UNIVERSITY OF TORONTO

Information Risk and Risk Management

Staff and Faculty E-Communications Outsourcing Project

Author(s):	Matt Wilks Axel Johnston Martin Loeffler
Reviewer(s):	Martin Loeffler
Date:	2014/08/07
Version:	2.0.9

Contents

Executive Summary

Opportunity Summary – Office 365

UTORmail, the University's legacy institutional email service, is near end-of-life and requires significant investment to bring up to current industry standards. The University successfully migrated student email to Microsoft Live@edu in 2011, and subsequently to Microsoft Office 365, the successor to Live@edu, in 2013. The University is now considering moving the email services of staff and faculty to the Microsoft Office 365 system.

The suite of tools offered through Office365 represents an improvement to the university status quo in the form of much larger mailbox quotas, calendaring services, Office Web Apps, and SharePoint Online Collaboration.

The objective of the proposed project is to migrate faculty and staff e-communications to Microsoft Office 365.

Risk Summary

The following table identifies the risk categories assessed, and identifies if they exceed, meet or do not meet current University of Toronto practices and / or performance expectations given the sensitivity of the information handled, threats associated with that data, and known vulnerabilities in the technology or environments through which that information passes.

This assessment may change with the introduction of new information in subsequent stages of the project..

Category	Assessment	Remediable
Privacy Impact Assessment		
Privacy By Design Guidelines	Meets	NA
Threat / Risk Assessment		
Access Controls	Does not meet	Yes [*]
Change Controls	Exceeds	NA
Business Continuity Practices	Exceeds	NA
Access, Change, and Fault Reporting	Meets	NA

[*] Please see ***Appendix N: Encryption Solutions***.

The remainder of this Information Risk & Risk Management document expands on the risk profile of, and risk mitigation recommendations for, the project in progressively greater detail.

Introduction

This Risk Management Document

An IRRM (Information Risk and Risk Management) document articulates threat, risk, and privacy considerations for a given opportunity under consideration by the University, evaluated against the regulatory, contractual, and aspirational contexts in which the University operates.

This IRRM includes a Privacy Impact Assessment (PIA) and the Threat / Risk Assessment (TRA) for the Office 365 service being proposed by the project.

A Privacy Impact Assessment (PIA) is a process for assessing, documenting and addressing privacy risk in the development, implementation and operation of projects that 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 describes and evaluates privacy risks as a project progresses, helping decision makers understand and address those risks as they become evident.

A Threat / Risk Assessment (TRA) is a process for assessing, documenting and addressing risk to information assets and recommends risk mitigation measures that can, if implemented, lower the risks to acceptable levels. Threats and risks are articulated in relation to how sensitive or valuable the information is, and what vulnerabilities are inherent in the environments through which the information passes, is stored, or is used.

In deciding whether to proceed or not, University decision makers must decide to accept or reject the residual risks identified by the PIA and TRA processes. (See Summary of Residual Risks Chart on page 44)

While the IRRM document is a 'living' document – that is, updated as understanding and contexts evolve – owing to potentially long update cycles it may not reflect the latest information on rapidly-evolving circumstances. Likewise, the IRRM document presents a narrow, but deep, risk management-focussed perspective on the risk of adopting a given solution, or not; a fully articulated and nuanced discussion of all possible options to approaching an opportunity is beyond the scope and purpose of the IRRM document.

Opportunity and Cost

An opportunity has the potential to bring value to the University – often recognized as a solution that brings cost savings, time savings, improved facility, or a combination of the three. However, solutions are not guaranteed to be successful, and often require significant investments of time, money, and effort before value is realized – if at all. That said, the University's experience with providing Office 365 for student use has shown the value, utility, and security of the solution – advantages that would accrue to staff and faculty, were Office 365 made available to them. In pursuit of alternatives, no free or acceptably low-cost alternatives were identified that resided solely within Canada.

Beyond the up-front investment required to pursue an opportunity, there may be hidden costs – identified as risks – associated with the pursuit and / or adoption of a solution. The IRRM document attempts to identify these risks (articulated as potential shortcomings in desired levels of security and privacy – please see Appendices A, C, D, F, and G), and to offer alternatives that may mitigate those risks while maintaining the attractiveness of the proposed solution.

The Measure of Risk

The University operates in a web of contextual elements: legal requirements, contractual obligations, and aspirational interests. The larger the opportunity-realizing solution, the more likely that there will be conflicts between one or more of these contextual elements.

The IRRM document attempts to identify and articulate the assets affected by a possible solution, and enumerate their characteristics – their sensitivity, where they reside, how they are used – and apply the expectations of each contextual element to the elements of that enumeration, identifying how the proposed solution meets those expectations, or not.

Information Risk & Risk Management

Project Description

Reports from I+TS staff demonstrated 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. As a result, the University migrated the student email system to Live@edu hosted by Microsoft, and upgraded to Office 365, the successor to Live@edu, in October 2013. In light of these successful migrations, the University is considering moving the email services of staff and faculty to the Office 365 platform, the successor to Live@edu. Staff and faculty are currently using UTORmail (email only) or UTORExchange (email and calendaring), and in some cases, locally managed systems for their e-communications platform. The suite of tools offered through Office 365 represents an improvement to the university status quo in the form of ubiquitous calendaring, and much larger inbox quotas. Other features under consideration include Office Web Apps, and SharePoint Online Collaboration.

This project represents a major shift in the way that the University provides its email service to staff and faculty. Staff and faculty email will be stored off-campus in data centers that are not located in Canada, raising the issue of applicability of foreign legislation over, and surveillance of, this data and loss of local control. The potential use of new document collaboration tools may also result in confidential data being stored in off-campus data centers. The University recognizes that beyond itself and its commercial partners exist external governmental agencies – both within and external to Canada – whose mandate is to surveil electronic communications, and with whom the University has no means of negotiating terms, conditions, or any sort of standard of notice or behaviour. This reality brings requirements for the University to take active steps to protect the confidentiality of sensitive information communicated via email. With this shift away from internally managed email / document collaboration comes the need to establish a level of trust with Microsoft appropriate to the sensitivity of the personal and confidential information that will be stored in email and the other tools offered. Although Microsoft ensures the security and privacy of information on its systems, the University would oversee the continuing protection of private and confidential information in this process.

Purpose of This Document

The **Information Risk and Risk Management** document details how information is, or is proposed to be used by a project; the sensitivity of that information; the University's obligations to protect that information; threats and vulnerabilities which create risk of misuse of that information; and options to manage risk to enable the University to meet those obligations if unacceptable unmanaged risks exist. The two tools that the IRRM uses to achieve these ends are the Privacy Impact Assessment (PIA) and the Threat / Risk Assessment (TRA). As both of these tools deal with risk to information, there is some overlap in content, however the focus of each is distinct and different: The PIA is primarily concerned with the anticipated uses of information and the intentions of service designers in support of maintaining the privacy of personally identifiable information; the TRA, a more technical document, is primarily concerned with identifying vulnerabilities in proposed systems and services, and how those vulnerabilities may be mitigated to create a more secure operational environment for all information within it. Further details of how the PIA and the TRA achieve their ends are detailed below.

What is a Privacy Impact Assessment?

A **Privacy Impact Assessment** (PIA) is a process for determining and addressing privacy risk during the development, implementation and post-completion operation of services that involve or affect personal information. A PIA is a living document that develops with the service 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, are 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 has structured its PIA on the **Privacy by Design** (PbD) principles (please see Appendix I) 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 (please see Appendix B). 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 regulated under the Ontario **Freedom of Information and Protection of Privacy Act** (FIPPA) legislation. 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;
- 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 FIPPA requirements.

What is a Threat / Risk Assessment?

A **Threat / Risk Assessment** (TRA) is a process for determining the risk to assets, based on the value of those assets, threats that may cause the assets to be destroyed, or inappropriately divulged, accessed or modified. The TRA also attempts to inform choices for risk mitigation during the development, implementation and post-completion operation of services that involve or affect information or information handling / storage / administration infrastructure.

As with a PIA, a TRA is a living document that develops with the service project, aligning with project milestones and decision points. A TRA contains an enumeration of information assets, their sensitivity, and details how controls are applied to that information throughout its lifecycle. The TRA will indicate the level of risk exposure at each stage of the information lifecycle, and whether this level of risk meets, exceeds, or is on par with currently accepted risk for information of similar sensitivity in similar contexts.

The TRA will identify:

1. Data within the scope of the TRA;
2. Data sensitivity to:
    a. Risk of disclosure, alteration, loss, and unrecorded use or repudiation of receipt;
    b. Agents or events that could cause such undesired outcomes to be realized; and
    c. Vulnerabilities that would enable threats to have an impact.
3. Risk mitigation strategies that address specific vulnerabilities.

This analysis also encompasses all of the above for supporting access, change, continuity, and accountability control systems.

Privacy Impact Assessment

PIA Summary

Microsoft has 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 staff and faculty e-communications.

PIA Analysis

The University is regulated under FIPPA legislation. 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 would 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 staff / faculty e-communications;
- All information created or maintained through this project remains accessible to the University for proper institutional purposes; and
- The contract signed with the external provider meets or exceeds the requirements of applicable legislation (FIPPA).

This PIA comprises a description of the staff and faculty 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.

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 staff and faculty 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 Office 365 contract with Microsoft.

The University recognizes that beyond itself and its commercial partners exist external governmental agencies – both within and external to Canada – whose mandate is to surveil electronic communications; agencies with whom the University is not in a position to negotiate practice, but whose influence on the

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

privacy of University information is acknowledged. To this end, the University recognizes its obligation to manage the risk to confidentially of confidential / FIPPA info presented by these external agencies.

Other Universities

In addition to key stakeholder input, experiences of universities that outsourced email services were examined. Universities and colleges worldwide have outsourced email services, including several in Canada, such as the 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.

University of Alberta

U of A outsourced student, faculty and staff email to Google's *Apps for Education* platform in March 2011. 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 that 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.

Ryerson University

Ryerson University began a transition from internal legacy systems to Google Apps for Education in 2012. Migration of faculty email was made optional, and continues to be so. By October 2012, 58% had migrated their email to Google, and by September 2013 that number had risen to 83%. All administrative staff were required to migrate except for counselors and others that might handle sensitive student information. Numerous academic and administrative departments are now using Google Forms to conduct university business.

Dalhousie University

Dalhousie selected Office 365 for their entire community. Their implementation is approximately 80% complete. The rollout started with staff, then went to students in August 2013, and is now working on the migration of faculty members to the new environment. The last group to be implemented will be alumni.

Queens University

Queens conducted an extensive privacy and security review of Office 365. By September 2013, students had been migrated into the new service. Further work is being performed on the viability of migrating faculty and staff into the services.

Lakehead University

Lakehead University 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

[2] http://www.edmontonjournal.com/technology/inks+Gmail+deal+with+Google/3949065/story.html

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].

Provisioning Alumni

For a number of years, the Division of University Advancement has offered alumni accounts in partnership with Google. They report:

1. Alumni experience has been good. Alumni respond well to the offer.
2. Approximately 23,000 active accounts have been provisioned.
3. Of affinity services, Google Mail is most popular, helping drive alumni to other offerings and communities.
4. With the implementation of the Microsoft-based UTMail+ service for current students, graduating students have been provided with an alum.utoronto.ca account in UTmail+. Planning is underway to provide the Office 365 services to those alumni who graduated prior to the adoption of the UTMail+ service.

Please see Appendix Q for a listing of Canadian and American comparator universities, and some others, that offer faculty and staff e-communications services in the cloud.

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)

[3] http://www.canlii.org/en/on/onla/doc/2009/2009canlii24632/2009canlii24632.pdf
[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

- *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)

[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-CTZ 3-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

Threat / Risk Assessment

TRA Summary

The security – both physical and logical – applied by Microsoft provides risk mitigation every bit as good as, and in many ways better, than what currently is provided by the University of Toronto to any of the University's many email systems; that said, the University acknowledges the reality of external governmental access, both with and without notice (see ***Appendix A: Governmental Surveillance***). As such, a decision to proceed to out-source the provision of email services to Office 365, would accrue a net security benefit to the University, with an investment of time and effort considerably less than that required for the University to provide the same benefit in-house. That said, there are a number of observations that came out of the process of considering the Office 365 service for faculty and staff:

1. Based on the University's Live@edu implementation for students and alumni, it is clear that the business relationship is key, and that near-constant contact was required to ensure that matters of service implementation were successfully resolved to the University's satisfaction. The University must be prepared to sustain this level of collaborative effort, as the greatest potential of the Office 365 suite would likely come in a second phase of implementation, and would not be realized without appropriate effort.

2. While the University of Toronto engages in internal security, vulnerability testing, and does respond to information security incidents in a timely manner, it is recommended that the University develop regular, formalized, network and IT service vulnerability scanning and Computer Security Incident Response (CSIRT) practices in support of our obligations as customers of Office365. So doing would bring the University's practices more in line with that of current best practice.

3. The University should consider maintaining a core of knowledge about the management and provision of email services, should the University ever decide that re-insourcing emails services is an attractive option.

4. The impact of allegations in the media that Internet traffic, even encrypted Internet traffic, is not secure in the context of a threat from nation-state level resources has been evaluated in this assessment. While these risks have existed for many years, their increased attention of late raises the question of whether this is an increase in risk, or an identification of an impact that has always existed but not been uniformly recognized. Network traffic, once it leaves the University's physical network, has never been considered to be a secure form of communication; as such, the security of information outside of the University's networks cannot be decreased. In addition, the nature of work done at the University is often performed over remote networks, and / or in collaboration with individuals at other institutions – even if systems physically located on the University network are a common nexus point. As such, given the already highly distributed nature of our work that is dependent on non-University of Toronto networks, the use of an outsourced network service provider presents only marginal new exposure to risk.

   By way of demonstration, On Thursday 17 October 2013, UTORmail and UTORExchange handled 1.441 million emails, not counting spam filtered out before delivery. Of messages being sent, 87.5% were delivered to recipients outside UTORmail and UTORExchange and 12.5% inside. Of messages being received, 92.9% originated from outside, and 8.1% came from within these internal systems.

Again to demonstrate, over the last year, 91% of the faculty and staff using UTORmail and UTORExchange accessed their email from outside the university's secure network (e.g., they used cellphones, home and hotel services, etc. to connect), exposing their data to the general risks of the wide internet.

5. While not a risk associated with the proposed solution, an additional risk has been identified in existing practice within the University: when faculty and staff enter personal agreements with cloud service suppliers and conduct university academic and administrative business, in the event of an incident, liability still rests with the University. Staff and faculty are individually unable to negotiate a contract as favourable to the protection of privacy and information as the University as a whole is able to do.

TRA Analysis

Threat / Risk Assessment Questionnaire

The project is evaluated against a standard questionnaire. Not every section (Software / Hardware / Outsourced and Contracted services) will be appropriate for all projects – only complete the appropriate sections.

Software to be installed on University of Toronto premises.

Not applicable

Networked Hardware / Appliances – to be installed on University of Toronto premises.

Not applicable

Outsource ('Cloud') Services – outside of University premises

Identification and Authentication

1.1.1. Is the solution SAML 2.0 compliant (i.e. will it work with Shibboleth federated access control software) for the purpose of authenticating users?

- ➢ Office 365 will authenticate via Microsoft Active Directory Federation Services which is SAML 2.0 compliant.

Authorization

1.1.2. What degree of granularity does the solution offer in defining roles?

- ➢ Office 365 provides for a great degree of granularity in defining roles and assigning permissions.

Isolation

1.1.3. What security standards are followed in the operation of the service?

- Office 365 facilities and services are protected as detailed in Microsoft's internal security standard, which meet or surpass the University of Toronto's security standards. Compliance with these internal standards are verified by an annual SAS70-II audit, however the standard itself is protected by NDA ("Non-Disclosure Agreement") and cannot be published but the University. Attestations made in Microsoft's internal security standard were verified by a physical inspection of the Microsoft Chicago data centre.

1.1.4. Is compliance with internal security standards assessed via a SAS 70 Type II or a CSAE 3416 (formerly CICA 5970) compliance audit, at least annually?

- Yes. SAS 70 Type II.

1.1.5. What external application vulnerability scans / assessments / audits are done? How often?

- Microsoft routinely has Penetration testing performed by internal and external parties.

1.1.6. Does data transit non-Canadian networks? If so, where?

- Yes. The United States of America.

1.1.7. Is data stored outside of Canadian borders? If so, where?

- Yes. The United States of America.

Continuity

1.1.8. What level of availability does the service offer?

- Both Office 365 and University of Toronto services are robust and redundant in design, however, are subject to potential service outages from intervening network service providers – this is an exposure that all users of the Internet are vulnerable to, given the shared nature of the Internet.

1.1.9. What provisions are in place to exit the service?

- The University of Toronto has exit options available to it, should an Office 365 service prove unsatisfactory for whatever reason, such that user data can be fully recovered and migrated to another service provider, or back under the direct administration of the University if so desired.

1.1.10. What provisions are in place to protect intellectual property?

- Routine back up of data, and all back ups are encrypted and secured to the same standards as production data.

1.1.11. What provisions exist for decryption key escrow, for encrypted solutions?

- Key Escrow has been identified as a requirement of locally-managed encryption solutions.

Reporting

1.1.12. What activity and resource usage reports are provided?

- The University of Toronto keeps a log of all successful user authentications.
- The University of Toronto keeps a log of all successful authentications by administrative users.
- Activity within the Office 365 service may be monitored through PowerShell scripts.

Functionality

1.1.13. Does the solution follow web standards, such as "REpresentational State Transfer" (REST), or Open Web Application Security Project (OWASP)?

- Yes.

1.1.14. If handling credit card data, is the solution PCI-DSS compliant?

- Credit card data is not handled.

1.1.15. What other, auditable, IT standards are followed (such as operational or security standards)? How often are the audits performed?

- Office 365 facilities and services are protected as detailed in Microsoft's internal security standard, which meet or surpass the University of Toronto's security standards. Compliance with these internal standards are verified by annual SAS70-II audit, however the standard itself is protected by NDA ("Non-Disclosure Agreement") and cannot be published by the University. Attestations made in Microsoft's internal security standard were verified by a physical inspection of the Microsoft Chicago data centre.

1.1.16. Are the annual results of audits and certifications made available to customers?

- Yes.

Professional Services

Not applicable.

Development Services

Not applicable

IRRM Recommendations and Associated Costs

Privacy Recommendations

a. *Proactive not Reactive; Preventative not Remedial*

No recommendations.

b. *Privacy as the Default Setting*

No recommendations.

c. *Privacy Embedded into Design*

Encryption of email contents and attachments of FIPPA/Confidential in-scope information recommended; see Information Security recommendation for Access Controls and ***Appendix N: Encryption Solutions***.

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

No recommendations.

e. *End-to-End Security – Full Lifecycle Protection*

No recommendations.

f. *Respect for User Privacy – Keep it User-Centric*

No recommendations.

Information Security Recommendations

a. *Access Controls*

Recommended that a university of Toronto-managed encryption solution / tool be available to protect FIPPA / Confidential info; see ***Appendix N: Encryption Solutions***.

b. *Change Controls*

No recommendations.

c. *Business Continuity Practices*

No recommendations.

d. *Access, Change, and Fault Reporting*

No recommendations.

Cost Summary

Ref	Recommendation	Cost	Benefit
Access Controls	A University-managed encryption solution for email contents and attachments. See: ***Appendix N: Encryption Solutions***.	TBD	Provide in-Canada, in-University managed access controls to mitigate risk of extra-territorial surveillance of email contents.

Appendix A: Governmental Surveillance

Developing Threats

It has been alleged since 1943 that the United States, in partnership with the five signatory states of the 'UKUSA Security Agreement' (Australia, Canada, New Zealand, the United Kingdom and the United States – collectively known as the 'Five Eyes') engages in wholesale interception, storage and analysis of telecommunications traffic (this activity is referred to as 'SIGINT' or 'Signals Intelligence'). The system, which captures and records analog voice communications, is referred to in the media as 'ECHELON'; since 2006 [Electronic Frontier Foundation (2006)] concerns have been raised that this SIGINT effort has been expanded to include Internet traffic.

Network traffic that passes between two geographically proximate locations within Canada is likely, through the effect of network routing weights set by long-distance network carriers, to pass through the United States (a phenomenon called 'Boomerang Routing' [Clement, et al. (2010)]). This effect, in conjunction with evidence of warrantless network wiretapping presented by Mark Klein (Electronic Frontier Foundation (2006)], indicates that the United States, through the infrastructure installed and maintained by their National Security Agency (NSA), is intercepting all network traffic passing through the United States' physical boundaries through a program called 'Upstream'. In addition, the NSA, through its 'PRISM' program, is alleged to be copying data directly from major cloud service providers, such as Microsoft, Google, Apple, and Yahoo, although all service providers named deny wholesale access to user data.

The fact that CSEC (the Canadian version of the NSA) is constitutionally prohibited from spying on Canadians has been identified by some as a risk mitigation to the threat of pervasive spying while within Canadian geographic boundaries. This may be true in principle, but in practice the current Canadian government does not view the capture of metadata to be in violation of this prohibition ("CSEC exoneration a 'mockery of public accountability'": http://www.cbc.ca/news/canada/csec-exoneration-a-mockery-of-public-accountability-1.2536561). While the authors this report may wish that this was not so, and hope that it will not be so in future, it is beyond the scope of this report to comment on legal cases, constitutional challenges, and governmental policy change yet to come.

Allegations have been made [Greenwald, G. (July 2013)] that the NSA is keeping archives of all intercepted network traffic at the NSA's datacenter in Utah. Also alleged is that the NSA has the wherewithal to break encrypted communications [Whittaker, et al. (2013)]. If it's reasonable to accept the first allegation of pervasive, persistent data capture, it's reasonable to accept the second, for what value is a vast trove of unreadable data? This allegation parallels other allegations that the NSA has compromised the encryption standards development process through their close proximity to NIST (the American National Institute of Standards and Technology)[Perloth, N. et al. (2013)], and CSEC (the Communications Security Establishment Canada) [Geist(2013)], and has compromised random number generator libraries, that form the mathematical core of encryption algorithms to make them more predictable / easier to break [Perloth, N. (2013)]]. Noted information security expert Bruce Schneier believes, after having unrestricted access to Edward Snowden's documents, that the NSA has been able to undermine fundamentals of current encryption solutions [Schneier (2013)]. More recently, NIST had commissioned an external report to asses the quality of its encryption standards. This report found concerning over-involvement of the NSA in NIST's encryption standards development process and recommended, in part, that:

> *"In the standards development process, cryptographers identified two security issues with [NSA-supplied cryptographic designs] : 1) the possibility of a backdoor in the algorithm based on the specific parameters, and 2) a statistical bias in the output of the [designs] (e.g., like a weighted die)."*
>
> [NIST (2014)]

And issued the following recommendation:

"The CoV individual reports point out several shortcomings and procedural weaknesses that led to the inclusion of [NSA-developed algorithms] and propose several steps to remedy them."
[NIST (2014)]

The University of Toronto is a player on the academic world stage – much of our work is done in collaboration with our partners at other institutions, worldwide. Data that travels between mail servers is typically not encrypted, and, if the above allegations are correct, that email is likely captured and stored as soon as it leaves our physical network. Even if the content of the email is encrypted, the metadata (see Appendix O) associated with the email (sender, recipient, date and time of sending, etc.) is not and cannot be encrypted as this would make it impossible for the email to reach its intended recipient. As well, every time email is read from outside of the University of Toronto's physical network – via smart phone, tablet device, laptop or home PC, regardless of encryption – that data is also likely subject to capture by the NSA. As such, an email system may be hosted entirely within the physical network of the University of Toronto, but its contents range far and wide over the Internet in the normal course of providing service – and are subsequently subject to surveillance. Therefore, the physical location of the email service does not afford substantial risk mitigation from the threat of surveillance by governments within the 'Five Eyes' group of countries.

Of course, this is not an exhaustive articulation of ways in which governments may surveil digital communications, nor is it even the most likely – even if the University were to perform background checks on administrative and technical staff, and to secure national security clearance for them, there still exists the possibility that, offered sufficient inducement, an individual with access to the email system could act as a conduit for its unauthorized disclosure in bulk, on an ongoing basis, to government agencies. While it is expected that data that remains within the University's physical network is not subject to surveillance by CSEC or the NSA, as Edward Snowden has shown, even individuals who have passed extensive background checks, and who hold high security clearance, can divulge sensitive information without authorization. In addition, as CSEC may conduct surveillance of Canadian network traffic on behalf of the Canadian Government [Brown, J. (2013)], it would be appropriate to consider the surveillance that the Canadian government conducts within its own borders, and how it shares that information with its Five Eyes partners. This TRA is not intended to be an exhaustive evaluation of all threats and risks to which our email service is currently exposed, but rather those threats and risks which may offer a delta between current state and the proposed new state of moving email services to an outsource service provider.

To mitigate external risks, ITS/ISEA is developing a solution to provide email encryption that would be wholly managed by the University of Toronto for its users. This solution would be in the form of Microsoft Certificate Authority, or PGP ("Pretty Good Privacy") enterprise service, plus GPG ("Gnu Privacy Guard") for non-UT mail recipients. This solution, while meeting the FIPPA 'gold standard' of providing effective encryption of sensitive data, may still be subject to the vulnerabilities in service administration, encryption algorithms, or random number generation that are alleged to beset encrypted communications outside of the University of Toronto network as detailed above.

Given the current awareness of governmental surveillance, the University should take care to articulate its risk rationale and educate users about how to minimize risk when communicating sensitive information, if the University chooses to store its data outside of its physical network – particularly in the United States.

References:

Brown, J. "Wanted: A Canadian Edward Snowden". August 26, 2013. Maclean's Magazine; retrieved from: http://www2.macleans.ca/2013/08/26/wanted-a-canadian-edward-snowden/

Clement, A., Paterson, N., Philips, D. 'IXmaps: Interactively mapping NSA surveillance points in the internet "cloud" '. June 30, 2010. Faculty of Information, University of Toronto

Watson, G. "*CSEC exoneration a 'mockery of public accountability*". Feb 14, 2014. CBC. Retrieved from: http://www.cbc.ca/news/canada/csec-exoneration-a-mockery-of-public-accountability-1.2536561 March, 2014.

Diebert, R. "To protect Canadians' privacy, telcos must shut the 'back door'". September 16, 2013. The Globe and Mail; retrieved from: http://www.theglobeandmail.com/commentary/to-protect-canadians-privacy-telcos-must-shut-the-backdoor/article14333544/

Electronic Frontier Foundation. 'Declaration of Mark Klein in support of plaintiffs' motion for preliminary injunction'. June 8, 2006. United States District Court, Northern District of California. Retrieved from: https://www.eff.org/sites/default/files/filenode/att/Mark%20Klein%20Unredacted%20Decl-Including%20Exhibits.PDF

Geist, M. "Canada Facilitated NSA's Efforts To Weaken Encryption Standards". September 11, 2013; retrieved from: http://www.michaelgeist.ca/content/view/6951/196/

Greenwald, G., "The crux of the NSA story in one phrase: 'collect it all'". July 15, 2013. Retrieved from: http://www.theguardian.com/commentisfree/2013/jul/15/crux-nsa-collect-it-all

Greenwald, G., "NSA Prism program taps in to user data of Apple, Google, and others". June 7, 2013. Retrieved from: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

NIST., NIST Cryptographic Standards and Guidelines Development Process: "*Report and Recommendations of the Visiting Committee on Advanced Technology of the National Institute of Standards and Technology*". July 2014; retrieved from: http://www.nist.gov/public_affairs/releases/upload/VCAT-Report-on-NIST-Cryptographic-Standards-and-Guidelines-Process.pdf

Perloth, N. "Government Announces Steps to Restore Confidence on Encryption Standards". New York Times, September 10, 2013; retrieved from: http://bits.blogs.nytimes.com/2013/09/10/government-announces-steps-to-restore-confidence-on-encryption-standards/

Perloth, N., Larson, J., Shane, S. "N.S.A. Able to Foil Basic Safeguards of Privacy on Web". New York Times, September 5, 2013; retrieved from: http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=all

Risen. J., Lichtblau, E. "Bush Lets U.S. Spy on Callers Without Courts". 16 December, 2005. New York Times, New York.

Schneier, B. "Did NSA Put a Secret Backdoor in New Encryption Standard?". November 15, 2007. Retrieved from: https://www.schneier.com/essay-198.html

Schneier, B. "The NSA Is Breaking Most Encryption on the Internet". September 5, 2013. Retrieved from: https://www.schneier.com/blog/archives/2013/09/the_nsa_is_brea.html#c1675929

Whittaker, et al. "PRISM: Here's how the NSA wiretapped the Internet". June 8, 2013. Retrieved from: http://www.zdnet.com/prism-heres-how-the-nsa-wiretapped-the-internet_p2-7000016565/

Appendix B: Privacy by Design Analysis

Given the nature of cloud computing, the University should 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 may replace.

There exist governmental agencies in both Canada and the United States that exercise a legal right within their jurisdictions to surveil network communications. Beyond the control of the University or its partners, the impact of this surveillance on privacy must be acknowledged. While these risks have existed for many years, they have received increased attention of late which raises the question of whether this is an increase in risk, or an identification of an impact that has always existed but not uniformly recognized.

Privacy by Design Summary

Former 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 I: Privacy by Design Principles***, 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 speech in 2010 at the University of Washington, former 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]

In 2000, Microsoft established a Corporate Privacy Group and appointed Richard Purcell as senior director of privacy, which was the first appointment of a chief privacy officer by a multinational company. Microsoft has articulates its commitment to Privacy by Design on the Microsoft Privacy website (http://www.microsoft.com/privacy/bydesign.aspx), which is comprised of people, processes, technologies, features and research intended to secure infrastructure and client data. All new Microsoft employees receive privacy training. Microsoft's central privacy team develops and implements programs for every aspect of their ecosystem, from products, services and processes through physical systems and infrastructure.

The "Microsoft Privacy Standard for Development" governs the development and deployment of Microsoft consumer products, enterprise products, and Web services. It is incorporated into their baseline development guidelines known as Security Development Lifecycle (SDL) with the objective of ensuring that Privacy is built in to all services from the beginning. 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 digital privacy technology 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."[17]

[16] http://www.microsoft.com/presspass/exec/steve/2010/03-04Cloud.mspx
[17] 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[18]. 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[19] such as asset management, physical and logical access controls, change management, and security surveillance to attempt 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 not to 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 6 phase incident response process including training, identification, containment, mitigation, recovery and analysis of lessons learned.

University of Toronto

The University is undertaking this PIA to anticipate and prevent privacy issues before they happen. Prior to the expected implementation date a working group will be established specifically to anticipate potential incidents. Key stakeholder feedback will be solicited in various ways. The University benchmarked other jurisdictions' and institutions' projects and experiences.

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

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 is expected to respond to issues at all times, to 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.

[18] http://www.its.utoronto.ca/rules-and-regulations/regulations_guidelines/Information_Security_Guidelines.htm

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

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?

There are no outstanding gaps. 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.

The University has to be proactive in assessing the nature of the data in the other services offered under Office 365 as well. Applications like document sharing and office web apps host much more different kinds and different levels of sensitive data.

2. Privacy as the Default setting

> *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."[20]

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 articulates its coverage under, and scope of applicability of personal information as protected by FIPPA legislation:

> FIPPA and its Application to the University of Toronto
>
> Beginning June 10, 2006 Ontario universities, including the University of Toronto, are covered by the Freedom of Information and Protection of Privacy Act (the Act), which supports access to University records and protection of privacy.
>
> Some key purposes of the Act are:
>
> 1. To provide the public a right of access to university information subject to limited exemptions; and

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

2. To protect the privacy of individuals with respect to personal information about themselves held by universities and to provide individuals with a right of access to that information.

> As a publicly funded institution, the University of Toronto has upheld these principles in its operations for many years. Please see University Statement Regarding Access to Information and Protection of Privacy.
>
> What information is covered by the Act?
>
> Most records in the custody or under the control of the University are subject to the Act and its privacy requirements. A few types of records, however are excluded so the Act does not apply to them, such as research records.

In addition, 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."*

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 University has ensured that the contract with Microsoft explicitly restricts the collection, use and disclosure of all personal information. The relevant section of the contract reads:

> "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 "Privacy Guidelines for Developers" document, developers are instructed 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 that 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.

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

The personal information placed in the O365 system by staff and faculty is regulated under the FIPPA legislation. Consistent with its regulation under FIPPA, the University analyzed how well Office 365 meets FIPPA privacy requirements and explored mitigation strategies to best reduce privacy risk. The details are in ***Appendix D: FIPPA Risk Analysis***. It is divided into six sections: collection, use, disclosure, retention, disposal of data and security. Many mitigation measures 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?

One new technology being introduced with O365 is the SharePoint collaboration software. This allows users of the system to share documents and create public or private team sites to further collaborative efforts. While the privacy controls are well laid out and are not shared by default in most cases[21], care should be taken to ensure that staff and faculty do not inadvertently make documents public that should otherwise be private. Since the ability to do so exists with existing technologies, this is not a material new risk.

[21] Documents created in a personal space are private by default. Documents created in a shared folder inherit the privileges of that folder, so the potential for sharing a document accidentally exists.

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 documented guidelines for its developers to follow when developing software products and services.[22] These guidelines address core privacy or security principles.

The document includes 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."

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

Data Integrity

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

University of Toronto

The University of Toronto embedded privacy design into the infrastructure that will be interfacing with the Office 365 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 Office365, 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 Flow Analysis 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?

The University follows a risk management methodology to fully document and articulate risk, the University’s risk tolerance, risk management options and residual risks. This methodology includes Privacy Impact and Threat / Risk assessment exercises. In the context of outsourced services, the University relies upon external assessment of compliance by outsource vendors to their own risk-management practices, reported by SAS70 type II or similar audit report.

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."[23] 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.

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 Office365 project through its lifetime.

What gaps remain?

Some residual risks have been identified in ***Appendix C: Analysis of Residual Risks***.

[23] *ISO/IEC 27001 Certification Standard*, http://www.iso27001security.com/html/27001.html (November 2010).

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 staff and faculty.

Microsoft has integrated both security and privacy into its Security Development Lifecycle (SDL)[24] [25], 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?

Office 365 provides a level of service that it would be prohibitively expensive for the University to duplicate. Some of the benefits of Office365 include:

- Increasing mailbox storage to 50 GB, an increase of some 200 times over what is available to current UofT-hosted Exchange clients.
- 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 is undertaking to implement a new Active Directory service that will provide secure authentication for Office365 users via ADFS ('Active Directory Federated Services'). ADFS will allow users

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

of Office365 at the University to authenticate to University-managed access control and identity management services; this will allow the University to protect the privacy of usernames and passwords by processing them at the University without providing them to external service providers. This is discussed in more detail in the Data Flow Analysis section referenced in principle 5 below.

Cloud Computing

Considerable effort was made to analyze the cloud computing model used by Microsoft to provide the *Office365* 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.

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 L: Cloud Computing Models***.

Office365 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. Microsoft's SAS70 Type II audited compliance with the ISO 27001 standard for an information security management system has been integral in establishing trust.

Microsoft offers transport layer encryption (protecting the data as it flows between the end-user and Microsoft) and strict, audited security controls.

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 Office 365 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. This is a risk that is managed through appropriate, verifiable, contractual assurances from a service provider. 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 F: USA PATRIOT Act (2001)***.

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 Office365.

See also Appendices A (Governmental Surveillance), D (FIPPA Risk Analysis), F (USA Patriot Act), and G (USA FISA Act and Amendments).

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?

Please see ***Appendix N: Encryption Solutions*** for a full discussion of lifecycle confidentiality management.

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 *Office 365* system, these transactions can only be examined at a relatively high level of granularity.

An overview of Office 365 service data flows 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: Office365 Dataflows and Processes***.

Summary

Transport encryption, which is used throughout the Office 365 system, protects information in transit, as it flows over the Internet from U of T to the Microsoft data centers and back.

Information at Risk

This PIA uses the FIPPA definition of personal information (see ***Appendix D: FIPPA Risk Analysis***) and Appendix H. Email is used to communicate personal and confidential information and other Office365 services may be usable to store or communicate personal information. This information is protected under FIPPA legislation. The following chart highlights some of the types of confidential information that will potentially be stored on Office365. In each cell there is an assessment of the perceived impact to the University (sensitivity) of the information being disclosed, altered, deleted or accessed without record of use.

	Confidentiality	Integrity	Availability	Accountability
Education Records	High	Low	Low	Med
Financial Data	High	Low	Low	Med

Investigations / Disciplinary Actions	High	Med	High	High
Personal Correspondence of Staff/Faculty	Med	Low	Low	Low
Research Data	High	High	Med	High
Medical Information	High	High	Med	High
Authentication Tokens (Passwords)	High	Low	Low	High

A full discussion of the potential for risk to these assets being realized is contained in the section '*Threat / Risk Assessment Analysis'.*

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.[26] [27]

Microsoft achieved Federal Information Security Management Act (FISMA) certification & accreditation for its data centres in May 2012.[28] This certifies that the security of Microsoft's cloud computing infrastructure is sufficient for obtaining U.S. government contracts.[29] [30]

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. The company conducts risk assessments, implements security controls and regularly monitors the success of those controls to protect its 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;

[26] http://en.wikipedia.org/wiki/ISO/IEC_27001
[27] Microsoft ISO 27001 Certifications
[28] http://blogs.technet.com/b/gfs/archive/2010/12/01/microsoft-s-cloud-infrastructure-receives-fisma-approval.aspx
[29] http://en.wikipedia.org/wiki/FISMA
[30] http://csrc.nist.gov/groups/SMA/fisma/index.html

- 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?

With the inclusion of UT-managed encryption solutions, there are no material residual gaps. 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.

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 (please see Appendix D: FIPPA Risk Analysis). It was found that the agreement gives the University the assurance that Microsoft is operating within the bounds of FIPPA. In addition, the agreement states that, except for alumni, the University may opt to turn off advertising in all of the Office365 services (except Messenger, for which this is not possible)

> "…Microsoft agrees not to display on the web interface to the E-Mail Service or any Thick Client interface to the E-Mail Service, any Advertisements that promote Microsoft or third party products or services, except that Microsoft may display such Advertisements on the web interface of the E-Mail Service available to Alumni." (2.c.ii)

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

The FIPP website provides information on the legislation and policies governing the management of personal information at the University,[31] and the website of the Provost details University privacy and personal information practices.[32]

Microsoft has detailed documentation about its security and privacy practices on its website.[33] 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.

[31] http://www.fippa.utoronto.ca/Page4.aspx
[32] http://www.provost.utoronto.ca/Assets/Provost+Digital+Assets/Provost/fippa.pdf
[33] 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 Office365 service and the technical issues that may arise.

A privacy principle 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."[34]

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

University of Toronto

While direct monitoring of the Office 365 environment is not possible, Microsoft has agreed to provide the University of Toronto and users of Office 365 with notification of access to personal information, where possible (see Appendix D: FIPPA Risk Analysis). As well, the University of Toronto monitors those aspects of the Office 365 environment that are externally visible, and which can have an impact on privacy (see 'FOPE' in our analysis of Microsoft's compliance below).

Microsoft

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 has responded to University privacy concerns, 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

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

worked with David Fischer of Microsoft who is Senior Product Manager of Office365 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 requested that it be turned on for its test users. FOPE has now been tested by the University and is active.

During the initial phases of the operational relationship between Microsoft and the University of Toronto, support was provided by submitting a "ticket" to the online Microsoft support system. The time to resolve the issue could be upwards of a couple of weeks and in these cases the customer would not have access to their email account. To mitigate this issue Microsoft responded by giving our technical staff direct access (for a certain class of problems) to Dave Fisher, who is able to resolve the issues in a shorter time frame.

One area of ongoing concern is the application of updates to the cloud software by Microsoft. The University of Toronto has little or no control over the scheduling of these updates, and has no choice to opt-out of them if it wishes. In some cases, this can have negative impacts on the customer, as it did in January 2012, when Microsoft applied an update to their software that broke connectivity to Live@edu for many Android mobile devices.

With the move of staff and faculty to O365, the University should be aware that such disruptions of service could potentially have a greater impact on the University's business if administrative staff had a long-running support request, or an update caused the loss of functionality to a subset of the population.

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?

University of Toronto

The University opened numerous channels to solicit the input of users affected by the proposed e-communications solution. Through the means of six Town Hall meetings, numerous meetings with technical support staff, administrative staff, faculty, the Faculty Association Executive, a number of academic administrator groups, and a formal Faculty and Staff Advisory committee, the University sought input from all stakeholder perspectives. During these consultations, issues surrounding security and privacy risk mitigation were raised and further explored, and feedback was received as to stakeholder expectations.

Stakeholder Expectations

It is clear that the variety of information staff and faculty will store on the service is much more diverse than that stored by students. In addition to this, there are a number of types of activities that staff and faculty carry out over email. These include, but are not limited to, administrative functions, teaching, research and personal activities. The addition of document sharing (SkyDrive) and website creation (SharePoint) will certainly increase the volume of data being shared through the system. These and other issues were addressed in the consultations.

In addition to several overarching conversations about security and privacy protection, the following specific privacy / security questions were discussed by the Advisory Committee:

1. Microsoft offers a chargeable service that allows the tracking of email receipt. Have you had reason to track email receipt in the past / do you anticipate you'll want to do so again in future? Is it worth the expense to the University to subscribe to this functionality?

   ➢ Committee members responded that tracking email has been required in the past, for example: when investigating unauthorized access to email accounts, in identifying who may have read a mis-sent email that contained Personally Identifiable Information, and in troubleshooting email that was not received. This type of service has been needed on the order of monthly; the committee felt that it was a worthwhile service to subscribe to, despite the fact that there was a cost associated with it.

2. Do you have any concerns with respect to cheating and plagiarism that uniquely arise from document sharing and collaboration features of Office365?

   ➢ The members who responded said that there were no concerns with regards to cheating and plagiarism that might uniquely arise from the document sharing and collaboration features of Office365.

3. Should we be investigating technical capacity to limit sharing of sensitive information with correspondents external to University?

    - In early discussion, members of the Committee suggested that Office365 afforded sufficient granularity of access management to mitigate the risk of unauthorized access to sensitive or research material, and that there were no additional controls required. Further, to apply technological controls to implement rule-based limitations on disclosure of information (e.g. Data Loss Prevention (DLP) tools) would be infeasible given the difficulty in creating rules to match the broad range of formats that can represent sensitive data.
    - Later discussion, in the context of extensive media coverage of state surveillance, turned opinion toward the requirement of having strong encryption resources available, and user education as to how to handle data of varying sensitivities.

4. What specific concerns should we be addressing / practices we should be encouraging with respect to medical data, research data, grade data?

    - If possible, the committee felt that it would be valuable to have access to required practices for the management of sensitive information as part of the Office365 interface – such as mouse-over information boxes or tabs that would reveal guidance when clicked on.

5. Are there other privacy risks that we have not yet identified, unique to faculty and staff?

    - The committee recommended that practical documentation and education materials should be developed and distributed to end-users so that they may understand new risks they may be exposed to, and any changes or additions to privacy and security-related practices they would be expected to follow in the new environment of Office365.

The University will be providing a locally managed solution that users can use to encrypt FIPPA / confidential and other email at their discretion.

Microsoft makes a commitment to empowering users in their *Privacy Guidelines for Developing Software Products and Services*

Email is a core service for many of the daily activities that staff and faculty undertake. Email (along with the document sharing applications like SharePoint) is fundamentally user-driven. Each user decides what information will be placed into the system.

Has free and specific consent been established for the collection, use or disclosure of personal information and can consent be withdrawn? Are individuals given a clear Notice of the uses and disclosures or their personal information? Yes. *How?*

The University should present a notice to staff and faculty as they register for this service that outlines how the service works, and what types of activities should and should not take place on the service.

Summary

Microsoft appears to have a strong 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.

Appendix C: Analysis of Residual Risks

Residual Risk Solutions

Microsoft has several features to effectively manage privacy risk such as transport layer encryption (protecting data flows between the user and Microsoft) and strictly audited security and privacy controls. The University has worked with Microsoft to build reasonable privacy protections into the contract. The Universities experience with working with Microsoft using the Live@Edu system has been positive and provides reassurance that Microsoft is committed to and capable of protecting privacy.

Summary of Residual Risks

The following table provides a short summary of risks. The source column indicates the relevant legislation or analysis from this PIA related to the particular risk.

Risk	**Description**	**Mitigation**	**Areas of Concern**
Proxy Server Compromise Probability - Low Impact – High	Microsoft authentication proxy server is compromised, revealing UTORids and passwords.	Monitoring of Proxy Server administrative access and system health status.	FIPPA *PbD*
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.	Same as current state. No new risk.	*PbD*
Microsoft Employee Acting Without Authorization Probability - Low Impact – High	An employee at Microsoft decides to use his/her administrative access without authorization to access *Office365* user information, potentially for illegal purposes.	UofT staff could do this today. No new risk.	FIPPA
Accidental disclosure by a Microsoft employee Probability - Low Impact - Medium	A Microsoft employee accidentally discloses a user's personal information	UofT staff could do this today. No new risk.	FIPPA *PbD*
Foreign Legislative Threat Probability – Low Impact - Medium	A request for information is made to Microsoft under USA PATRIOT / FISA Act or similar legislation	UT-managed encryption of email contents and attachments.	FIPPA
Attacks from within the cloud Probability - Low Impact – High	Due to the shared nature of cloud computing, vulnerabilities of *Office365* might be exploited by other customers of Microsoft's cloud computing architecture	Receipt and review of regularly scheduled Microsoft Penetration Testing reports.	FIPPA *PbD*

Risk	Description	Mitigation	Areas of Concern
Mishandling of data by UofT Probability - Low Impact – Low	A University of Toronto employee accidentally discloses a user's personal information	IT staff will always have administrative access over systems: No new risk.	FIPPA
Updates to O365 break functionality Probability - Medium Impact - Privacy: Low Operational: High	Microsoft applies a software update to the O365 service that causes some users to lose a function that they rely upon to conduct business.	This could occur when current software is patched. MS have a robust testing process. No new risk.	
Disclosure of Sensitive Data Probability - Medium Impact – High	The volume of sensitive information will increase with staff / faculty on the outsourced system. The residual risk increases accordingly.	End users must be educated and trusted to maintain confidentiality when handling sensitive data.	FIPPA
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.	Contract has appropriate language to govern the termination of the relationship. Microsoft is a mature vendor so risk is not material.	

This appendix sets out the residual risks. 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 and UT-managed 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 *Office365* 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 has implemented a proxy server that allows non-Shibboleth enabled clients to use Shibboleth authentication. This allows Microsoft to accept authorization provided by the University's identity management system. The user's 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 *Office365* 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 staff / faculty UTORids and passwords could potentially be harvested from a compromised Microsoft authentication proxy server.

Probability: Low, Impact: High.

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 staff or faculty members could be accessed by the attacker, with possible outcomes such as identity theft, harm to reputation or personal distress.

Existing Mitigations:

Microsoft integrated security and privacy into their Security Development Lifecycle which minimizes 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 *Office365*, these are somewhat offset by the decommissioning of the UTORmail infrastructure that was serving students, staff and faculty. 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[35].

Impact:

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

[35] http://techcrunch.com/2010/09/14/google-engineer-spying-fired/

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.[36]

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 / FISA Acts 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.

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

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:

- The use of encryption to mitigate this risk has been discussed in detail in other sections of this document.

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:

Within the same Microsoft data centers as *Office365* 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 *Office365* 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, *Office365* 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[37]:
  "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[38]:
  "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:

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

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

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 and Microsoft Technical Administrators

Description of risk:

During the migration to *Office365*, 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, hosted and managed by the University, 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, 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 confidential data.
- The University should audit its staff's privileged access to *Office365* 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.
- The use of encryption to mitigate the risk to data exposed to administrators with privileged access has been discussed in detail in other sections of this document.

Residual Risk:

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

Updates to O365 Break Functionality

Description:

With a cloud-based service such as O365, the vendor is in charge of software updates, and can apply them to their systems without consulting their user base. In some circumstances this can cause service outages.

Impact:

It is possible that access to email / calendaring / documents could be interrupted by a mis-applied software update.

Potential Mitigations:

- Since Microsoft controls the software, there is no mitigation for this risk.

Residual Risk:

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

Disclosure of Sensitive Data

Description:

With the move of staff and faculty to the cloud-based O365, the University can expect that the amount of confidential information residing in the system will increase drastically. Further, allegations have been made that encryption of transmitted data may be vulnerable to attacks by the US NSA, owing to weakening of encryption standards.

Impact:

There will be much more sensitive information stored in the cloud, with the resulting increase in the impact to the University if this data is exposed.

Potential Mitigations:

- The use of encryption to mitigate this risk has been discussed in detail in other sections of this document.

Residual Risk:

Probability: Medium, Impact: High

Improper Termination of Agreement

Description:

The University must consider that the agreement with *Office365* will eventually come to an end. It has been estimated that it could take the University of Toronto at up to six months to migrate data out of *Office365* with the current amount of data. When it is eventually time to migrate out of *Office365*, 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 *Office365*.

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 *Office365*.

- 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

Appendix D: 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 practices data minimization.[39] Microsoft provides security and privacy training to its staff. Despite these assurances, proper notification need be provided to Office365 users informing them of the personal information that will be disclosed to Microsoft. In addition, since the Office365 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:

- Except with respect to data provided to Microsoft for the purpose of providing the E-Mail Service to End Users, no Personal Information of End Users will be required to be provided by one party to the other under this Agreement. In providing the E-Mail Service Microsoft will be receiving information from End Users that may contain Personal Information. 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. (4.a)
- There are no cookies, actions tags, or any similar technology used by Microsoft in the E-Mail Services to obtain, track, monitor, implement any form of profiling, or assessment of Covered Data and Information except as may be described in this Agreement to provide and improve the E-Mail Service. (3.d.iv)
- In order to provide the Microsoft Services, Microsoft may collect certain information about Microsoft Service performance, End User machines and Microsoft Service use. (4.f) Microsoft assures us that this information is not Personally Identifiable Information.

Karen McGregor, Education Solution Specialist from Microsoft has provided the following information to the University:

"Service Data include performance data or information from the PC as to the browser being used so that the OWA experience can be optimized. Information is aggregated for reporting but not tracked with Personal Identifiable Information."

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

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

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 Office365 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 Office365 service must be expressly set out in the contract.

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

- …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. (4.a)
- Each party shall take commercially reasonable security and other measures to protect the Covered Data and Information and Credentials under its control from unauthorized access, use, disclosure, alteration and destruction and will protect Covered Data and Information and Credentials in its possession and control as it protects its own confidential information of like nature. Such security measures will include authentication controls, encryption of Covered Data and Information while in transit, physical controls or other means in accordance with each party's own information security policy. (4.c.i)
- In order to operate and provide the Microsoft Services, Microsoft may collect Personal Information about End Users as provided for under this Agreement. Microsoft may access or disclose Institution or End User information, including the content of End User communications, in order to: … (2) take action or pursue other remedies against suspected purveyors of spam, viruses, malware, phishing or other attacks that have in any manner disrupted or diminished, or may in the future in any manner disrupt or diminish, Microsoft's services; ... (4.e)

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

There is a risk that Microsoft or an affiliate could *disclose* personal information collected by Office365 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:

- Microsoft states in the agreement that it will implement security measures including "encryption of Covered Data and Information while in transit". (4.c.i)
- A technical analysis of Office365 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:

- …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. (4.a)

- …Microsoft may access or disclose Institution or End User information, including the content of End User communications, in order to: (1) comply with the law or respond to lawful requests or legal process; (2) take action or pursue other remedies against suspected purveyors of spam, viruses, malware, phishing or other attacks that have in any manner disrupted or diminished, or may in the future in any manner disrupt or diminish, Microsoft's services; or (3) act on a good faith belief that such access or disclosure is necessary to protect the personal safety of any individuals from a life threatening emergency. Solely with respect to any disclosure made pursuant to subsection (1) above, Microsoft will use commercially reasonable efforts to provide Institution notice, when legally permissible to do so, that a demand for Institution and/or End User information has been made, prior to the disclosure of any such information. In any instance where Microsoft is prohibited by law from providing notice, Microsoft will comply with any such lawful request or legal process demanding Institution and/or End User information. Solely with respect to any disclosure made pursuant to subsections (2) and (3) above, Microsoft will provide Institution notice, within a commercially reasonable amount of time that a disclosure has been made of Institution and/or End User information. (4.e)

- Microsoft shall, within a commercially reasonable period of time after discovery of any unauthorized or unlawful access to, loss or disclosure or alteration of or malicious compromise of any Covered Data and Information in its possession or control (a "Security Incident"): (4.c.vi)

    1. notify Institution of the Security Incident;
    2. investigate the Security Incident and provide Institution with detailed information about the same;
    3. provide reasonable assistance to Institution to the extent necessary to enable Institution to comply with applicable law implicated by the Security Incident;
    4. take steps to mitigate the effects and minimize the damage resulting from the Security Incident; and
    5. make changes to minimize the likelihood that the Security Incident will re-occur.

Retention

The University must retain personal information for at least a year after the date of its last use. Confidential 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 staff and faculty. Notice will be provided to the University as follows:

- Microsoft will notify Institution of any suspended or terminated End User email account. (4.c.ii)

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 Office365 could be *disposed* of improperly, leading to a disclosure of personal information.

The Agreement states:

Microsoft will provide Institution with industry standard interfaces and protocols to enable Institution, at any time, to extract all Covered Data and Information, and, upon request, Microsoft shall destroy or return to Institution all Covered Data and Information, content, technology and materials forwarded to Microsoft by Institution or its End Users under this Agreement. (8.d)

Microsoft has also indicated in its SAS70 Type II report that it has an audited backup tape disposal process.

Security

In addition to security analyses of Office365 set out elsewhere in this assessment, the agreement states:

- 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 E-Mail Service. Where the SAS 70 Type II report identifies material deficiencies 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. (4.k)
- Each party shall take commercially reasonable security and other measures to protect the Covered Data and Information and Credentials in its possession and control from unauthorized access, use, disclosure, alteration and destruction and will protect Covered Data and Information and Credentials in its possession and control as it protects its own highly confidential information. Such security measures will include authentication controls, encryption of Covered Data and Information while in transit, physical controls or other means in accordance with each party's own information security policy (4.c.i)

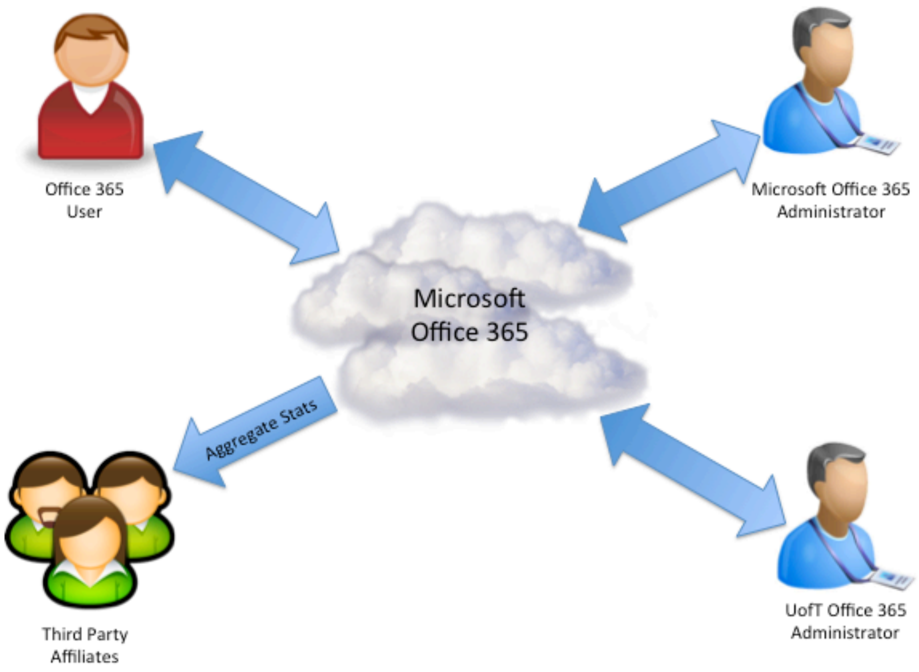
These clauses provide security assurances consistent with FIPPA requirements.

Appendix E: Office365 Dataflows and Processes

Overview

The following section is adapted from the Live@edu PIA for students. Some of the information here may be inaccurate since the procedures surrounding the move of staff and faculty have not been fully worked through at time of writing. While some details may change, the main features of outsourcing email as outlined in these data flows will remain the same.

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



***Office365* User**
These are the users of the service, UofT staff and faculty, whose personally identifiable information will be stored in the system.

Microsoft *Office365* Administrator
These are administrators employed by Microsoft to staff their data centers and provide support for their *Office365* platform. From the standard *Office365* 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 *Office365* Administrator
These are UofT administrators who will have some access to the *Office365* platform. UofT policy governs the access a UofT administrator has into the *Office365* system.

Third Party Affiliates

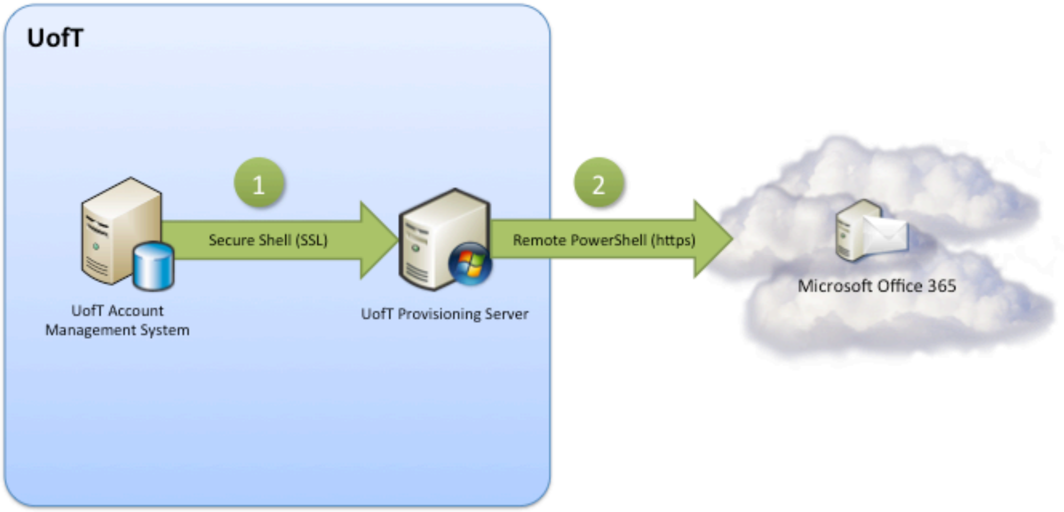
Microsoft has indicated that it may provide aggregate statistics to third party affiliates but ensures that no personally identifiable information will be revealed in this transfer.

Initial Setup

There are two steps in this process: provisioning and migration.

Provisioning

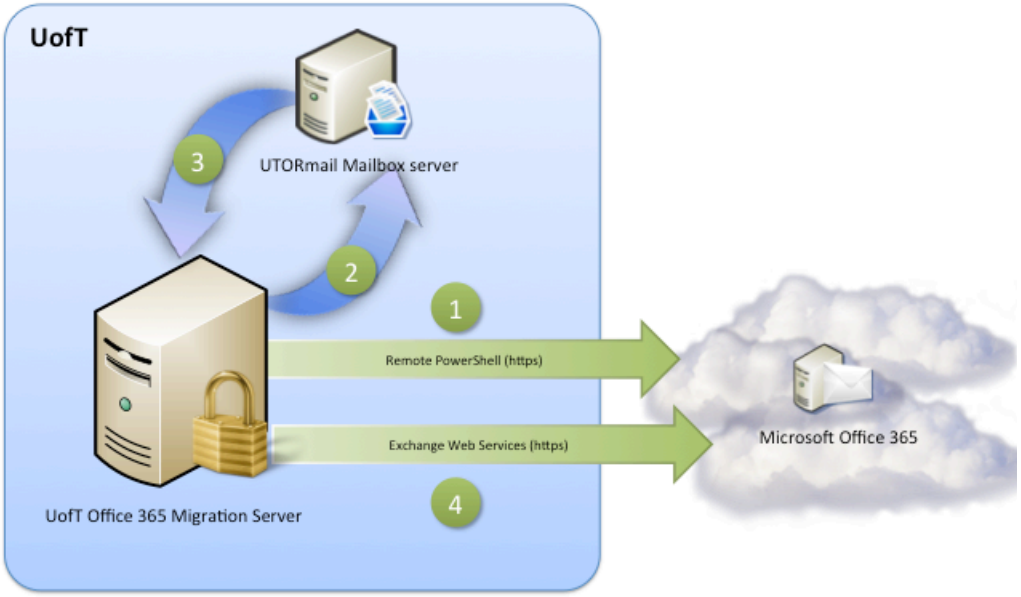
"Provisioning" refers to the process by which an account is created for a user on the *Office365* servers. This is a two step process:



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 *Office365* 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 Office365 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 *Office365*

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 Office 365
UofT Office 365 Migration Server

1. Using Remote Powershell, the UofT Administrator establishes a secure connection from the UofT *Office365* Migration server to the Microsoft *Office365* 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 *Office365* 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 *Office365*.

From a privacy perspective, this migration process is well thought out. All of the connections to the *Office365* service are fully encrypted to ensure that communication between UofT and Microsoft is protected from eavesdroppers.

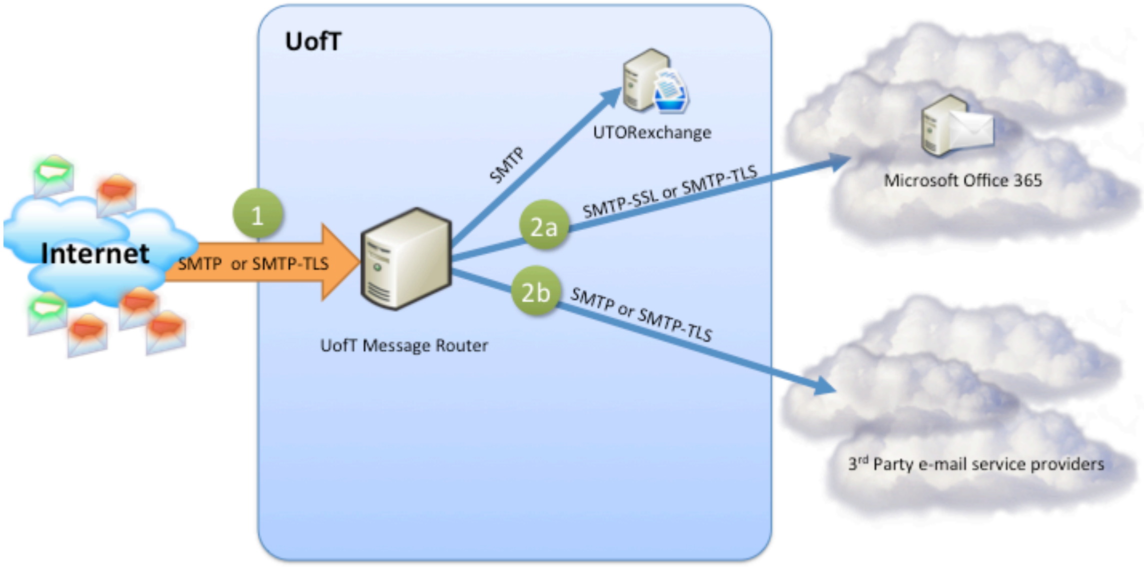
Email Flow

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 *Office365* and the users of their service. This means that the University is able to force encryption between UofT mail routers and the *Office365* 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.

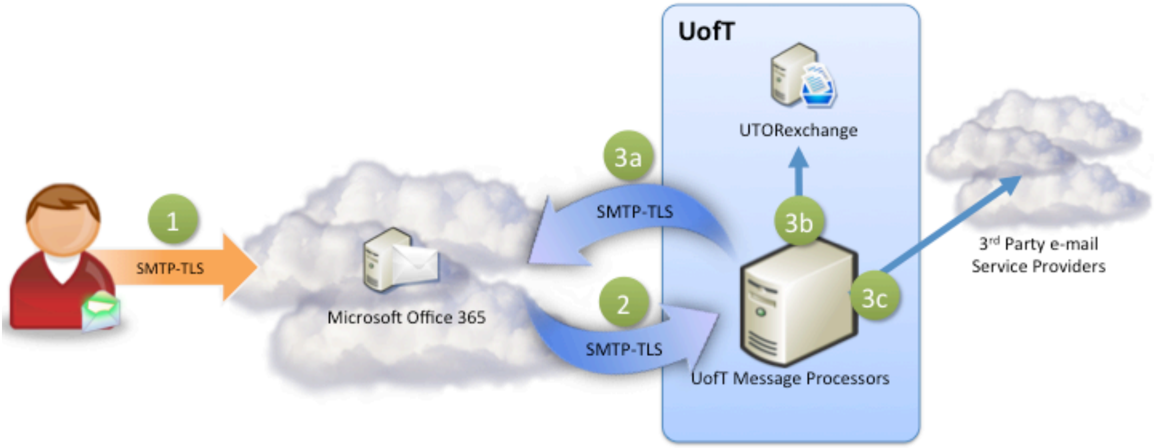
2. On the UofT routing servers a lookup is performed that determines whether a user is using *Office365* or whether they have opted-out and forwarded their mail elsewhere. (UTORexchange is included in this diagram only to indicate that staff / faculty email remains within the University and is not forwarded on to an external 3rd party).

   a. If the user uses *Office365*, the message is sent to the *Office365* 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 *Office365* 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 *Office365* 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 *Office365* service over an encrypted channel if the recipient specified is another UofT *Office365* user.

    b. To the UTORexchange servers if the recipient specified is a staff / faculty member of UofT who uses the UTORexchange service.

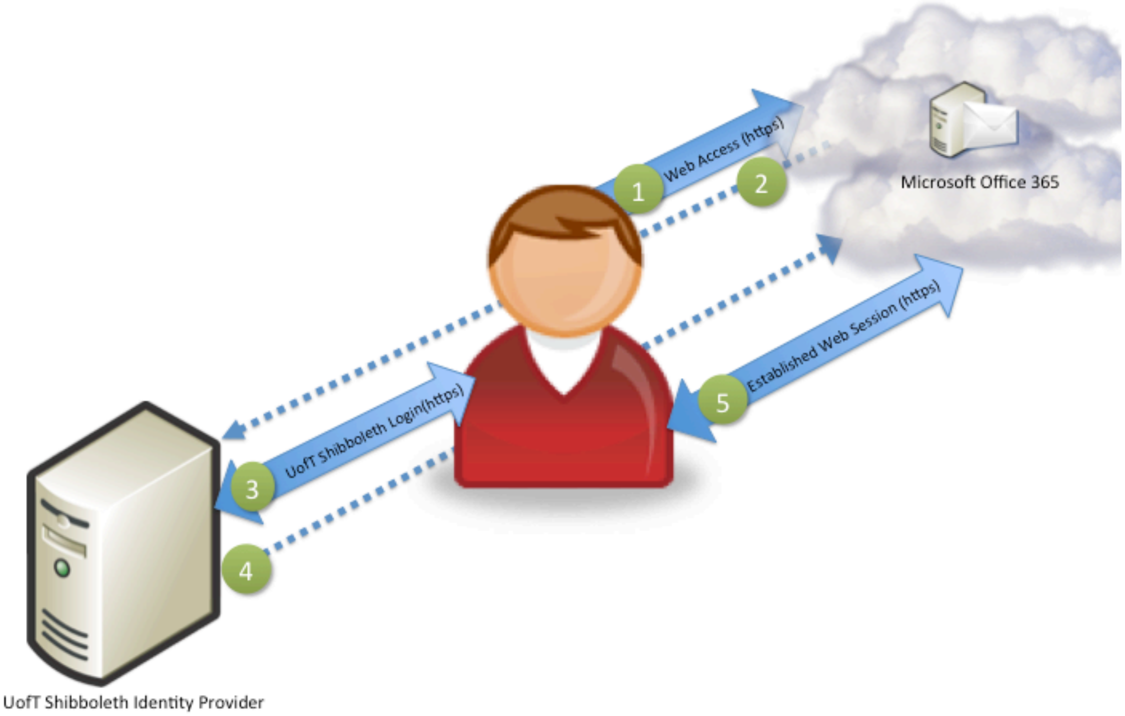
    c. Otherwise, the message is routed out to the recipient's email provider outside of the UofT.

The assurance that the University can force the encryption of email flowing between UofT and *Office365* provides an essential guard to privacy.

Web-Based Access to Office365

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 *Office365*. The services included under this authentication method are:

- Outlook Web Access


Web Access (https)
1
2
Microsoft Office 365
UofT Shibboleth Login(https)
3
4
Established Web Session (https)
5
UofT Shibboleth Identity Provider

1. The user initiates a request to connect to *Office365* through a web browser or other web technology. This session is conducted over HTTPS, which is encrypted with SSL/TLS.

2. The *Office365* 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.

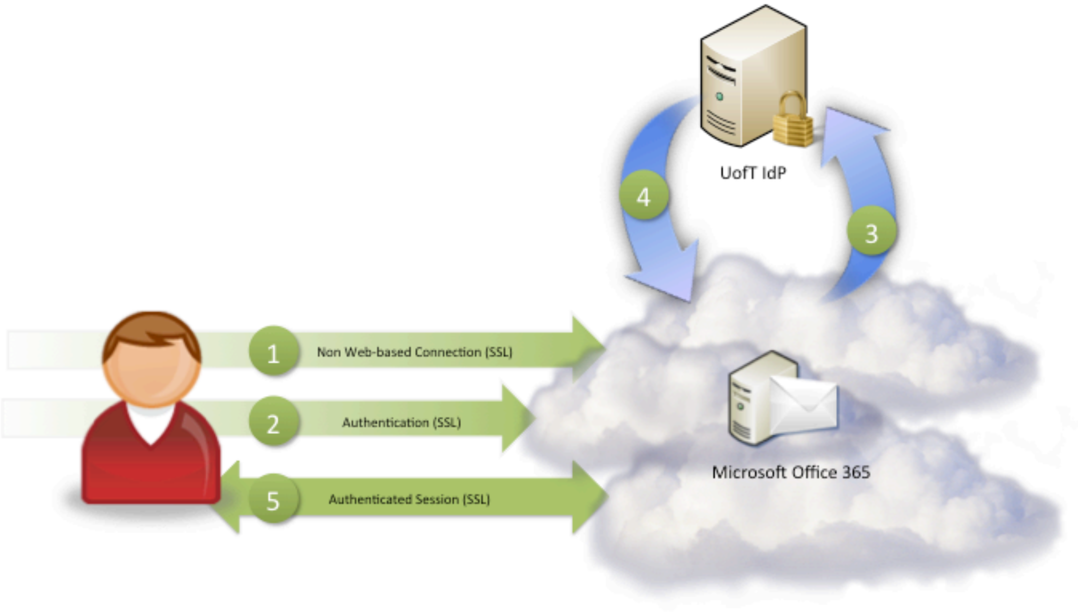
4. Upon successful login, the UofT IdP server will send the user back to *Office365* (over SSL) with an assertion, which includes the following attributes:
   a. User's WLID-eppn (UTORid@domain)
   b. User's WLID-uid (a one way hash of the UTID)
   c. An authentication token that indicates to *Office365* that UofT has authenticated the user

5. The user now has an established web-based session with *Office365* and begins to use their services. This session is encrypted with SSL/TLS for the entire duration.

Non Web-Based Access to Office365

While the University does anticipate that the majority of users will connect to *Office365* 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 *Office365* servers, encrypted with SSL/TLS. Authentication is requested by *Office365*.

2. User sends their authentication credentials consisting of their username (UTORid) in the form *utorid@mail.utoronto.ca* and their password.

3. *Office365* 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 *Office365* that UofT has authenticated the user

5. The user can begin to use the *Office365* 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 *Office365* 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 an *Office365* user is no longer a staff/faculty member of the University they will no longer have access to *Office365*'s services through the University. *Office365* does not have access to staff status data, and therefore relies on UofT to terminate service. *Office365* will hold all the contents of all deleted accounts for 30 days, at which point the information will be disposed of.

Appendix F: USA PATRIOT Act (2001)

The 'USA PATRIOT' act amended the Foreign Intelligence and Surveillance act of 1978 (FISA), the Electronic Communications Privacy Act of 1986 (ECPA), the Money Laundering Control Act of 1986 and Bank Secrecy Act (BSA), as well as the Immigration and Nationality Act. Its purpose was to strengthen US legal system to respond to perceived threats of terrorism.

The University of Alberta email outsourcing project website provides useful information about the USA PATRIOT act, which is included here for reference.[40]

> **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 Commissioner 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

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

> 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." [41]

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

> "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."

[41] *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)

Appendix G: USA FISA Act and Amendments

Concern has been raised about the scope of the USA Foreign Intelligence Surveillance Act of 1978 (and subsequent amendments of 2008); the exposure of Canadians under this act in general and its implication for information within the proposed e-Communication system in specific. The act was originally created to give the US the ability to legally, and secretly and without court order, surveil the activities of foreign entities within the United States. Successive amendments introduced provisions to allow wiretapping of communications that begin or end in a foreign country from the US, without court oversight.

While this appendix is not, nor can it be, a legal analysis of the implications of the FISA act on Canadian communications in the US, it is possible to see that the act does allow for the surveillance of communications in the context of the proposed e-Communications solution. To that end, however, there is no provision that requires the University of Toronto to surrender encryption keys to US authorities singly or en masse, should the University choose to encrypt data within the e-Communications environment.

Without a comprehensive analysis of the legal implications of the FISA act, it is recommended that if the University wishes to avoid capture and analysis of confidential / FIPPA-included information, a University-managed email encryption solution should be pursued.

Appendix H: 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 I: 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 J: 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 K: 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 Office365.

3. User Agent - This is the user who is accessing Office365 through their web browser.

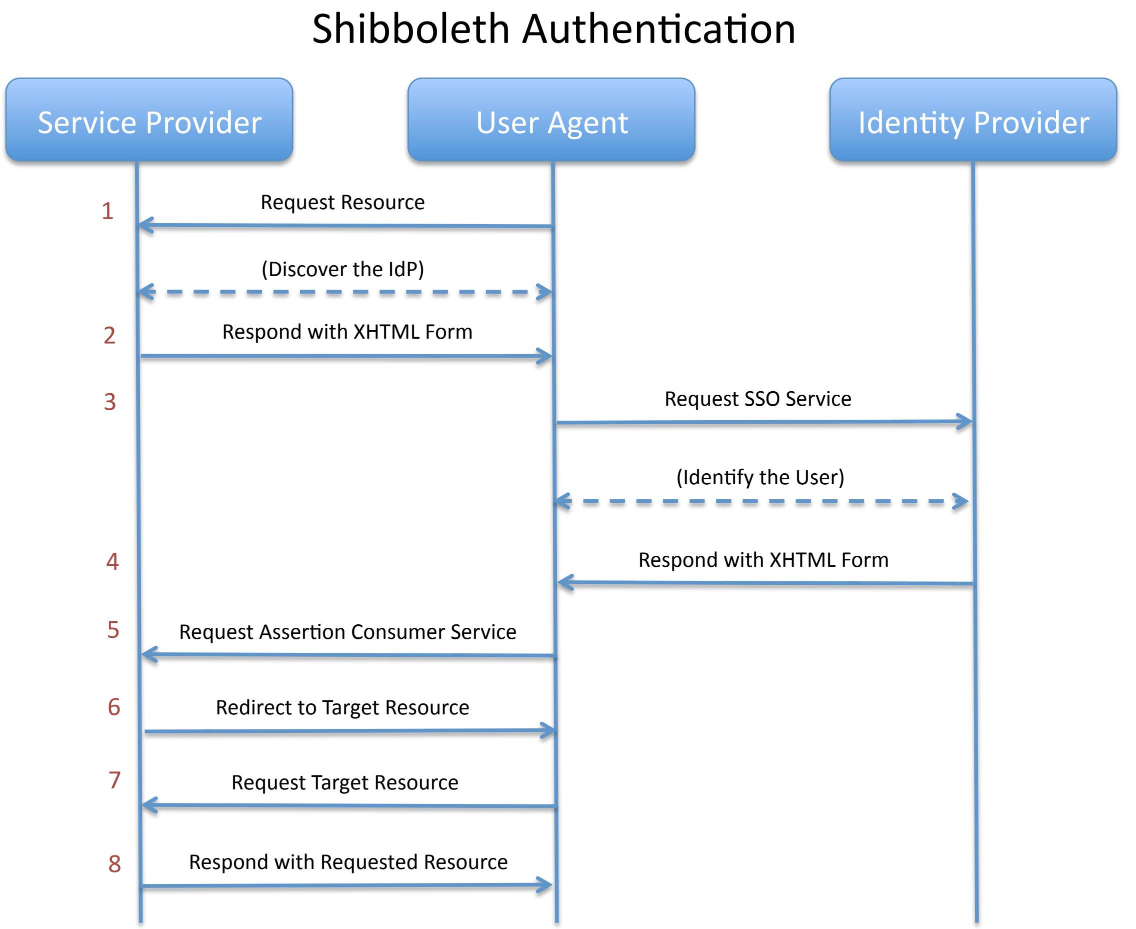


Figure 1: SAML 2.0 Authentication Flow [42]

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.

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

8. Since the security context has been established, the SP returns the requested resource.

Appendix L: Cloud Computing Models

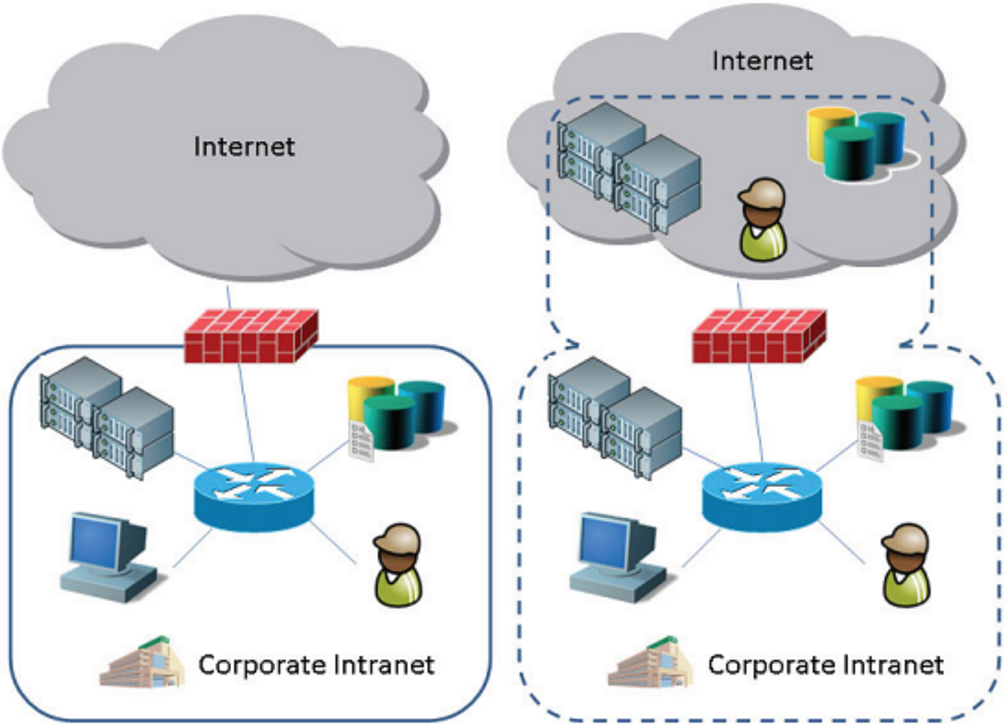


Figure 2 -- Left: Clear Distinction between the Trusted and the Untrusted; Right: Fuzzy Security Perimeter[43]

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[44]

- **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.

[43] *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

[44] *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[45]

- **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).

[45] ibid., p. 17

Appendix M: Work Units

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

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

University of Toronto

Information + Technology Services

Name	Role
Robert Cook	Information + Technology Services, CIO
Martin Loeffler	Information Security, Director, Security Lead
David Auclair	Information Security, PIA Author
Matt Wilks	Information Security, PIA Author
Axel Johnston	Information Security, PIA Author
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

Freedom of Information and Protection of Privacy office

Name	Role
Rafael Eskenazi	FIPP Director
Howard Jones	FIPP Coordinator

Microsoft

Name	Role
David Fisher	Senior Product Manager, Office365 Research and Development
Brad Tipp	Education Solution Specialist, Office365
Richard Wakeman	Solution Architect, Microsoft Consulting Services
Raj Mukherjee	Senior Product Manager, Online Services
Gabe Long	Release Manager, Office365 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

Appendix N: Encryption Solutions

The former Ontario Privacy Commissioner has identified encryption as the 'gold standard' for protecting information in hostile environments. As such, a need has been identified for ubiquitous, easy-to-use email encryption that would protect FIPPA-covered and other sensitive information while shared between anticipated University of Toronto staff and faculty users of Microsoft's Office 365 service. The functional requirements of such an encryption solution beyond 'encrypt all the data' are many and varied, and often limited by what commercial solutions are available, as the space inhabited by both commercial and open-source encryption solutions is small (although this may change with growing customer demand paralleling increased public awareness of privacy issues).

An acceptable encryption solution would enable users to completely determine who should be able to interpret both email contents and associated attachments, regardless of who may have a copy of the data. Of course, as trusted recipients may actually be intentionally or unintentionally untrustworthy, encryption systems can never protect data from disclosure once it has been received and decrypted by a trusted recipient. In addition to controlling who should be able to receive and interpret data, the solution must also allow for users to recover access to encrypted data should they forget their passwords or lose their own personal decryption keys. Such a solution would also perform encryption and decryption on local, trusted, systems only so that unencrypted data never exists in the memory of untrusted systems (i.e. external 'cloud' servers). The solution must also support strong protection and management of encryption and decryption key pairs as a loss of confidentiality for key pairs eliminates the protection afforded by encryption and an inability to revoke keys leaves information available to users after a time where they are no longer authorized to access the data. "SafeNet eTokens" have been proposed to provide this functionality, as they are a key-management technology that the University is familiar with, and is already using to provide secure access to confidential systems. Finally, the solution must be compatible with the service / technology it is intended to protect – in this case, Office 365 – on both Windows and Apple OS X platforms. Resolution of finer operational concerns such as the sharing or delegation of keys, ease of use, and integration with underlying infrastructure technologies would also be required.

Within these terms of reference, a market survey has indicated that there exist solutions which would meet our initial requirements to protect FIPPA-covered and other sensitive information while within the Office 365 environment, and which do not rely on external parties to implement or manage., There is a range of options, both commercial and open-source, balancing component cost, administrative cost, automation, and functionality.

The University proposes to mitigate risk to the confidentiality of sensitive information through the provision of University-managed content encryption tools. These tools will be configured to operate automatically wherever possible to minimize the burden of data management on users. A project to develop appropriate encryption services has moved past the proof-of-concept stage, and has been severed from the IRRM effort. Information about a proposed solution will be shared with the community separately as it is finalized.

The University also proposes to exercise its strength in the area of education by proactively raising awareness amongst staff, students, and faculty, as to the risks inherent in all e-communications.

While a great deal has been speculated about the NSA's ability to defeat current encryption protocols, documents released by Edward Snowden (http://www.theregister.co.uk/2014/01/03/snowden_docs_show_nsa_building_encryptioncracking_quantum_system/) suggest that current encryption algorithms can be trusted, for the time being, absent a compromise of / weakness in the implementation of those algorithms in technology (compromises which are being actively pursued by the NSA: http://www.reuters.com/article/2013/12/20/us-usa-security-rsaidUSBRE9BJ1C220131220, http://online.wsj.com/article/BT-CO-20140225-709664.html and http://www2.macleans.ca/2013/09/11/nsa-says-it-finessed-canada-seizing-control-of-global-crypto/).

Appendix O: Metadata Risks, Protection, and Limitations

Summary

There are limited options for protecting metadata from surveillance. Encryption, the preferred strategy, imposes limits on service functionality primarily by breaking search and indexing functions, and secondarily by limiting the University's ability to send email to sites that do not support encryption if transmission encryption is mandatory.

What is Metadata?

Briefly, metadata is secondary information associated with a document or record. It is often contextual information – file name, file author / owner, creation data, revision history, notes and comments – or system-level information, such as email sender, subject, or recipient. Metadata may be contained within a document or record (intrinsic metadata), or may be stored in a system that handles such (extrinsic metadata). As well, metadata may be user-supplied (such as an email subject), or automatically generated (such as a file creation date).

While often overlooked, metadata represents the mechanism through which much value is delivered in information systems – the presence, absence, and quality of metadata controls our ability to search and locate documents, contacts, and calendar entries among other things.

Risks

Metadata has been identified as an asset having value within the scope of outsourced information services. Besides having innate value, it is recognized as representing risk to the University if its confidentiality, integrity, or availability is compromised. Existing agreements with Microsoft for student email prohibit the non-operational (i.e. data mining) use by Microsoft of metadata associated with data in student email accounts. State-sponsored surveillance and harvesting of metadata is still a concern however; it is believed by many that hosting data outside of Canada increases the risk of state surveillance over such data, however this risk exists within Canada as strongly as in any international context.

In the context of an outsourced service, metadata resides in an almost innumerable variety of contexts: it may be found in the names of file attachments to email; stored within contents of those attachments (file author, creation date, reviewer's comments, etc. which are often invisible, or at least not immediately obvious); and in the email itself (including the familiar "From", "To", and "Subject" fields, and a host of usually invisible email header information such as: "Keywords", "Priority", and less intuitive fields including: "Fcc", "Xref", and "Content-Transfer Encoding" that are either optional, non-standard, or used by mail servers for automatic mail handling. [For a full discussion of email headers, please see RFC 2076: http://www.ietf.org/rfc/rfc2076.txt]).

As well, metadata exists within the outsourcer's own systems for purposes of keeping track of files and email; in this way, servers – be they in-house or outsourced – function exactly as a desktop computer, using file names, creation dates, sizes, and ownership(s), as a means to store or retrieve the information, and to enforce access and change controls.

To discuss the security of data at rest in an outsourced environment then, it is necessary to not only define the scope of what metadata is at risk, but also what metadata can be protected and at what cost to functionality. No out-sourced information service that ITS is aware of runs on an operating system where some final, highest level of administrator is unable to see all system-level metadata; however, in the context of concerns over outsourcing to non-Canadian service providers, the desire is that the Canadian customer of the service provider exercise final (or as close to final as possible) control over the confidentiality, integrity, and availability of that information. The only metadata that falls under that rubric is metadata provided and protected by the users of the service themselves.

As for data in transit, the Government of Canada has indicated that does not hold that bulk gathering of metadata is contrary to Canadians' lawful rights and freedoms (http://www.cbc.ca/news/canada/csec-exoneration-a-mockery-of-public-accountability-1.2536561). In the specific case of corresponding outside of the University by email, the University may be able to ensure that communications between email clients and its own email servers must be encrypted, but has no control over external email servers used by email recipients and may be forced to send email over unencrypted channels or not at all.

Protection

Encryption is the 'gold standard' identified by the office of the Ontario Information Privacy Commissioner (IPC) for the protection of the confidentiality of Personally Identifiable Information (PII). The application of encryption to protect non-metadata (email contents, file attachments, uploaded documents) is conceptually straightforward, either being supported natively in email clients, through software plugins for email clients, or in external applications.

The encryption of extrinsic metadata is more problematic than that of intrinsic metadata which is encrypted along with the document that it is associated with – extrinsic metadata needs to be intelligible to an online service for the purposes noted above – primarily delivery (in the case of email) and recovery (in the case of stored files). The threat of surveillance of source and destination metadata is one which will remain constant for all data save that which originates and remains entirely within the University of Toronto network – either the metadata could be surveilled at the service provider, or in transit to those destinations that are unable or unwilling to accept encrypted email transport connections.

Given the identified threats and vulnerabilities in email services, users of such services are advised to educate themselves, and those with whom they correspond, about ways in which encryption solutions may be used to protect email and other data while in transit, storage, use, and under administrative access – indeed, one should expect constant, ubiquitous surveillance and capture of unencrypted data on the Internet as the default state: "Surveillance is the business model of the Internet" – Bruce Schneier (http://edition.cnn.com/2013/11/20/opinion/schneier-stalker-economy/index.html). For text communications where both sender and recipient must remain anonymous, there are better (albeit not perfect) solutions than email.

Limitations

The general lack of products that encrypt data seamlessly and reliably across a variety of server and client platforms strongly limits the opportunities to protect data at rest in an outsourced solution. Outsource vendors seem generally unwilling to extend knowledge about planned service format changes to third-party encryption vendors – this limits these vendors' ability to prepare for such changes. Any changes to the interface of the online service may render encryption (and more importantly – decryption!)

inoperative until the encryption product is updated to navigate the new online format – potentially subjecting users to a service outage of days or weeks.

Beyond a general lack of encryption products, there are limitations as to how much encryption can protect; functions such as searching for, or within, documents will be unavailable without compromising the protection offered by encryption. An encrypted message could have a list of encrypted keywords extracted and attached to it to enable a limited form of searching. However, single encrypted words are trivial to decrypt and would give a good idea of the content of the email, even if the encrypted words were not in the order in which the email was composed (for example, an email with the encrypted words 'milk', 'bread', 'eggs' attached to it could reasonably be assumed to be a grocery list, even if the exact order of the words were unknown). Emerging technologies such as homomorphic encryption offer the ability to search for keywords within encrypted documents, however homomorphic encryption is still at a developmental stage, and does not yet offer this level of functionality.

Conclusion

Encryption, where possible and where products exist, improves the confidentiality and integrity of email messages, but is not a 'silver bullet' solution – shortcomings exist in the fundamental nature of encryption that introduce vulnerabilities that cannot be avoided without compromising service functionality. In support of this document's recommendation to apply encryption wherever possible, the University of Toronto is committed to identifying and adopting locally-controlled data encryption solutions; solutions that support the greatest amount of service functionality, compatible with the broadest cross-section of service users as transparently as possible.

Appendix P: Microsoft responses to security questions

Introduction

In the Office 365 Town Halls conducted by ITS in September and October, a number of questions were raised relating to the security of data – whether e-mail or documents – that would be stored in Microsoft's servers in the USA and would travel across the Internet.

Below is information provided by Microsoft regarding the issues raised. Our primary contact is John Weigelt, Microsoft Canada's National Technology Officer and the primary contact on matters of privacy and security. The responses that are provided below come from Brad Smith, General Counsel & Executive Vice President, Legal & Corporate Affairs, Microsoft.

1. Does Microsoft provide back-door access to its servers for USA security agencies?

- Enterprise Email and Document Storage: If we receive a government demand for data held by a business customer, we take steps to redirect the government to the customer directly, and we notify the customer unless we are legally prohibited from doing so. We have never provided any government with customer data from any of our business or government customers for national security purposes. In terms of criminal law enforcement requests, we made clear in our Law Enforcement Requests Report that throughout 2012 we only complied with four requests related to business or government customers. In three instances, we notified the customer of the demand and they asked us to produce the data. In the fourth case, the customer received the demand directly and asked Microsoft to produce the data. We do not provide any government with the ability to break the encryption used between our business customers and their data in the cloud, nor do we provide the government with the encryption keys.[46]

2. Are documents in Skydrive made available to governments?

- SkyDrive: We respond to legal government demands for data stored in SkyDrive in the same way. All providers of these types of storage services have always been under legal obligations to provide stored content when they receive proper legal demands. In 2013 we made changes to our processes to be able to continue to comply with an increasing number of legal demands of governments worldwide. None of these changes provided any government with direct access to SkyDrive. Nor did any of them change the fact that we still require governments to follow legal processes when requesting customer data. The process used for producing SkyDrive files is the same whether it is for a criminal search warrant or in response to a national security order, in the United States or elsewhere.

3. Are Skype calls made available to governments?

- Skype Calls: As with other services, we only respond to legal government demands, and we only comply with orders for requests about specific accounts or identifiers. The reporting last week made allegations about a specific change in 2012. We continue to enhance and evolve the Skype offerings and have made a number of improvements to the technical back-end for Skype, such as the 2012 move to in-house hosting of "supernodes" and the migration of much Skype IM traffic to servers in our data centers. These changes were not made to facilitate greater government access to audio, video, messaging or other

[46] 16 July 2013 – http://blogs.technet.com/b/microsoft_on_the_issues/archive/2013/07/16/responding-to-government-legal-demands-for-customer-data.aspx

customer data. Looking forward, as Internet-based voice and video communications increase, it is clear that governments will have an interest in using (or establishing) legal powers to secure access to this kind of content to investigate crimes or tackle terrorism. We therefore assume that all calls, whether over the Internet or by fixed line or mobile phone, will offer similar levels of privacy and security. Even in these circumstances Microsoft remains committed to responding only to valid legal demands for specific user account information. We will not provide governments with direct or unfettered access to customer data or encryption keys.

4. Does Microsoft route all traffic through the NSA for analysis?

- We only respond to requests for specific accounts and identifiers. There is no blanket or indiscriminate access to Microsoft's customer data. The aggregate data we have been able to publish shows clearly that only a tiny fraction – fractions of a percent – of our customers have ever been subject to a government demand related to criminal law or national security.

5. Is Microsoft collaborating with the US government in releasing private communications to intelligence agencies?

- To followers of technology issues, there are many days when Microsoft and Google stand apart. But today our two companies stand together. We both remain concerned with the Government's continued unwillingness to permit us to publish sufficient data relating to Foreign Intelligence Surveillance Act (FISA) orders.

- Each of our companies filed suit in June to address this issue. We believe we have a clear right under the U.S. Constitution to share more information with the public. The purpose of our litigation is to uphold this right so that we can disclose additional data….

- Over the past several weeks Microsoft and Google have pursued these talks in consultation with others across the technology sector. With the failure of our recent negotiations, we will move forward with litigation in the hope that the courts will uphold our right to speak more freely. And with a growing discussion on Capitol Hill, we hope Congress will continue to press for the right of technology companies to disclose relevant information in an appropriate way.

Transparency

Microsoft, and other cloud providers, issue publicly available transparency reports that show how many requests were received and filled by Microsoft in response to lawful data requests. From the latest 6-month report:

- Law enforcement sought information about only a tiny fraction of the millions of end users of our enterprise services, such as Office 365. We received 19 requests for e-mail accounts we host for enterprise customers, seeking information about 48 accounts. We disclosed customer data in response to five of those requests (4 content; 1 only non-content), and in all but one case, we were able to notify the customer. We rejected the request, found no responsive data, or redirected law enforcement to obtain the information from the customer directly in thirteen of those cases. One request is still pending.

- For all 19 enterprise requests, the legal demands were from law enforcement entities located in the U.S., and sought data about accounts associated with enterprise customers located in the United States. In addition, to date, Microsoft has not disclosed enterprise customer data in response to a government request issued pursuant to national security laws.

The U of T is an enterprise customer.

All of the 19 enterprise data requests were for enterprise customers located in the USA in response to USA-based government requests. Of those, five resulted in the release of data, and the customer was notified with one exception.

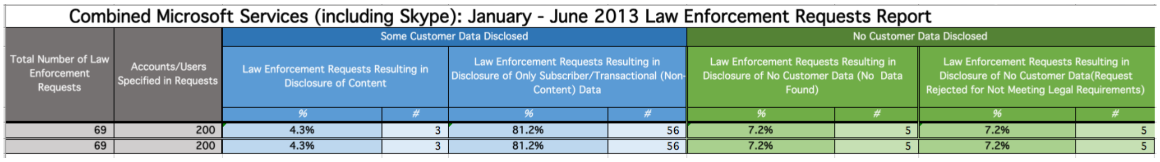
Transparency Reports

Transparency Reports are located at:

http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/#FAQ_Section

Country-by-country breakdowns are displayed in the report. Information for Canada, between January and June 2013 is extracted below in two sections – Microsoft Services and Skype:

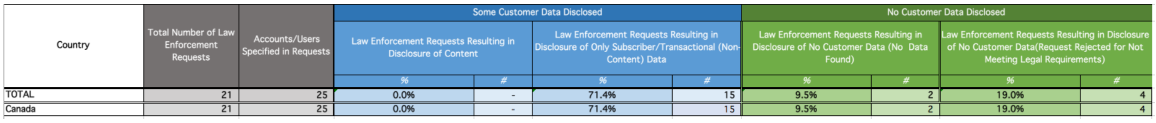
For Microsoft Services:



Combined Microsoft Services (including Skype): January - June 2013 Law Enforcement Requests Report

Total Number of Law Enforcement Requests	Accounts/Users Specified in Requests	Some Customer Data Disclosed				No Customer Data Disclosed			
		Law Enforcement Requests Resulting in Disclosure of Content		Law Enforcement Requests Resulting in Disclosure of Only Subscriber/Transactional (Non-Content) Data		Law Enforcement Requests Resulting in Disclosure of No Customer Data (No Data Found)		Law Enforcement Requests Resulting in Disclosure of No Customer Data(Request Rejected for Not Meeting Legal Requirements)	
		%	#	%	#	%	#	%	#
69	200	4.3%	3	81.2%	56	7.2%	5	7.2%	5
69	200	4.3%	3	81.2%	56	7.2%	5	7.2%	5

For Skype:



Country	Total Number of Law Enforcement Requests	Accounts/Users Specified in Requests	Some Customer Data Disclosed				No Customer Data Disclosed			
			Law Enforcement Requests Resulting in Disclosure of Content		Law Enforcement Requests Resulting in Disclosure of Only Subscriber/Transactional (Non-Content) Data		Law Enforcement Requests Resulting in Disclosure of No Customer Data (No Data Found)		Law Enforcement Requests Resulting in Disclosure of No Customer Data(Request Rejected for Not Meeting Legal Requirements)	
			%	#	%	#	%	#	%	#
TOTAL	21	25	0.0%	-	71.4%	15	9.5%	2	19.0%	4
Canada	21	25	0.0%	-	71.4%	15	9.5%	2	19.0%	4

References:

16 July 2013 – http://blogs.technet.com/b/microsoft_on_the_issues/archive/2013/07/16/responding-to-government-legal-demands-for-customer-data.aspx

Appendix Q: Other Universities' Experience

Other Canadian universities, and those of our standard Comparators, that offer faculty and staff e-communications services in the cloud

University	Current State
University of Alberta http://www.vpit.ualberta.ca/email/	Google Apps for Education for faculty, staff, students
Dalhousie University http://www.dal.ca/dept/its/its-services/Office365.html	Office 365 for faculty, staff, students
Ryerson University www.ryerson.ca/google/index.html	Google Apps for Education for faculty, staff, students
Nipissing University www.nipissingu.ca/departments/technology-services	Google Apps for Education for faculty, staff, students
U of Michigan http://safecomputing.umich.edu/protect-um-data/google.php	Google Apps for Education for students, faculty, staff, alumni
Ohio State https://ocio.osu.edu/blog/community/2013/08/15/making-connections-migrating-to-a-single-university-email-service/	Buckeye Mail – Office 365 for students, faculty and staff
University of Minnesota http://www.oit.umn.edu/google/	Google Apps for Education for faculty, staff, students
UC Berkeley http://ist.berkeley.edu/services/catalog/collab	Google Apps for Education for faculty, staff, students
U of Texas –Austin http://www.utexas.edu/its/email/FAQs	Gmail available to all

University	Current State
U Washington http://depts.washington.edu/uwtscat/googleapps	Google Apps, Office 365 – for faculty, staff, students, alumni – multiple options
U of Wisconsin - Madison http://www.365transition.wisc.edu/early-adoption-process-beginning-with-preview-tech-update/	Office 365 being rolled out to faculty, staff and students