabilities, some of which may be exploited to gain unauthorized access to data stored in the system.

Impact:

The personal information of one of more U of T students could be accessed by the attacker, with possible outcomes such as identity theft, harm to reputation or personal distress.

[44] "All users" in this context refers to the users that the University of Toronto creates in their own instance of *Live@edu,* not all users of the *Live@edu* service worldwide.

Existing Mitigations:

Microsoft integrated security and privacy into their Security Development Lifecycle which results in fewer software defects. Microsoft has also implemented comprehensive security training for their employees. Systems in their data centres are monitored continuously for evidence of security breaches.

Residual Risk:

While there are risks pertaining specifically to *Live@edu*, these are somewhat offset by the decommissioning of the UTORmail infrastructure that was serving students. Microsoft's concern for their reputation in the industry gives them sufficient motivation to ensure the security of their service.

Probability: Low, Impact: High

Microsoft Employee Acting Without Authorization

Description of risk:

Given the nature of outsourcing the University's email infrastructure, the University is trusting that Microsoft and its employees will be responsible with its data. If one of those employees were to maliciously violate corporate policy, they could abuse the personal information stored within their infrastructure. This occurred with Google's Gmail in July 2010[45].

Impact:

The personal information of one of more U of T students could be misused by Microsoft staff acting without authorization, with possible outcomes such as identity theft, harm to reputation or personal distress.

Existing Mitigations:

Microsoft maintains excellent access control policies and mechanisms as evidenced by the material in their SAS 70 report.

Residual Risk:

Only some of the University's data would be vulnerable until the unauthorized access were discovered by internal audit, or otherwise detected. Depending on the effectiveness of Microsoft's internal audit, such an exposure could last from days to months.

Probability: Low, Impact: Medium.

Accidental disclosure by a Microsoft employee

Description of risk:

It is possible that a Microsoft employee could mishandle data or applications, leading to exposure of personal information. This happened in December of 2010, when a "configuration issue" in one of Microsoft's services allowed address book information to be downloaded by unauthorized users.[46]

[45] http://techcrunch.com/2010/09/14/google-engineer-spying-fired/
[46] http://www.pcworld.com/article/214591/microsoft_bpos_cloud_service_hit_with_data_breach.html?tk=mod_rel

Impact:

The personal information of one or more individuals may be inadvertently disclosed to unauthorized persons.

Existing Mitigations:

In their SAS70 report, Microsoft indicates that they provide security and privacy training to their employees.

Residual Risk:

Because of employee training, and limited access to information, the residual risk is low. If there was a window of exposure it would last until detected by internal audit, or until reported.

Probability: Low, Impact: Medium

Foreign Legislative Threat

Description of risk:

Microsoft is clear about their requirement as a U.S. corporation to release information requested under the USA PATRIOT Act regardless of where that information is stored (even if it were housed on servers physically located in Canada). Microsoft is also prohibited from informing us about some types of USA PATRIOT Act requests.

Impact:

US authorities can request records of individual users, including emails, access logs and other personal information. In some cases the University will have no way of knowing if and when this is happening.

Potential Mitigations:

There are no mitigations for this, other than encryption. Products such as 'PGP Desktop Email', or the open source GnuPG are capable of encrypting the content of the email (but not the message headers, including sender, recipient and subject)[47]. These solutions are available to individuals, but would be either costly (PGP) or difficult to support (GnuPG) institution wide.

Residual Risk:

Because Microsoft is prohibited from informing us that data was released under the USA PATRIOT Act, the University has no way of reliably determining the probability of such occurrences.

Probability: Low, Impact: Medium

Attacks from within the cloud

Description of risk:

[47] Besides being technically hard to implement, encrypting only the message body is of dubious value given the circumstances. As Fred Carter of the IPC said at the Email Symposium held at Ryerson University: "Without minimizing the importance of encryption … all the action is in traffic data and who is talking to whom. A PGP type system doesn't [protect], in fact it actually facilitates … [the ability to] track everyone [a person] is communicating with and how frequently. … Maher Arar was hung because of who he spoke with, not because of anything he said."

Within the same Microsoft data centers as *Live@edu* are other Microsoft services, including Azure. There is a potential for attacks within the data center (or cloud) to leverage shared resources in order to attack the University's *Live@edu* service. The University could potentially experience a Denial of Service (DoS) attack, or a data breach leveraging shared hardware within the Microsoft data center.

Impact:

During a DoS attack, *Live@edu* services may be unavailable. A data breach leveraging shared hardware would likely result in a large amount of disclosed personal information.

Existing Mitigations:

- Microsoft monitors the networks and services within their data centers closely[48]:
"If any anomalies are detected, they will be investigated and resolved. Operational controls are incorporated to facilitate automated monitoring and early notification if a breach or problem occurs…"
- Microsoft invested significant effort into designing a secure data center infrastructure. They also routinely test their infrastructure to make sure it's resistant against hackers[49]:
"Penetration testing performed by internal and external parties provides important insight into the effectiveness of security controls for the Microsoft cloud infrastructure. The outcome of these reviews and ongoing evaluation of the resulting controls are used in subsequent scanning, monitoring, and risk remediation efforts."

Residual Risk:

Attacks from within the cloud may be able to leverage shared infrastructure, but the entire infrastructure in managed by Microsoft. They monitor the infrastructure, and have the ability to quickly terminate any malicious processes.

Probability: Low, Impact: High

Mishandling of data by University of Toronto

Description of risk:

During the migration to *Live@edu*, or during the ongoing management of the service, it's possible that the University of Toronto could inadvertently mishandle user data. User credentials or personal information could be inadvertently disclosed, through unencrypted communications, or other means.

Impact:

In the event of inadvertent disclosure, the number of potentially affected users would likely be large, but the probability of the data being intercepted is low.

Existing Mitigations:

- The University will not send user credentials to Microsoft. The authentication will use Shibboleth to integrate with the University's existing identity management system.

Potential Mitigations:

- The University must ensure that all communication channels between the U of T and Microsoft are encrypted. Based on discussions with Microsoft, this should be possible,

[48] http://www.globalfoundationservices.com/security/documents/SecuringtheMSCloudMay09.pdf, page 17
[49] http://www.globalfoundationservices.com/security/documents/SecuringtheMSCloudMay09.pdf, page 20

but some additional assurance that they will work with the University to enforce encryption is desirable.

- The University should define a set of best practices that define internal handling of student data.
- The University should audit its staff's privileged access to *Live@edu* in order to detect any potential abuse.
- The University should have a plan for users to opt-out prior to migration.
- The University should have a plan for users to migrate to a different email service provider.

Residual Risk:

If the University implements the above mitigations, the residual risk should be minimal. Probability: Low, Impact: Low

Improper Termination of Agreement

Description:

The University must consider that the agreement with *Live@edu* will eventually come to an end. Derek Yuen indicated that it would take the University of Toronto at least six months to migrate data out of *Live@edu* with the current amount of data When it is eventually time to migrate out of *Live@edu*, the University must ensure that there is sufficient time to exit in a secure and appropriate manner.

Impact:

The University could potentially lose all or part of stored messages within *Live@edu*.

Potential Mitigations:

- The University should ensure that its contractual agreement includes a clause that would provide U of T with suitable time to migrate its data out of *Live@edu*.
- When the time comes to end the agreement, the University should try to end it on good terms.

Residual Risk:

Microsoft is a professional organization with their reputation in the industry at stake. This is very unlikely to be a problem. There is little risk to privacy, as in the event of an abrupt termination of the agreement, Microsoft is more likely to delete data than disclose data.

Probability: Low, Privacy Impact: Low, Operational Impact: High

Summary of Residual Risks

The following table provides a short summary of the risks and an accept/reject box for each. The source column indicates the relevant legislation or analysis from this PIA related to the particular risk.

Risk	Description	Areas of Concern	Accept?
Proxy Server Compromise Probability - Low Impact - High	Microsoft authentication proxy server is compromised, revealing UTORids and passwords.	FIPPA *PbD*	□ Yes □ No
Global Address List Probability - Medium Impact - Low	The Global Address List exposes names and email addresses of subscribed users.	FIPPA *PbD*	□ Yes □ No
Unknown Software Vulnerabilities Probability: Low Impact: High	All complex software systems contain unknown vulnerabilities, some of which may be exploited to gain unauthorized access to data stored in the system.	*PbD*	□ Yes □ No
Microsoft Employee Acting Without Authorization Probability - Low Impact - Medium	An employee at Microsoft decides to use his/her administrative access without authorization to access *Live@edu* user information, potentially for illegal purposes.	FIPPA	□ Yes □ No
Accidental disclosure by a Microsoft employee Probability - Low Impact - Medium	A Microsoft employee accidentally discloses a user's personal information	FIPPA *PbD*	□ Yes □ No
Foreign Legislative Threat Probability - Low Impact - Medium	A request for information is made to Microsoft under USA PATRIOT Act or similar legislation	FIPPA	□ Yes □ No
Attacks from within the cloud Probability - Low Impact - High	Due to the shared nature of cloud computing, vulnerabilities of *Live@edu* might be exploited by other customers of Microsoft's cloud computing architecture	FIPPA *PbD*	□ Yes □ No
Mishandling of data by UofT Probability - Low Impact - Low	A University of Toronto employee accidentally discloses a user's personal information	FIPPA	□ Yes □ No
Improper termination of agreement Probability - Low Impact - Privacy: Low Operational: High	Potential for the relationship between U of T and Microsoft to sour, ending the contract prematurely.		□ Yes □ No

Appendix B: Cloud Computing Models

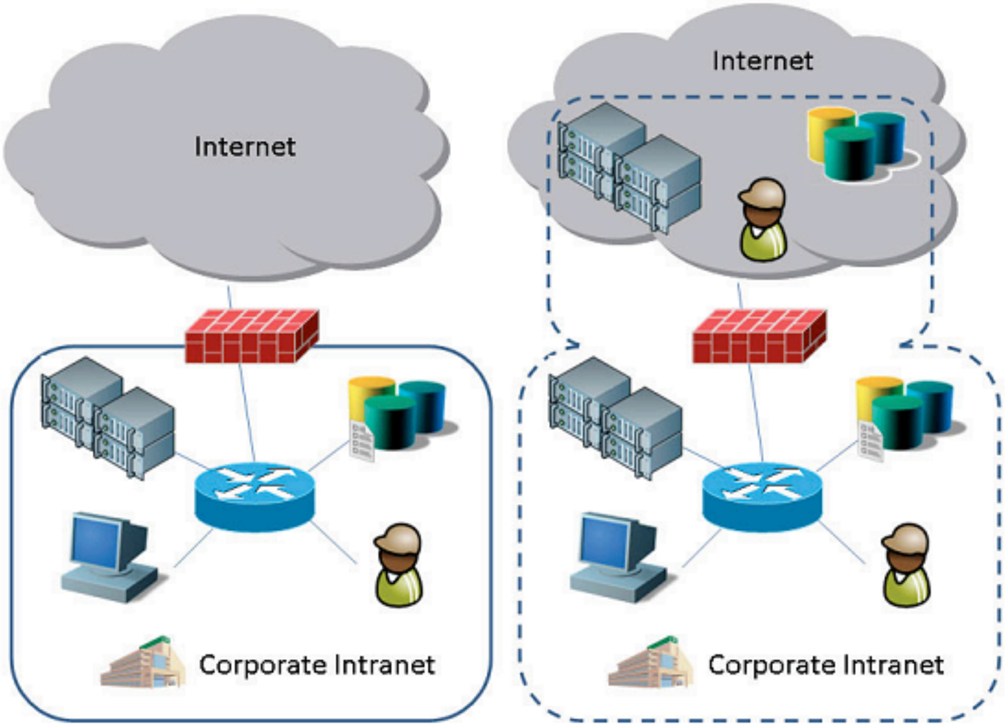


Figure 1 -- Left: Clear Distinction between the Trusted and the Untrusted; Right: Fuzzy Security Perimeter[50]

Cloud Computing has become an umbrella term for so many emerging technologies, that some clarification of what is meant is necessary. A paper released by the *Cloud Security Alliance* provides a helpful delineation of Cloud *Service* and *Deployment* Models.

Cloud Service Models[51]

- **Software as a Service (SaaS)** – This is the capability provided to a consumer to run the provider's applications in a cloud infrastructure. The applications are made accessible from various client devices usually through a thin-client interface such as a web browser. In this model the consumer does not manage or control any of the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

[50] *Modelling Cloud Computing Architecture Without Compromising Privacy*, 2010 http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=961 (July 2010), p. 6

[51] *Security Guidance for Critical Areas of Focus in Cloud Computing v2.1*, 2009 http://www.cloudsecurityalliance.org/csaguide.pdf (November 2010), p. 15-16

- **Platform as a Service (Paas)** – The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

- **Infrastructure as a Service (IaaS)** – The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

Cloud Deployment Models[52]

- **Public Cloud** – The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

- **Private Cloud** – The cloud infrastructure is operated solely for a single organization. It may be managed by the organization or a third party, and may exist on-premises or off-premises.

- **Community Cloud** – The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, or compliance considerations). It may be managed by the organizations or a third party and may exist on-premises or off-premises.

- **Hybrid Cloud** – The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

[52] ibid., p. 17

Appendix C: USA PATRIOT Act

The University of Alberta email outsourcing project website provides useful information about the USA PATRIOT act, which is included here for reference.[53]

> **Q. Does the US Patriot Act allow the US government to access my personal information?**
>
> A. Yes. The Patriot Act allows for the US Government to access personal information that is held or accessible by anyone within the United States or any US citizen by two different methods. The first tool which the US Government possesses is found in Section 215 of the Patriot Act. Under this section the relevant Government agency must apply to a court for an order allowing them to access the personal information in question. The information which can be collected pursuant to this court order is very broad. The second tool which the US Government has is found in Section 505 of the Patriot Act. It is under this section that the Government can issue National Security Letters whereby they can request that personal information be disclosed to them. The information can be accessed where it meets the following criteria: that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities. No court order is necessary for a National Security Letter to be issued; however, the type of information that is retrievable is more limited than through that available in a Section 215 (see above) order.

It should be noted that Canadian authorities have very similar abilities to access personal information to those in the USA PATROIT act, in Canadian legislation such as the Criminal Code, the Canadian Security Intelligence Service Act and the National Defense Act, among others. A key difference is that in general Canadian legislation requires warrants for seizure of personal information to be issued by a judge. Commenting on PIPEDA case #313 (*Bank's notification to customers triggers PATRIOT Act concerns)*, the federal Privacy Commisioner states:

> "The risk of personal information being disclosed to government authorities is not a risk unique to U.S. organizations. In the national security and anti-terrorism context, Canadian organizations are subject to similar types of orders to disclose personal information held in Canada to Canadian authorities. Despite the objections of the Office of the Privacy Commissioner, the Personal Information Protection and Electronic Documents Act has been amended since the events of September 11th, 2001, so as to permit organizations to collect and use personal information without consent for the purpose of disclosing this information to government institutions, if the information relates to national security, the defense of Canada or the conduct of international affairs. In addition to these measures, there are longstanding formal bilateral agreements between the U.S. and Canadian government agencies that provide for mutual cooperation and for the exchange of relevant information. These mechanisms are still available." [54]

At a recent symposium on cloud-based email services hosted by Ryerson University, Ontario Privacy Commissioner Dr. Ann Cavoukian stated:

[53] *Frequently Asked Questions*, 2010 http://www.vpit.ualberta.ca/email/index.php?ref=faq#PrivacyShow (December 2010)

[54] *PIPEDA Case Summary #313 (Bank's notification to customers triggers PATRIOT Act concerns)*, 2005 http://www.priv.gc.ca/cf-dc/2005/313_20051019_e.cfm (December 2010)

> “Whether you have the PATRIOT ACT doesn’t matter, there will always be law enforcement techniques that will access certain types of [personal] information. What you should concern yourself with is the kind of accountability that you will be able to maintain if your email system should go into the cloud. … In my book, you can outsource your services but you cannot outsource accountability.”

Appendix D: FIPPA Definition of Personal Information

FIPPA s. 2 defines personal information as follows:

“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,

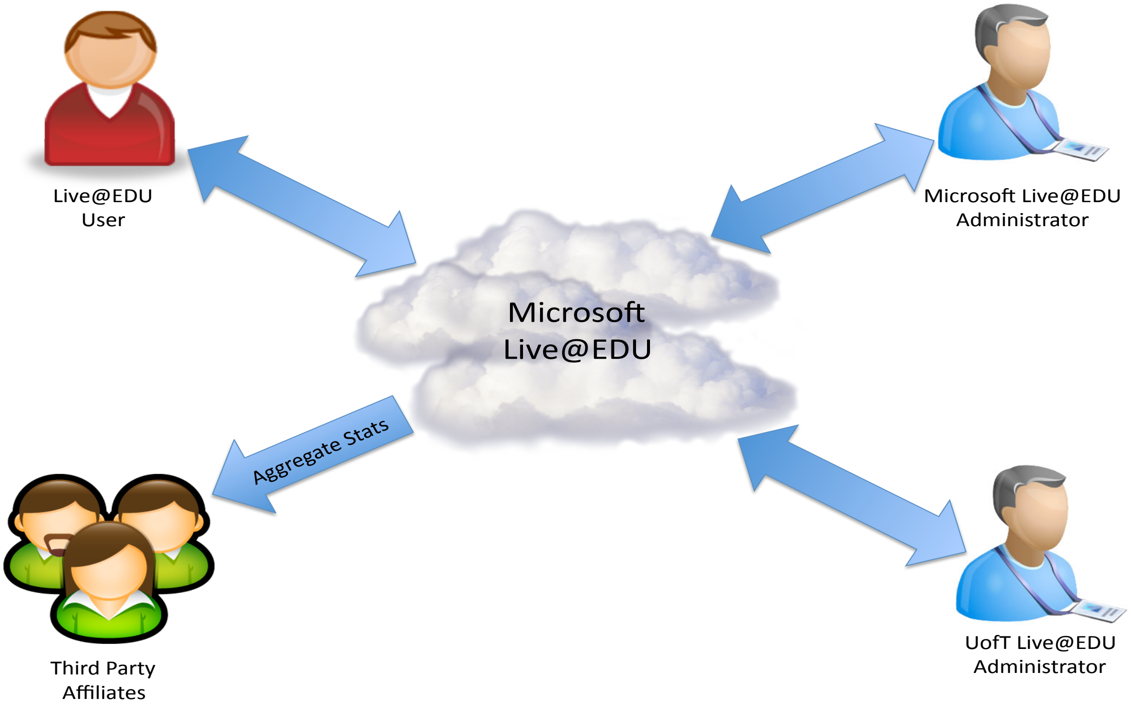
g) the views or opinions of another individual about the individual, and

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”)

Appendix E: Live@edu Dataflows and Processes

Overview

The following diagram is an overview of major parties involved in this service:



Live@edu User

These are the users of the service, currently UofT students, whose personally identifiable information will be stored in the system.

Microsoft *Live@edu* Administrator

These are administrators employed by Microsoft to staff their data centers and provide support for their *Live@edu* platform. From the standard *Live@edu* contract, Microsoft does "not use or allow access to personally identifiable information from education records, other than directory information, except in connection with services to be provided under the Agreement or as the Institution otherwise directs."

UofT *Live@edu* Administrator

These are UofT administrators who will have some access to the *Live@edu* platform. UofT policy governs the access a UofT administrator has into the *Live@edu* system.

Third Party Affiliates

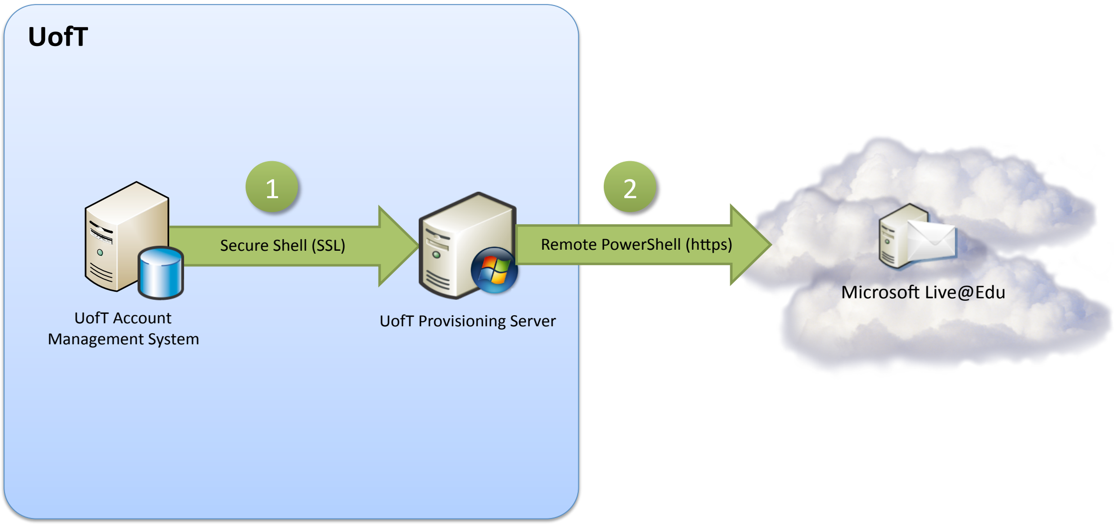
Microsoft has indicated that it may provide aggregate statistics to third party affiliates but ensures that no personally identifiable information will be revealed in this transfer.

Initial Setup

The University of Toronto will offer an opt-out to students who do not wish to use the *Live@edu* service; if a student chooses to use Live@edu, the student does so voluntarily. Those choosing to opt-out will be required to provide an email address where the University can forward all of the student's email communication. Once students have been notified of their option to opt-out and sufficient time has been granted to allow the decision to be made, the University will begin the migration process: moving current email stored on the UTORmail internal servers to the *Live@edu* servers. There are two steps in this process: provisioning and migration.

Provisioning

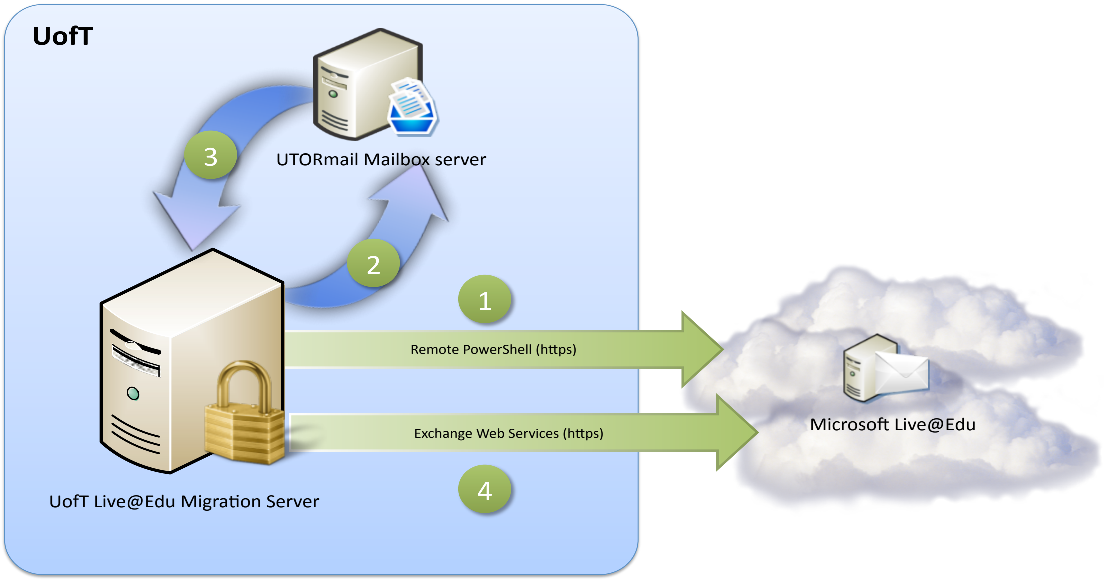
"Provisioning" refers to the process by which an account is created for a user (student) on the *Live@edu* servers. This is a two step process:



1. A secure connection is established from the UofT account management system to the UofT provisioning server by a UofT system administrator. All communication over this channel is encrypted using the SSL protocol.
2. Using Remote Powershell, the UofT admin then establishes a secure connection to the Microsoft *Live@edu* service.
    a. The user's first name, last name, WLID-eppn (UTORid@domain), WLID-uid (a one-way hash of the UTID) and email address are communicated to the Microsoft Live@edu servers during this step
    b. This connection is authenticated with a UofT System Administrator username and password and all communication over this channel is over HTTPS, an internet protocol that is encrypted using the SSL protocol.

Migration to *Live@edu*

Once provisioning is complete, migration user mailbox may begin. This is a four step process:


UofT
UTORmail Mailbox server
3
2
1
Remote PowerShell (https)
Exchange Web Services (https)
4
Microsoft Live@Edu
UofT Live@Edu Migration Server

1. Using Remote Powershell, the UofT Administrator establishes a secure connection from the UofT *Live@edu* Migration server to the Microsoft *Live@edu* service. This connection is authenticated with a UofT System Administrator username and password and all communication over this channel is over HTTPS, an internet protocol that is encrypted using the SSL protocol.
2. A connection is then established with the UTORmail Mailbox server that contains the user's email inbox. This connection uses the SSH protocol which is encrypted with SSL.
3. The user's mailbox is "mounted" on the migration server, giving the migration server access to the contents of the user's email inbox.
4. The user's email is transferred to the *Live@edu* service, into the account that was provisioned for this user.

Once this process is complete, the UofT Administrator will update the mail routing data for the user's email address. This will result in all new and queued messages for that user being processed and delivered to *Live@edu*.

From a privacy perspective, this migration process is well thought out. Students are given the option to opt-out of the service and forward their email elsewhere. All of the connections to the *Live@edu* service are fully encrypted to ensure that communication between UofT and Microsoft is protected from eavesdroppers.

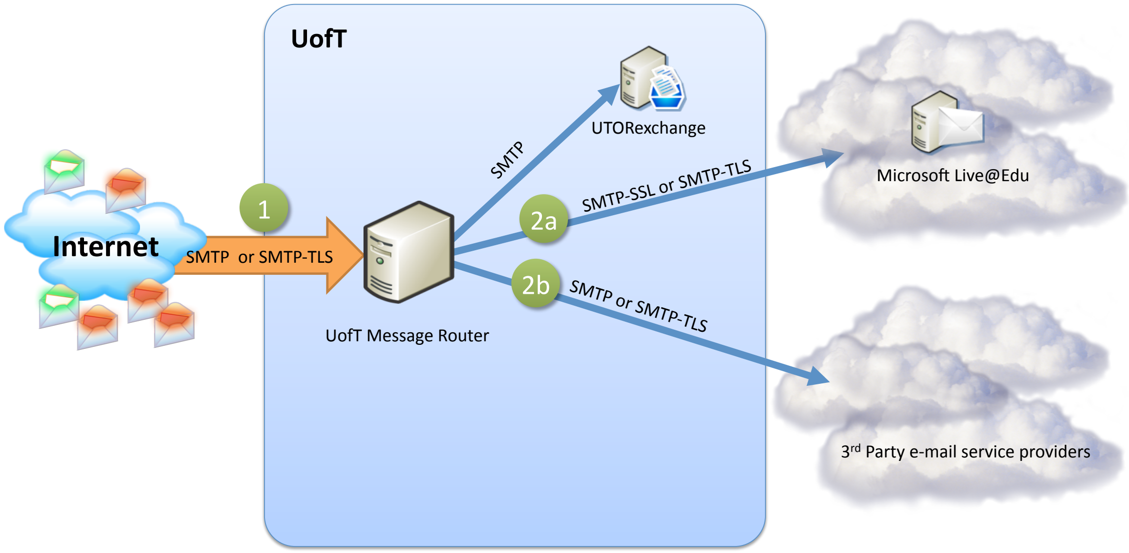
Email Flow

One of the primary sources of personally identifiable information in this service will be email. Microsoft has indicated that they support a protocol extension called "opportunistic SMTP" for encrypting the email flow between *Live@edu* and the users of their service. This means that the University is able to force encryption between UofT mail routers and the *Live@edu* mail servers (this is done by ensuring that the University's mail routing servers will only initiate or accept connections to and from Microsoft that are encrypted). The digital certificates used to implement encryption can also function as a verification of identity (authentication). It should be noted that in the case of email flow, Microsoft uses the certificates primarily to encrypt the data, not provide authentication. In this context the primary concern is encryption, so there is little problem with Microsoft using the technology in this way.

Forefront Online Protection for Exchange

The encryption of mail flowing between the University's mail routers and Microsoft's is provided by a service called Forefront Online Protection for Exchange (FOPE). This service has been tested to be active by the University of Toronto. The functioning of this service is reinforced through firewall rules, managed by the University of Toronto, that block traffic on unencrypted ports, and through the configuration of the UofT Message Router to only accept encrypted traffic, regardless of network port.

Incoming Flow

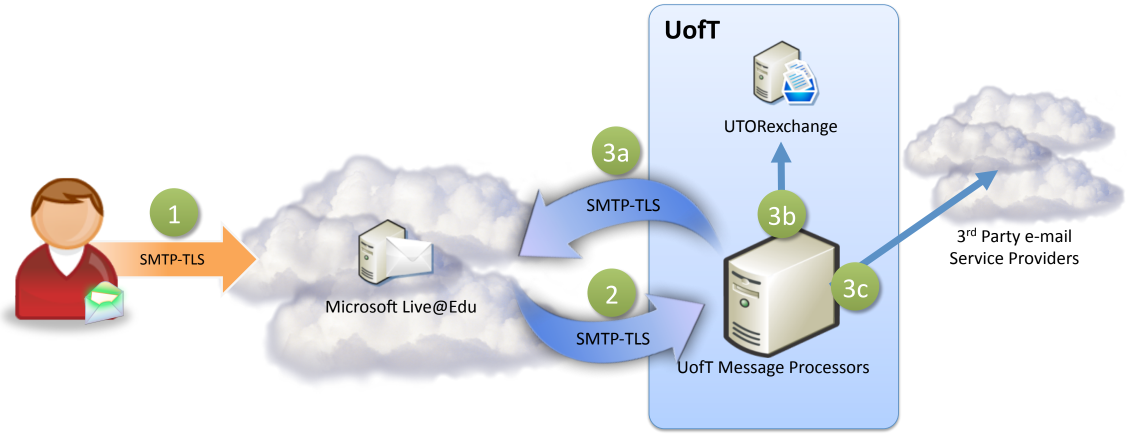


Message routing is handled at UofT

1. Email arrives at the UofT Message Routing Servers from somewhere else in the world. UofT offers "Opportunistic TLS", which means that if the sending email server supports encryption via TLS, the University prefers that method of exchange.
2. On the UofT routing servers a lookup is performed that determines whether a user is using *Live@edu* or whether they have opted-out and forwarded their mail elsewhere. (UTORexchange is included in this diagram only to indicate that staff / faculty email remains within the University and is not forwarded on to an external 3rd party).
    a. If the user uses *Live@edu*, the message is sent to the *Live@edu* servers over a secure channel encrypted with SSL/TLS.
    b. If the user has opted-out, the message is forwarded on to the 3rd party service provider the user has chosen. Here again, UofT is willing to use TLS to encrypt the exchange if the 3rd party agrees, although encryption will not be forced.

Outgoing Email Flow

All Email that leaves a user's account on *Live@edu* will be routed through UofT's message routing servers. Please note that this is based on preliminary information from UofT's implementation team and may change slightly with the final architecture.



Message routing is handled at UofT

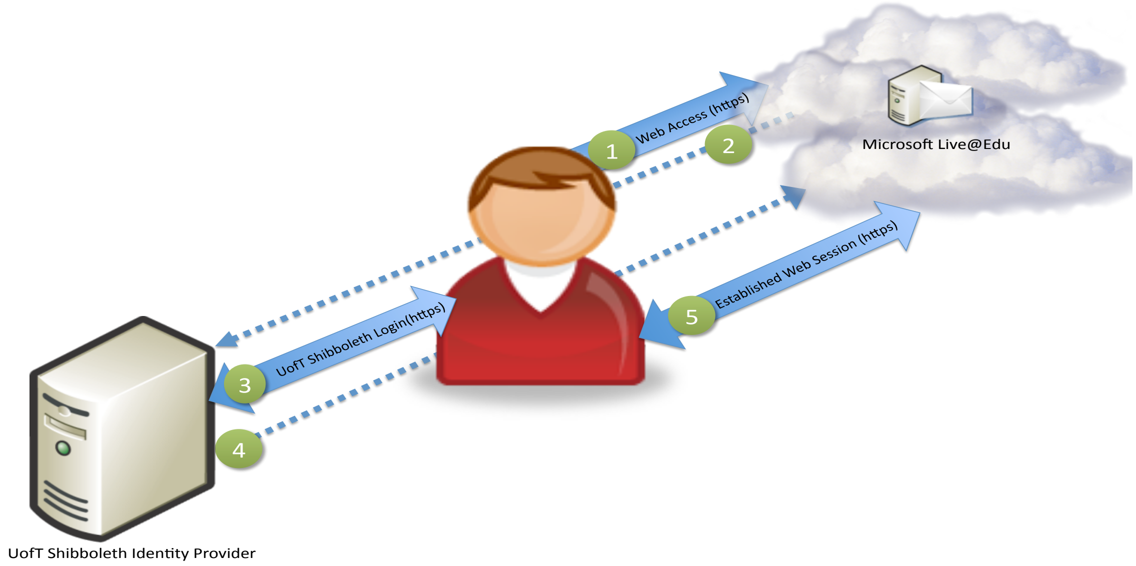
1. A user sends an email through the Microsoft *Live@edu* service.
2. That email is sent securely through an encrypted channel to the UofT Message Processors which will determine where the message is to be delivered.
3. The message will be delivered:
    a. Back to the *Live@edu* service over an encrypted channel if the recipient specified is another UofT *Live@edu* user.
    b. To the UTORexchange servers if the recipient specified is a staff / faculty member of UofT who uses the UTORexchange service.
    c. Otherwise, the message is routed out to the recipient's email provider outside of the UofT.

The assurance that the University can force the encryption of email flowing between UofT and *Live@edu* provides an essential guard to privacy.

Web-Based Access to Live@edu

The University anticipates that the majority of users will access their email through a web-based interface. This is excellent from a privacy perspective because the type of authentication used for web-based services does not send the user's username and password to *Live@edu*. The services included under this authentication method are:

- Outlook Web Access

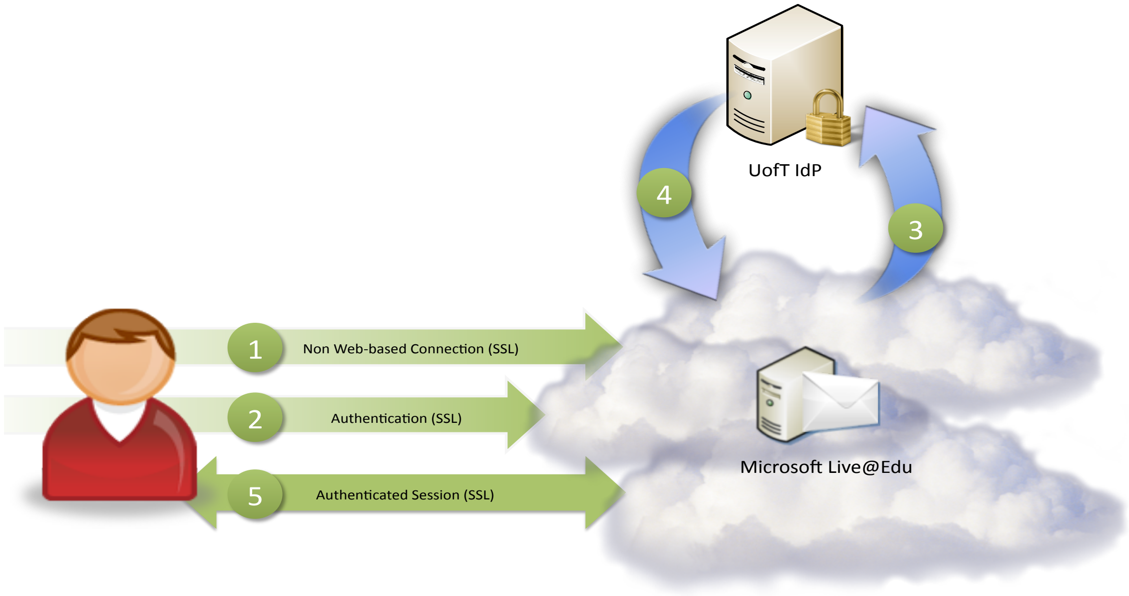

Microsoft Live@Edu
1
Web Access (https)
2
UofT Shibboleth Login(https)
3
4
Established Web Session (https)
5
UofT Shibboleth Identity Provider

1. The user initiates a request to connect to *Live@edu* through a web browser or other web technology. This session is conducted over HTTPS, which is encrypted with SSL/TLS.
2. The *Live@edu* server redirects the user to UofT's Identity Provider (IdP) for authentication.
3. The UofT IdP will present the user with the standard UofT login page into which the user will type their UTORid and password. The UofT login page is encrypted with SSL/TLS.
4. Upon successful login, the UofT IdP server will send the user back to *Live@edu* (over SSL) with an assertion, which includes the following attributes:
   a. User's WLID-eppn (UTORid@domain)
   b. User's WLID-uid (a one way hash of the UTID)
   c. An authentication token that indicates to *Live@edu* that UofT has authenticated the user
5. The user now has an established web-based session with *Live@edu* and begins to use their services. This session is encrypted with SSL/TLS for the entire duration.

Non Web-Based Access to Live@edu

While the University does anticipate that the majority of users will connect to *Live@edu* through web-based technologies, there will undoubtedly be some who use other methods to connect. The authentication procedure is slightly different in this case, as is detailed in the following diagram. The services included under this authentication method are:

- IMAPS, POP3S (Mail receiving protocols)
- SMTP (Mail delivery protocols)
- LDAP, LDAPs
- Outlook Anywhere (RPC/https)
- Exchange Web Services
- ActiveSync



1. A secure connection is established with the *Live@edu* servers, encrypted with SSL/TLS. Authentication is requested by *Live@edu*.
2. User sends their authentication credentials consisting of their username (UTORid) in the form *utorid@mail.utoronto.ca* and their password.
3. *Live@edu* infers from the @mail.utoronto.ca portion of the username the proper Identity Provider (IdP) to contact and sends the username / password pair to the IdP over an encrypted channel.
4. UofT's IdP validates the credentials and responds with an assertion that includes:
   a. User's WLID-eppn (UTORid@domain)
   b. User's WLID-uid (one way hash of the UTID)
   c. An authentication token that indicates to *Live@edu* that UofT has authenticated the user
5. The user can begin to use the *Live@edu* service over their encrypted channel.

It is important to note that in this process Microsoft has assured UofT that no usernames and passwords are ever stored on the *Live@edu* servers. The username and password are only kept temporarily in memory for the purposes of authenticating the user and are then removed.

Backups

Protecting the data in a system includes making sure that it is regularly backed up in case of a failure. Microsoft has provided assurances in the SAS 70 report that data is encrypted before it is backed up, and backup tapes are securely destroyed at the end of their lifecycle.

Termination of Service

When a *Live@edu* user is no longer a student of the University they will no longer have access to *Live@edu*'s services through the University. *Live@edu* does not have access to student enrolment data, and therefore relies on us to terminate service. Prior to terminating service, there must be a way for the student to extract or migrate all of their information from the service. *Live@edu* will hold all the contents of all deleted accounts for 30 days, at which point the information will be disposed of.

Appendix E: Privacy by Design Principles

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**

   We can all be certain of one thing – the default rules! *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.

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.

Appendix F: CSA Privacy Code Principles

1. Accountability
An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

2. Identifying Purposes
The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

3. Consent
The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate.

4. Limiting Collection
The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

5. Limiting Use, Disclosure and Retention
Personal information shall not be used or disclosed for purposes other than those for which it is collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of the stated purposes.

6. Accuracy
Personal information shall be as accurate, complete and up-to-date as is necessary for the purpose for which it is used.

7. Safeguards
Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

8. Openness
An organization shall make specific information about its policies and practices relating to the management of personal information readily available to individuals.

9. Individual Access
Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information, and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. Challenging Compliance
An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

Appendix G: Technology Overview

SSL/TLS

Secure Sockets Layer (SSL) and its successor Transport Layer Security (TLS) provide security for data that is in transit through the use of cryptographic protocols. SSL/TLS provides a vital piece of a privacy-respecting software solution by protecting with encryption all of a user's communications with a remote third-party. A SSL/TLS session is initiated by the two parties (in most cases this is a client and a server) taking part in what is called a "handshake". The essential features of this handshake include:

1. The server and client decide on the strongest form of encryption that both support.
2. The server sends its identification to the client in the form of a digital certificate.
3. The client verifies the validity of the server's certificate by ensuring that the authority that issued it is a trusted third-party (called a certificate authority).
4. The client generates a random number that will be used to encrypt all further communications, encrypts it in a way that only the server can read, and sends this encrypted number to the server.

Once the handshake has been completed as detailed, all further communications between the server and client during the session are securely encrypted with this random number that the two have exchanged. For the purposes of this document when service supporting SSL/TLS is referred to, it is meant that the communications between server and client for that service implement this protocol to ensure all transmissions between them are encrypted and unreadable by anyone else *while in transit*.

Shibboleth

Shibboleth is a framework for the exchange of authentication and authorization information between organizations without the need for either organization to see the usernames or passwords of the other. The protocol underlying Shibboleth is the Security Assertion Markup Language (SAML) which defines how security assertions are made between two organizations that trust one another. This technology provides a key building block in protecting a user's privacy since it does away with the need to transmit such highly personal information as a user's password to an organization outside of the University of Toronto. The Shibboleth technology is mainly used for web-based applications although work is underway to enable it to support "rich" clients like Outlook and Thunderbird as well.

A typical SAML authentication process has a number of steps which are summarized in the diagram below. In this diagram, three parties are referenced:

1. IdP (Identity Provider) - The organization that is providing the authentication credentials; in this case, the University of Toronto
2. SP (Service Provider) - The organization that is providing a service; in this case, Microsoft *Live@edu*.
3. User Agent - This is the user who is accessing *Live@edu* through their web browser.

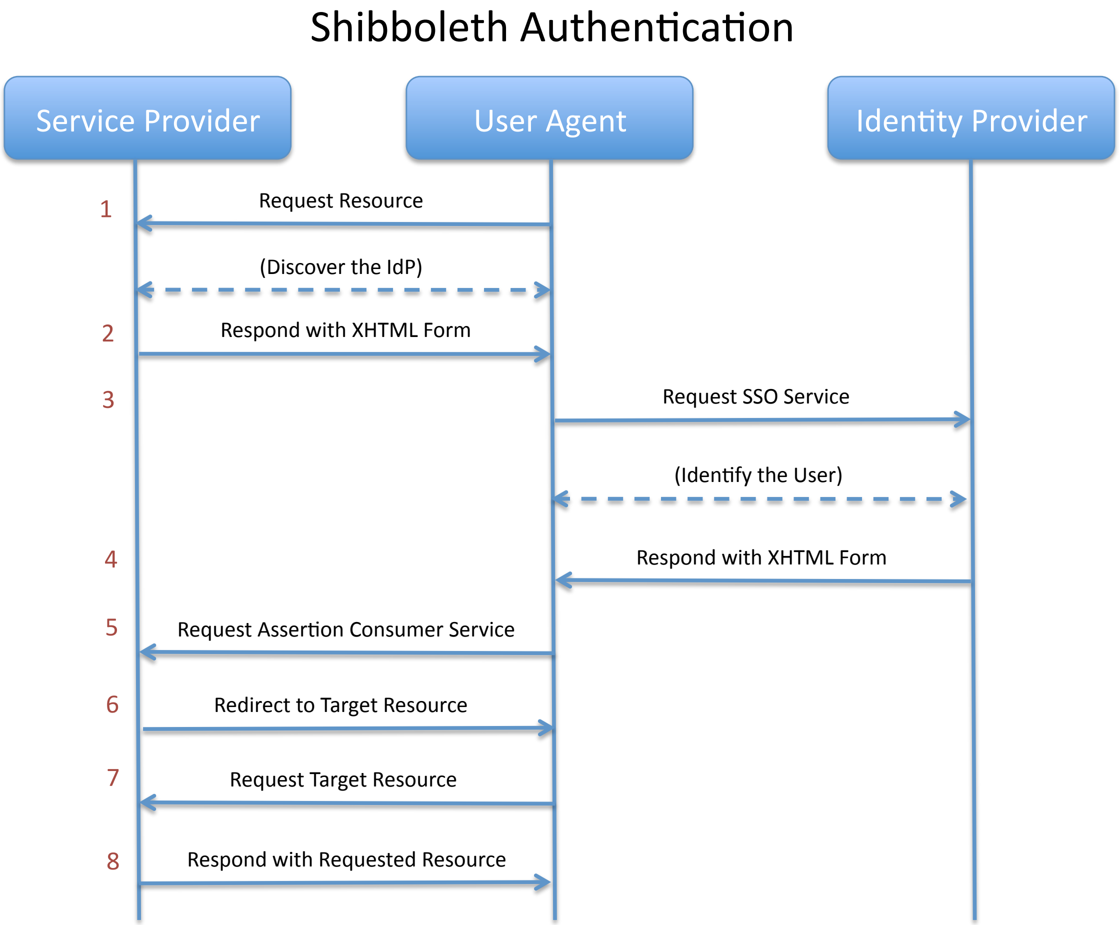


Figure 2: SAML 2.0 Authentication Flow [55]

1. A user accesses a resource hosted by a SP that is protected, requiring authentication.
2. After discovering the user's IdP either through configuration or a WAYF (Where Are You From) screen, the SP responds with an XHTML form specially crafted to bounce the user over to their IdP for authentication.
3. The user issues an authentication request to their IdP, and the user is identified with an appropriate access control mechanism.
4. The IdP passes back a SAML assertion in an XHTML form that is crafted in the form of an "assertion".
5. The user once again requests the assertion service at the SP.
6. The SP processes the request, creates a security context (often referred to as "logging in") and directs the user to the target resource.
7. The user once again requests the target resource.
8. Since the security context has been established, the SP returns the requested resource.

[55] https://secure.wikimedia.org/wikipedia/en/wiki/SAML_2.0

Appendix H: FIPPA Risk Analysis

The following privacy risks apply to all six sections of the FIPPA analysis. These are:

1. Collection, use or disclosure of personal information inconsistent with FIPPA.
2. Individual dissatisfaction with University or Microsoft privacy actions.
3. Privacy complaints to the University, Microsoft or the IPC from individuals dissatisfied with the collection, use or disclosure of their personal information.
4. Harm to the University's reputation.

Risks specific to each section are set out in that section.

Collection

There is a risk that Microsoft or its affiliates could *collect* or *store* user personal information in a manner not authorized by the University. To help alleviate these concerns, Microsoft collects the least possible amount of personal information (it practices data minimization). [56] Microsoft provides security and privacy training to its staff. Despite these assurances, proper notification need be provided to Live@edu users informing them of the personal information that will be disclosed to Microsoft. In addition, since the Live@edu service's privacy policy is expected to change over time, University staff will continue to monitor it to ensure that changes continue to comply with Ontario privacy legislation, and that such changes are communicated to users.

The contract includes statements for protection of personal information in the collection stage:

- [Redacted]

The University Notice of Collection will explain purposes of collection of personal information.

The University is satisfied that Microsoft's conduct, as stated in the Agreement, provides privacy protection of personal information in collection that is equal to or exceeds FIPPA.

Use

There is a risk that Microsoft or its affiliates could *use* the personal information collected by the Live@edu service in a manner not consistent with the intent of the collection. After Microsoft collects information, the University will be unable to confirm how the information is used so all uses use of the information in the Live@edu service must be expressly set out in the contract.

The contract includes the following statements about use of personal information:

- [Redacted]

With these provisions, the University understands Microsoft's conduct to provide privacy protection of personal information in use that is equal to or exceeds FIPPA expectations.

Disclosure

[56] http://go.microsoft.com/?linkid=9746120, page 9

There is a risk that Microsoft or an affiliate could *disclose* personal information collected by Live@edu in a manner not consistent with the intent of the collection. In addition to impacts listed in the introduction to this section, inappropriate disclosure of personal information could lead to identity theft and invasion of privacy. Mitigations to address these concerns include:

- [Redacted]
- A technical analysis of Live@edu security infrastructure was performed based on a SAS70 Type II report and other documents available on the Microsoft website, referenced in the “Resources Consulted” section. The Microsoft security environment was found to be equivalent to or better than that of the University. See the “Privacy by Design” and “Data Flows” sections of this document for more detail. One relevant quote from the SAS70 states: “The Online Services Security Policy establishes the access control requirements for requesting and provisioning user access for accounts and services in the […] environment. The policy requires that access be denied by default, follow least privilege principles, be allocated through role-based controls, and be granted only upon business need. The policy also requires asset owners or associated agents to review the appropriateness of access and privileges on a periodic basis.”

The contract with Microsoft states:

1. [Redacted]

Retention

The University must retain personal information for at least a year after the date of its last use. Student information must also be protected from destruction and kept accurate and up-to-date. Microsoft will maintain user information in its systems in accordance with terms of use agreed to by students. Notice will be provided to the University as follows:

- [Redacted]

It will be the University’s responsibility to retain records for one year consistent with FIPPA.

Disposal

There is a risk that personal information stored in Live@edu could be *disposed* of improperly, leading to a disclosure of personal information.

The Agreement states:

[Redacted]

Security

In addition to security analyses of Live@edu set out elsewhere in this assessment, the agreement states:

- [Redacted]

These clauses provide security assurances consistent with FIPPA requirements.