Faculty and Staff eCommunications Advisory Committee

Final Report

11 August 2014

Background

For years, UTORmail was the principal email offering used by most faculty, staff, students and alumni across the University, but its static and limited features became apparent some time ago. Driven by demand to integrate mail and calendaring services, about a decade ago the University established a Microsoft Exchange-based server, UTORExchange, for academic administrators, most administrative staff and some faculty. Alongside several divisionally managed Exchange services, UTORExchange was an improvement, but its local infrastructure is aging, and it is plagued by unsatisfactory performance and incompatibilities for multi-device users.

Responding to student demand for more contemporary standards of service, in November 2009 the University initiated community consultation to identify student needs and solutions for email and other institution-provided e-communications services. An advisory committee consisting of students, staff working closely with students, and faculty, from all three campuses, was established.

In March 2010, with the Committee's first report in hand, the University decided to "actively and aggressively pursue the single course of determining the best features and costs possible in an outsourced solution for student email." Upon the recommendation of Procurement Services, it was decided to develop and release a public *Request for Information (RFI)* soliciting information from the supplier community on free outsourced options. Three submissions resulted, and the Committee reconvened to conduct an evaluation. It was also decided that in parallel with the detailed investigation of student email outsourcing, the Committee and IT staff should be sensitive to the implications on future options for managing employee e-communications. In September 2010, the recommendation of the CIO to pursue an agreement with Microsoft was accepted.

Details of each step in the student project's development are provided in the several reports and updates provided at the project Web site, http://main.its.utoronto.ca/about/committees/student-e-communications-consultation/#1110.

As a result of this agreement, since the summer of 2011, students and recent graduates have had access to the enhanced e-communications features of UTmail+, a service sponsored and administered by the University and hosted offsite by Microsoft. To date over 162,000 accounts have been created under the new service to great user satisfaction. Planning is underway to migrate prior alumni to UTmail+ from the e-communications service currently offered by Alumni Affairs. In the fall of 2013, the UTmail+ service was upgraded from Microsoft Live@edu to the even richer features of Microsoft Office 365 for Education.

This leaves faculty and staff served by the legacy offerings of UTORExchange, UTORmail and a number of departmentally or divisionally based email systems. The departure of most students, staff and alumni from UTORmail has left it with a user population consisting mostly of faculty. Like the students before them, these users are aggravated by limited quotas and out-of-date features, and are relying on a service that is at risk from aging hardware, and software that has no development path.

As noted, UTORExchange is also aging, and it is plagued by performance issues. While software licensing fees have recently diminished with the University's purchase of a Microsoft Campus Agreement, extending UTORExchange to all faculty would require renewal of all existing hardware, investment in additional hardware to accommodate the balance of faculty users, and growth of technician capacity to locally operate such an expanded service. By contrast the Microsoft hosted solution, Office 365 for Education, offers numerous other e-communications features (see below), requires no massive renewal of equipment, is sustainable with current staffing levels, and is free.

Consequently, the Vice-President and Provost asked the Chief Information Officer to develop a proposal to enhance faculty and staff e-communications services, aligned with the successful UTmail+ offering. While drawing upon the planning and implementation experience for the student/alumni service, the CIO has treated this project as independent, and sought information and advice from central ITS staff, IT staff in departments, divisions and campuses, academic and administrative leaders, and most importantly from faculty and staff users of e-communications services. One consultative vehicle has been the Faculty and Staff eCommunications Advisory Committee. This is the report of that Committee.

Committee Terms of Reference

The terms of reference of the Advisory Committee were:

1. To identify core expectations for enhanced faculty and staff e-communications services.
2. To identify obligations and concerns in matters such as the protection of privacy and information security, and review the adequacy of proposed service arrangements.
3. To recommend any variation in service provisioning required to satisfy the range of academic and administrative activities of faculty and staff.
4. To review the viability and adequacy of implementation plans.
5. To recommend future directions for e-communications services that reflect changing academic and co-curricular needs, enhanced student experience, and administrative requirements.

Committee Membership

The following individuals generously offered to participate in the consultation:

Michael Luke (Committee Chair)	Professor, Department of Physics
Kelly Lyons	Associate Professor, Faculty of Information
Cynthia Messenger	Senior Lecturer and Director Writing and Rhetoric Program, Innis College (until June 30, 2013)

Hugh Gunz	Professor of Organizational Behaviour and HR Management, Department of Management, UTM
Lisa Austin	Associate Professor, Centre for Innovation and Policy, Faculty of Law
Corey Goldman	Senior Lecturer, Department of Ecology & Evolutionary Biology, Associate Chair (Undergraduate Studies)
Don Boyes	Senior Lecturer, Department of Geography
Erin Jackson	Director, Central Administrative Human Resources
Helen Lasthiotakis	Assistant Dean & Director, Office of the Dean, Faculty of Arts and Science
Zoran Piljevic	Director, IITS, UTSC
Rosanne Lopers-Sweetman	CAO, Faculty of Kinesiology and Physical Education
Wes Robertson	Director, Discovery Commons, Faculty of Medicine
Robert Cook	Chief Information Officer
Assessors:	
Marden Paul Martin Loeffler Jeremy Graham	Director, PGAC and eCommunications Project Director, ITS Director, Information Security and Enterprise Architecture, ITS Operations Manager, Academic and Collaborative Technologies, ITS/CTSI

E-communications Requirements of Faculty and Staff

The consultation on student e-communications identified a wide range of needs and aspirations, drawn from experiences and functionality familiar to students from communications services available in their personal lives but not provided by the University. These are discussed in the first report of the Student Advisory Committee, available at: http://main.its.utoronto.ca/about/committees/student-e-communications-consultation/reports/#1196.

Requirements included:

- Increased service availability, greater data capacity, folder management, calendaring, handling rich media formats, group workspace, chat, global address book, file exchange and storage, improved search, integrated messaging;

- User-friendly interfaces;
- Service access anywhere/anytime;
- Multiple channels for communicating (e.g., Web, voice, instant messaging, email);
- Improved capabilities and operability with a variety of mobile devices; and
- Personalization of interface to individual preferences.

In addition students expressed a desire for:

- Enhanced security;
- Privacy protection;
- Freedom from data mining and advertising;
- Protections afforded by an institutional contract;
- e-literacy instruction in communications best practices:
- A uniform solution across all campuses; and
- Complementary services to accomplish tasks that are inappropriate for email, such as assignment submission, research data storage, etc.

When the Committee to advise on faculty and staff e-communications convened, it recognized a high correspondence between these student requirements and those of faculty and staff. To these common elements were added unique factors associated with the academic information (research data, discoveries and inventions, student grades and other assessments, advising, etc.) that faculty process and the privileged information administrative staff may receive, handle, transport and store. The Committee specifically noted the Tri-Council requirements for Privacy and Confidentiality, available at http://www.pre.ethics.gc.ca/eng/policy-politique/initiatives/tcps2-eptc2/chapter5-chapitre5#tphp.

The project's ***Information Risk and Risk Management*** **assessment (IRRM)**, available at http://main.its.utoronto.ca/about/committees/faculty-staff-ecommunications-consultation/faculty-staff-ecommunications-reports/, considers the specific responsibilities that the University and its employees have to protect Personally Identifiable Information (PII) as a requirement under the *Freedom of Information and Protection of Privacy Act* (*FIPPA*). But more generally, the IRRM is sensitive to the University community's interactions with a broad range of valuable information assets and their means of creation, use, transport, storage and destruction by faculty and staff.

The University's ***Information Security Guidelines***, available at http://main.its.utoronto.ca/wp-content/uploads/2013/07/Information-Security-Guidelines.pdf , anticipate this breadth of information and associated activity. Providing definitions for confidential and non-confidential information, and encouraging the categorization of information assets, the document presents a range of approaches to protecting sensitive data (including metadata) and records across their lifetime from creation to destruction. The document also links to specific solutions for data encryption.

In its assessment and recommendations, the Committee was informed by the special needs of faculty and staff e-communications, situated in the context of existing University commitments to information security. The recommendations to develop a range of services that map to the spectrum of data sensitivity, and to provide more robust encryption services arise from this consideration (see below).

Features of Office 365

The current offering of Office 365 for Education makes the following services and quotas available to the University for implementation. While support logistics and other considerations would require a staged introduction of specific services like videoconferencing or Sharepoint, faculty and staff subscribers could immediately experience dramatic service increases upon creation of their accounts.

Services include:

- Exchange 2013 – e-mail (Outlook 2013, Outlook Web Application--OWA), Calendar, Contacts, Tasks;
- Lync Communications – Instant messaging, Web meetings, future potential for Voice over IP, conference calls;
- Office Web-based Apps – Word, Excel, PowerPoint, One Note;
- Document sharing, synchronous editing;
- Excellent integration with PC/Mac-based Office applications;
- 50 GB mailbox + 1 TB OneDrive personal storage;
- 99.9% uptime guarantee – indirectly (on same platform as for those who pay);
- Spam and malware filtering.

Users who prefer to use a different e-mail client, e.g., Thunderbird, IMAP or POP mail clients, would be able to continue to do so. Depending on the email client used, there might be some reduction in functionality as compared to Outlook.

In addition to these user-facing benefits, the service would also provide certain back office advantages, such as: uptime guarantees, service continuity assurance through geographically dispersed redundancy, improved security (physical security, encryption of data-in-transit and at-rest), accountability and security audit compliance reports.

Additional Service Considerations

In addition to the above features, the Committee understood that faculty and staff subscribers to Office 365 would enjoy the following experience, analogous to the current experience under the student service:

- Faculty and staff email addresses would continue to be their current @utoronto.ca addresses, and the option to retain subdomain addresses such as dept.utoronto.ca;
- There would be no advertising for faculty, staff, students or alumni;
- Faculty and staff use of the Microsoft service would be governed by an agreement between the University and Microsoft, which provides greater protection than individual consumer agreements;
- Microsoft clearly states that they have no ownership claim on data provided by users. Current University practices regarding ownership and administrative access to data would

continue;

- Microsoft would provide tools to University system administrators for incident management;
- Microsoft would perform no data mining on customer data and metadata[1];
- Authentication credentials to access Office 365 would be managed locally by the University;
- Microsoft would make available to the University, SAS 70 Type 2 (industry standard) internal controls compliance reports;
- Microsoft is ISO27001 compliant and is annually audited. ISO27001 is a standard for Information System Security Management; and
- Data would be encrypted in transit between the University and Microsoft, at-rest in Microsoft servers, and during 2014, in transit between Microsoft data centres at an increased level of encryption than previously.

Committee Deliberations and Consultations

The Committee met six times (April, 5, May 30, June 21, September 6, Oct 25, 2013, and January 9, 2014). Members had access to the project Web site for the student eCommunications renewal project, http://email.utoronto.ca/?page_id=20, which includes all of its reports.

The Committee reviewed the results of the extensive community consultation that had occurred during the development of the student e-communications solution, that included not only ideas and concerns from students, but also staff and faculty comments on both student services and their own as well.

The Committee also heard the results of the consultation that has occurred among ITS staff and various faculty and staff communities of interest. These include the Provost's Advisory Group, PDAD&C, the IT "Middle Tables" (consisting of the Process and Technology Committee and the Priorities and Accountability Committee), UTFA Executive Council, UTSC and UTM senior administrative tables, IT Leaders Forum, the committee of Faculty of Arts & Science department IT managers, the Faculty of Arts and Science business officers, as well as comments from a number of individual staff and faculty members. The Committee specifically noted that letters were sent to the Vice-President and Provost from the Faculties of Law and Information, the Departments of Geography and History, and the Centre for Criminology and Sociolegal Studies, expressing concern about the risks of hosting data in the USA.

Members discussed a number of issues and concerns with respect to the adoption of Office 365 as discussed below. The Committee also advocated creation of an informational Web site for the proposed project, and other efforts to alert the staff and faculty communities. It can be found at:

http://main.its.utoronto.ca/about/committees/faculty-staff-ecommunications-consultation/#1108

The Committee suggested that open forums be held on our three campuses to present information about the proposed project and solicit additional feedback from interested members of faculty and staff. Memos regarding the town hall meetings were sent via email to divisional IT leaders,

[1] For operational purposes. Microsoft may use service and traffic data to analyze service performance, or for instance, to identify patterns that indicate denial of service attacks.

campus CAOs, and divisional and campus academic leaders. Those consultations occurred as follows:

- **University of Toronto Scarborough (UTSC)**
  Monday, September 23, 2013, and Thursday, October 10, 2013
- **University of Toronto Downtown**
  Tuesday, September 24, 2013, and Wednesday, October 9, 2013
- **University of Toronto Mississauga (UTM)**
  Wednesday, September 25, 2013, and Monday, October 7, 2013

Much of the information presented to the Committee, the insights of the members themselves, and comments at the town halls clustered around a number of themes that bore strong resemblance to the issues and priorities identified in the student project:

- The inadequacy of existing e-communications services;
- The risk to the University and its students from the practice of individual faculty and staff using cloud services to conduct academic and administrative activity without the protection of an overarching contract between the University and the supplier;
- Desired features in e-communications services (e.g., improved functionality, availability, capacity, calendaring, group workspace, global address book, file exchange and storage, improved search, rich media handling, multi-channel access, integration with other University services, integration with third party services…);
- Privacy and security concerns, specifically the impact of the USA PATRIOT Act, PRISM, MUSCULAR, and Canadian and foreign government agency surveillance;
- Special considerations for the types of data and metadata faculty communicate via University services;
- Questions about alternatives to Office 365, whether locally or externally provided;
- Expectations around the security of the University's e-communications services, including FIPPA, PHIPA and PIPEDA compliance;
- Local identity as supported by subdomains (e.g. @math.utoronto.ca, @rotman.utoronto.ca);
- An option for academic units that may wish to continue to support locally operated communication servers;
- Requirement to educate staff and faculty in email best practices, especially around security;
- Expectations regarding the reliability of the provided services and support services for issues management;
- Expectations regarding equality of services for both Mac and Windows OS users, as well as compatibility with Linux systems.

The Committee reviewed and discussed the Office 365 features and service understandings, and whether Office 365 would meet the identified needs. Several matters for further discussion and review were identified, and are presented below.

Privacy and Security

The Committee spent much time discussing the privacy and security provisions of the proposed Microsoft service. During the period of the Committee's work, new risks associated with the revelations that US and Canadian intelligence agencies engage in surveillance of data and metadata on the Internet came to dominate the Committee's considerations. Privacy considerations were a prevalent issue discussed in several of the town hall meetings, and communications from a number of individual faculty as well as the previously noted faculties and departments were shared with the Committee.

In light of these issues, the Committee spent considerable time seeking to understand the risk in the University's current practice as well as the risk of the proposed solution in order to assess what increase or decrease in risk the migration might bring.

Staff in the Information Security and Enterprise Architecture department of ITS, in consultation with the University's Freedom of Information and Protection of Privacy Office, undertook a rigorous ***Information Risk and Risk Management*** (IRRM) assessment, incorporating both a Privacy Impact Assessment and a Threat/Risk Assessment of the proposed service. The IRRM is organized around *Privacy by Design Framework and Foundational Principles* of the Information & Privacy Commissioner of Ontario from whose office University staff sought guidance in this project. The IRRM was augmented in response to questions raised by the Committee and consultations with the University community.

The Committee discussed the risks associated with the proposed solution, many of which are common to our current practice and any other solution that would connect to the Internet. In particular, email – whether hosted locally or in the cloud – is fundamentally an insecure communications channel, not designed with security foremost. It is not uncommon practice to send personally identifiable information and other sensitive information via email, even when these messages leave the presumed security of internal email services such as UTORmail and UTORExchange. Recognized as well, were the risks associated with running 75 or more email systems across the campuses each with potentially varying levels of maintenance and security.

The Committee noted that the University's communications activity is not just with members of our internal community, but ranges across Canada, into the USA, and around the world:

- From an analysis of UTOR email services the Committee learned: 91% of faculty and staff using UTOR email services access their email from outside the University's secure network (via cellphones, home and hotel services, etc.), exposing content and metadata to risks across the broader Internet and to potential transborder data flow. The Committee recognized in this context that it is the nature of the University's academics to interact internationally.
- To better understand the movement of information, data for UTORemail services for the week of 17-24 November 2013 was reviewed, and illustrated the following:
    - Of all sent messages (plus messages received by but then automatically forwarded outside UTOR email services), 38% stayed within UTORservices or other U of T departmental services, and 62% went outside U of T (made up of 18% to students at UTmail+ and 44% to the broader Internet.)

- Of all received messages (excluding those received by but then automatically forwarded outside UTOR email services), 19% were from within UTORservices or other UT departmental services, and 81% were from outside U of T (made up of 2% from students at UTmail+ and 79% from the broader Internet).

The Committee also heard that many faculty and staff create an undocumented increase in risk for the University through the practice of entering personal agreements for cloud services. DropBox, Google Docs, Facebook, Gmail, CoursePeer and many others are then used to conduct University academic and administrative business, without a security assessment, or the protections such as no advertising, no data mining, and no claim to content, that would be available under a U of T contract for O365.

The Director of Information Security & Enterprise Assessment, in his remarks to the Committee, was clear that Microsoft was better positioned through its superior resources availability at preventing unauthorized access from hackers, plus better able to provide business continuity given the services architecture of geographically dispersed data redundancy.

In light of the recent revelations about security, the Committee considered:

- To what degree does removing data storage from on-premises at the University increase the risk of unauthorized access to data and metadata?
- Does moving data offshore expose data and metadata to foreign law that affords a range of uses and intelligence surveillance not permitted by Ontario and Canadian law?
- Can the University satisfy its FIPPA obligations if its service provider must comply with contradictory foreign law?

All of these risks are identified and discussed in the IRRM assessment.

Risk Mitigation

In considering these risks, the Committee explored what strategies could be adopted to reduce negative impact such as data loss or unauthorized access or monitoring of data and metadata. In addition to practices to enhance security listed earlier, the Committee considered (and will recommend below) a number of measures:

1. A University managed encryption service in which keys are held in an on-premises service. Encryption could be compulsory for classes of users or content, and made available upon request to any user. This would provide a dramatic improvement in security over current practice;
2. Provision of a spectrum of University managed data services suitable to the escalating sensitivity of data being handled, in particular allowing the secure transfer of documents within the University without the need to use email;
3. Local (U of T side) processing of credentials (as is currently the case for the student/alumni service) such that ID and password are not provided to Microsoft;

4. An option so that individual faculty may opt out to an institutional, on-premises e-mail service but with less capacity and with fewer capabilities than Office 365. The service would be akin to the existing UTOR e-mail services; and
5. A program of community education as to the risks and best practices in e-communications.

Summary of Privacy and Security Issues

Security and privacy threats arise in many different ways, from careless password practices to malicious hackers to inconsistent systems maintenance. While risk is widespread, revelations in the last year have focused attention on state-sponsored data and metadata surveillance, and this dominated the Committee's deliberations.

The Committee acknowledged the risks associated with implementing Office 365 with data centres located in the United States, or more generally, in a location where data may traverse international borders.

But Committee members also asked if the collection of risks from US-based hosting should be balanced against the risks currently at play, the proportion of risk that may be mitigated with the application of various technologies and contractual agreements, and the likelihood of defined risks affecting members of the community – while noting that in an evolving world of technology, politics, and security, it may not be possible to provide an exhaustive analysis of the risks, nor an exhaustive set of mitigations to provide certainty and zero risk around all issues.

In its deliberations, the Committee weighed many factors:

- Email is fundamentally insecure, whether locally or remotely hosted;
- Most of our email traffic is already outside U of T networks;
- The international nature of communication and collaboration requires transborder data flow. Data cannot remain within one nation's boundaries;
- Attempts to access data lawfully and unlawfully occur in most countries, for security purposes, political purposes, commercial and industrial purposes;
- Hackers and other malicious agents pose a real security risk which is at least as compelling as state surveillance programs;
- Our status quo is not an option as communications services available to the broader community far exceed the scale and capacity of University-provided systems;
- That alternative communication and collaboration solutions, offered at a cost and scale approaching those offered in Office 365 did not exist. Alternatives that addressed the US hosting issues were either expensive, did not resolve data travelling over the Internet and potentially crossing national borders, or did not offer the range of services available in Office 365;
- The guidance received from the Ontario Privacy Commissioner's Office in assessing risk, embedding privacy practices in our approach, providing opt-out, while at the same time recognizing the reality and value of outsourcing options;

- Implementation of the risk mitigation strategies as noted above are essential to creating the best case for securing data and preserving privacy.

Recognizing that the majority of external threats to security are of the unlawful kind, the Director, Information Security & Enterprise Architecture concluded that the risk to confidentiality, integrity, and availability of data – while not absent in any context – is considerably lower in Office 365 than in a University-hosted service. After extensive internal discussion, the majority of the Committee accepted these conclusions.

Other Issues

Investigation of Office 365 Alternatives

Although the mandate of the Committee was to assess the viability of extending to faculty and staff the Microsoft cloud solution embraced by students and alumni, the Committee asked for information about alternative solutions and their costs. ITS staff presented information on three models:

- An in-Canada, commercially-hosted Exchange service for e-mail and calendaring only
- A private email and calendaring service developed at another Canadian university
- Internal hosting of email and calendaring only.

The costs associated with these basic solutions ranged from $1,000,000 to $2,500,000 annually with some having significant one-time-only setup costs.

The alternative solutions provide a hosted-in-Canada solution, though the Committee was advised that data do not necessarily remain in Canada, and more importantly relative to communications over the public Internet, inside the University's network.

The in-Canada, Outlook solutions were based on carrier-grade vendors, and costs were about $5/month/person. Targeting only the faculty and staff, estimated at 20,000 accounts, yielded an annual cost of $1.2 million.[2]

The in-Canada, non-Outlook solutions were less expensive but would not achieve the functional benefits of a common communications and collaboration suite, or take advantage of the existing expertise and experience with Outlook, Exchange, and the current student offering.

The local hosting estimates were generated by industry standard estimation tools by the ITS staff who currently provide the configuration and operational support to UTORservices. It was noted that to be remotely comparable to the uptime and continuity offered in Office 365, at least two hardware configurations in separate locations and hot-synced would be required. Round-the-clock Exchange, intrusion and attack, and hardware support staff would also be required, and

[2] Estimates were based on 5-10 GB mailbox, Outlook e-mail and calendar only. Estimates do not include students or alumni. Their addition would increase annual costs proportionally. It should be noted that the cost estimates were produced outside of an RFP. It could be expected that an increased number of users would reduce the per person costs. The non-Exchange costs with a non carrier-class provider were lower, but the trade-off would be a non-standard e-mail system that would differ from the service offered to the students. Were students included, it would mean a migration to a service with lesser functionally.

these resources would be scaled to a service 20-times larger than the existing UTORExchange configuration. This estimate would only cover e-mail and calendaring, not the other services available through Office 365.

Continuation of local email systems

While the proposed Office 365 service provides multiple features beyond current email and calendaring offerings at the University, it may be that the departments, divisions or other units currently operating independent email systems wish to continue their local services and bear the staffing, equipment and other costs of their operation. The Committee supported the idea of permitting continued operation of local email solutions.

Maintaining local subdomains

There are a number of instances across the university where departments or divisions have chosen to identify their community users by use of a designator subdomain: e.g., @utsc.utoronto.ca. ITS has confirmed that our implementation of Office 365 service would be technically able to sustain subdomains. Consequently, the Committee recommended that the subdomain option be made available.

Implementation roadmap

While migration of student UTORmail users to UTmail+ was relatively easy, with a very common experience shared among most migrating students, the Committee recognized that faculty and staff migration may share fewer common elements among users, and may require more time and substantially more individual support. In anticipation of this, ITS and Information Commons staff have been working to orient distributed IT support units to possible requirements, and developing resources to support those migrations. The Committee supported an ITS staff recommendation that if the project proceeds, migration be done by cohort (whether departmental, research centre, or by other common characteristic), to enhance availability of support resources. The migration plan should be clear on all anticipated issues, how issues will be managed, the interface between local and central supports, the way in which issues will be escalated in order to be resolved, and service level expectations for users who encounter problems.

Staff have recommended staging migration of staff and faculty cohorts over a ten to twelve month period, starting with those groups most eager to get going. The Committee supported this staged implementation approach.

Faculty who do not wish to migrate to Microsoft service

Consultations suggest there are likely members of the University community who would not want to locate their professional email in the US cloud, or with Microsoft in particular. While it is expected the majority of users will be satisfied with the University's assessment of security and privacy provisions, and the increased functionality and availability, it is proposed that faculty who do not wish to use Office 365 services be given access to an alternative, University-operated email system that would have functionality analogous to that of the existing UTORservices. They would maintain their @utoronto.ca address, but would be unable to participate in the collaborative service of Office 365. A decision to use a University-operated email system will not preclude the ability of individuals to migrate to Office 365 at a later date.

There was consensus in the discussions that staff should be required to migrate to the enterprise solution when it is their cohort's time, and not be given the individual option of remaining in the legacy-like environment.

Premier services required by some users

The Committee recognized that faculty and staff users may have differing requirements for e-communications services. While the base, free, offering under the Microsoft Office 365 for Education plan is far beyond the scope and volume of service offered by current University-wide services, it may be that some users will require additional capacity or features. (The Committee noted that such exceptional demand has likely diminished during the course of project planning. The new Microsoft Campus Agreement implemented in the spring of 2013 provides access to common software resources – see https://microsoft.utoronto.ca for more information. Microsoft has also expanded the features or caps on the free offering at least three times.) One advantage of the Office 365 service is that it offers additional, premier services for additional cost. The Committee was of the view that while any operational costs associated with the basic service should be borne centrally by the university, these optional premier service costs should be the responsibility of the individual user or their department.

Should users require service beyond the level of even Microsoft's premier offerings, they will have the opportunity to make those additional arrangements themselves or at the department level.

Need for e-communications training

In addition to discussing the technical arrangements in place to reduce risk in the areas of security and privacy, the Committee recognized that pro-active communication and training in best-practices in the use of electronic communications will be an important component of protecting the information assets handled by faculty and staff. The Committee encouraged the Director of Information Security and Enterprise Architecture to develop a multi-channel training strategy for faculty and staff as well as student communities.

Recommendations

The Committee agreed that email and calendaring should be the first services made available with the expectation that further analysis of the implications, value, risks etc. of additional services would be conducted before the decision were made to role each one out. Factors to assess would include not only privacy risks, but also help desk capacity to support additional services, and alignment or interface with other services like institutional videoconferencing and voice communications. An agreement with Microsoft would make the full suite of O365 services available to the University to deploy; but as with the student implementation, the decision on which services to release to users would rest with the University.

In providing Microsoft service to our students, the University of Toronto was not the first institution to adopt an outsourced, and free, communication and collaboration suite. The majority of our key comparators in the USA have adopted Microsoft's Office 365 or Google Apps for

Education. In Canada, adoption has been slower, but the University of Alberta, Ryerson, Dalhousie and Lakehead have adopted cloud services for their entire community of students, staff and faculty, and many other schools have adopted the suites for their students and alumni. (See the project's IRRM, Appendix Q at http://main.its.utoronto.ca/about/committees/faculty-staff-ecommunications-consultation/faculty-staff-ecommunications-reports/) The rationale for adoption, even in light of the Snowden allegations, is to attain an excellent set of communication and collaboration services for their faculty, staff and students, at a scale far beyond anything possible to be provided locally. The physical data security, malware and virus protection, access to the enterprise resources of these firms, and business continuity protection, provide their communities with the communications functionality they require and deserve.

From the inception of this project, the protection of data and privacy has received significant attention. The IRRM assessment continues to be revised as privacy concerns not already addresses are raised during consultations, and in response to the new revelations from the Snowden papers.

The Committee, supported by ITS staff, has worked to address issues raised through the extensive consultations. Consultation with the IPC and adoption of the *Privacy by Design Framework*, have been essential in understanding and responding to the identified risks.

Committee members also looked at the American Association of University Professors report, *Academic Freedom and Electronic Communications* http://www.aaup.org/file/AcademicFreedomandElectronicCommunications.pdf for an academic viewpoint on communication and collaboration services, and their perspective on outsourcing applying a faculty member lens. The AAUP report identifies eight key actions to perform when considering an outsourcing arrangement, and as is the case with *Privacy By Design*, U of T has addressed the project in a manner consistent with their principles[3]

The Committee achieved general agreement in many areas of its consideration:

- the inadequacy of our current tools to meet faculty and staff needs
- the advantage of providing better e-communications features to support world-class scholarship and administration

[3] *1. The institution should formally involve faculty in decisions to outsource core electronic communications technologies.*

2. The process of selecting an outside provider selection must involve the consideration of factors other than price, including institutional needs, legal and ethical obligations, and the norms and mission of the institution.

3. IT leadership should carefully evaluate the outside provider's ability to access content and electronic traffic data. It is important to note that even if a provider promises not to provide usage data to advertisers, that promise does not foreclose analysis of electronic communications data for other purposes, including commercial purposes. An agreement should be reached in advance with the outside provider to prohibit the sharing of such data with commercial interests.

4. Faculty should encourage campus IT leadership to collaborate with other institutions in jointly identifying problems and mitigating risks.

5. IT leadership should carefully evaluate the outside provider's uses, processing, and analysis of user content and transactional data. All uses of data should be reviewed by the institution and specifically authorized.

6. IT leadership should follow policy decisions and changes of outsource providers, and notify faculty when these decisions implicate governance issues.

7. IT leadership should consider technical approaches to reduce lock-in to outside providers and, where possible, to mask content and traffic data from these providers.

8. Contracts with outside vendors of electronic communications services should explicitly reflect and be consistent with internal institutional policies regarding such communications and with applicable federal and state laws.

- the imminent risk of failure of our current services
- the risk in our community's current practice of making individual arrangements for cloud services
- Office 365's enhanced security with regard to conventional threats by hackers and data thieves
- the lower cost advantage of implementing Office 365.

The Committee also achieved general agreement on the threat to privacy and personal freedom represented by the ungoverned activity of American, Canadian and other intelligence gathering agencies. Where the Committee differed was predominantly in how to respond to that threat.

The Committee debated whether government intelligence-gathering threats to privacy create an unacceptable risk in adopting a US-based cloud service like Office 365; or whether that risk can be mitigated and then evaluated alongside the advantages that Office 365 would offer. The majority of Committee members concluded that by taking specific actions related to data encryption, opt-out provisions, and user education in best email practices, the risk can be reduced to an acceptable level and the benefits of adopting Office 365, such as features, cost, conventional security, and reduction of risk from existing practices can be realized. The majority concluded that tangible benefits to the community outweigh the risks, and the mitigating actions will further increase confidence in the recommended approach. A minority of the Committee, however, felt that in the absence of more extensive exploration of alternatives, it is not in the best interest of the university to proceed with negotiating an agreement with Microsoft at this time, and hence did not support the following recommendations.

The recommendations supported by a majority of the Committee members are:

Overall Recommendation:

1. That the University of Toronto proceed to negotiate an agreement with Microsoft to extend UTmail+ services to faculty and staff, through a staged implementation of *Office 365 for Education* starting with email and calendaring, followed by other services if and when considered appropriate.

Specific Recommendations

2. That the University of Toronto express its opposition to the practices of Canadian, US and other foreign intelligence services in their wholesale implementation of data and metadata surveillance, and call for the legislation of rigorous oversight by elected representatives;
3. That the University develop and offer a university managed encryption service in which keys are held in an on-premises service. Encryption could be compulsory for classes of users or classes of content, and made available upon request to any user;
4. That the university develop and offer a spectrum of university managed data services (likely on-premises) suitable to the escalating sensitivity of data being handled, including

a secure, locally hosted means of transferring sensitive files within the university system without the use of email;

5. That departments, divisions or other units wishing to continue operation of local email services shall be permitted to do so within the utoronto.ca domain;
6. That departments or divisions wishing to identify their community of users with a designator subdomain shall be supported in Office 365;
7. That the implementation of the Office 365 service be initiated as soon as an agreement with Microsoft is reached, and that migration occur by cohorts of faculty and or staff, identified by affinity groupings of manageable size;
8. That ITS maintain an on-premises email service with features analogous to the current UTOR services for individual faculty members who do not wish to migrate to Office 365;
9. That any costs associated with the addition of premier services beyond the free offering of Office 365 for Education be borne at the departmental or unit level; and
10. That concurrent with the roll out of Office 365, ITS develop a program of communications and training to promote best practices in the use of various e-communications channels by faculty, staff, students and alumni.

The report and recommendations of Committee members who did not support these recommendations are found in the Appendix that follows. The report and recommendations presented in the Appendix have not been revised or endorsed by the full Committee.

Minority Report

We thank the other committee members for their thoughtful discussions, and the staff at the CIO's office for responding to many requests for information and clarification.

There are many things that we agree with in the committee's report (hereafter referred to as the *majority report*), including the assessment that O365, on technical grounds, is a good product that would meet faculty and staff email and calendar needs. We do not in principle object to outsourcing our email and calendaring, nor do we in principle object to cloud computing solutions. It is not entirely clear how urgent or universal the need is for moving from the current data services infrastructure, though it is understood that many faculty and staff are attracted by the features of O365 that have now been made available to students and alumni.

Our concerns are prompted by the Snowden revelations. As a result of these revelations we now have ample information in the public sphere that points to the need to secure our communications against various forms of state surveillance. We are pleased that the committee as a whole has agreed that these risks are such that we cannot at this time recommend the adoption of features of O365 such as integrated communications or document storage. However, as outlined below, the committee has heard numerous arguments that we can better protect our communications against state surveillance if we either provide our email in-house or use a Canadian provider. We would like to see the University fully explore these options.

The committee also heard many concerns regarding the absence of a full cost/benefit analysis for the O365 proposal as well as requests from a number of concerned stakeholders that the University proceed with caution and explore alternatives. These concerns about process are underscored by the fact that the public consultation process on campus proceeded on the basis of an Information Risk and Risk Management Report (IRRM) that did not address the issue of state surveillance practices post-Snowden at all, and did not discuss encryption solutions. It is important that this decision not only be the right one but that the process to arrive at any decision should also be "done right."

In the absence of fully exploring alternatives, we feel it is not in the best interest of the University to proceed with negotiating a contract with Microsoft at this time. Therefore, we cannot support the main recommendation in the majority report of the committee. We propose two recommendations below.

Lisa M. Austin, Faculty of Law
Corey A. Goldman, Faculty of Arts and Science
Rosanne Lopers-Sweetman, Faculty of Kinesiology and Physical Education
Kelly Lyons, Faculty of Information

Recommendations

1. That the University of Toronto not negotiate at the present time an agreement with Microsoft to extend UTmail+ (Office 365 for Education) services to faculty and staff.

2. Given the risks and uncertainties associated with a US-based outsourcing of its e-communication services for faculty and staff, that the University of Toronto conduct a thorough and transparent analysis of its e-communication needs and of all potentially viable alternatives to US-based outsourcing.

Assessing the Risks

The majority report accepts that the privacy risks associated with outsourcing are significant enough that we should not adopt any of the features of O365 apart from email and calendaring. This exception to email/calendaring rests on several arguments. The most significant include the view that email is "fundamentally insecure" and the conclusion of the IRRM report that "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."[1] However, during its consultations the committee has heard many arguments regarding the limitations of these arguments. Dean Seamus Ross, of the Faculty of Information, went so far as to write to the committee that "[t]he fact that the Information Risk and Risk Management Report does not, in my opinion, adequately address, let alone grapple with, the concerns raised by the community is a cause for anxiety."[2]

Drawing upon what we heard during our consultations and meetings, there are a number of important considerations that lead us to conclude that it is in the best interest of the University to more fully explore alternatives. We summarize these considerations below.

Email is a core communicative activity of the University.

- Email has been widely adopted across all significant areas of contemporary organizational life and become critical to effective daily operation.
- Email communication is absolutely central to the teaching, research, and administrative functions of the University. It is the official mode of communication at the University and, in storage, forms a vast institutional archive.

There are aspects of email that can be made secure.

- The majority report states that email is fundamentally insecure. Email can be made more secure, including in a variety of ways that do not depend upon the individual choices and actions of users.[3]
- According to the U of T email traffic data provided to the committee, at least 56% of our email remains *within* the University of Toronto community. [4] This email (a majority of U of T email traffic) can be made very secure through transport layer security of the kind commonly deployed for online banking.
- Over 90% of faculty and staff access their email remotely (through phones, home computers, etc.). These connections can also be made very secure through transport layer security of the kind commonly deployed for online banking.
- Forms of end-to-end encryption (like PGP) allow individual users to identify particular email messages and encrypt their contents (but not the associated metadata).
- Email can also be made secure in storage.
- Laws can also make data secure. Even if information is easily accessible as a matter of fact, that does not mean that it is lawful to either collect it or share it, either for private entities or the state.[5]

[1] See IRRM (October 29, 2013), Appendix A, p. 25.

[2] Letter from Seamus Ross, Dean of the Faculty of Information (January 9, 2014).

[3] This information is based upon conversations with two experts in communications security: Dr. Ian Goldberg (Associate Professor and University Research Chair, Cheriton School of Computer Science, University of Waterloo) and Paul Wouters (Red Hat, ICANN, The Libreswan Project), both of whom attended "Teach-in on University e-Services Outsourcing to U.S. Corporations" at the Faculty of Information, November 16, 2013.

[4] These numbers are from the University's *second* study of email traffic patterns: see *UTORservices traffic patterns Nov 2013*. 18% of sent messages from UTOR email went to students. This email currently travels to the US as a result of student email already having been outsourced, but otherwise would not. All of these numbers are also based on UTOR email services so does not include the number/destination of emails sent from other UT departmental email services or from students at UTmail+.

[5] As the Supreme Court of Canada recently stated: "It goes without saying that by appearing in public, an individual does not automatically forfeit his or her interest in retaining control over the personal information which is thereby exposed. This is especially true given the developments in technology that make it possible for personal information to be recorded with ease, distributed to an almost infinite audience, and stored indefinitely." *Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401*, 2013 SCC 62 at para. 27.

There are significant legal differences between the US and Canada.

- The important legal issue is not *whether* state authorities can gain access to data, but *according to which standards*. It is quite clear that Canadians have a much higher level of legal privacy protection for their data when it is in Canada than when it is in the United States.[6]
- Even though Canadian authorities may share data with authorities in the United States, the terms of both their collection and their sharing are subject to Canadian law, which is more protective of privacy rights of Canadians and Canadian residents.
- Although Canadian telecoms are permitted to share customer data with law enforcement and national security agencies, in the absence of a court order this is discretionary. Organizations like U of T can enter into agreements to prevent this.[7]
- Stephanie Perrin, former Director of Privacy Policy at Industry Canada and currently a data protection expert advising ICANN, wrote to the committee stating that, despite some of the inadequacies of Canadian oversight mechanisms, including weak commissioners, we continue to have oversight here that is denied to us, as non-US persons, once our data are in the United States.[8]
- Even if Canada is engaged in *illegal* activities, as current news reports suggest, the issue of whether an activity amounts to lawful or illegal surveillance impacts the effectiveness of various mitigation strategies (see below).

Privacy risks vary considerably across jurisdiction, geography and communication channel.

- The risk of state surveillance varies depending on jurisdiction, geography and communication channel.[9]
- Privacy risks need to be addressed separately in relation to: 1) remotely accessing our email, 2) sending email within the University of Toronto community, 3) sending email to non-University of Toronto community members, 4) sending or routing email outside Canada, and 5) storing our email.
- Because the students are already using O365, we need to also assess our communication risks in light of all of our communications with students being routed to the U.S. and stored there. In fact, we should more generally re-assess student privacy risks.

The cost and effectiveness of various mitigation strategies vary considerably depending upon type of information, jurisdiction, geography, and communication channel.

Some examples (this is not meant to be comprehensive):

- As Stephanie Perrin pointed out to the committee, security breaches and lawful access are more difficult to detect once our data are offshore, and mitigation strategies are more difficult to ensure.[10]
- The IRRM report proposes end-to-end encryption, such as PGP, as a mitigation strategy, which allows individuals to selectively encrypt the contents of particular emails; and the use of which does not require providing Microsoft with the "keys". However, this does not protect metadata and diminishes the ease of use and functionality of software-as-a-service.[11] It also raises questions about whether

[6] See: Letter from Professor Austin to Commissioner Cavoukian (October 8, 2103); Editorial from Canadian Privacy Law experts, "Our Data Our Laws" (National Post, December 12, 2013); Letter from the members of the Faculty of Law (December 20, 2013).

[7] See Canada's *Personal Information Protection and Electronics Documents Act,* S.C. 2000, c.5, s.7 (PIPEDA).

[8] Letter from Stephanie Perrin (January 8, 2014). ICANN is the Internet Corporation for Assigned Names and Numbers. It is the non-profit global body responsible for, in effect, the address book of the Internet.

[9] See: Memo from Professor Austin (October 17, 2013); Letter from Professor Clement to Commissioner Cavoukian (October 24, 2013); Email from Professor Clement (January 9, 2014); Letter from Stephanie Perrin (January 8, 2014).

[10] Email from Stephanie Perrin (January 8, 2014).

[11] Caspar Bowden's remarks at "Teach-in on University e-Services Outsourcing to U.S. Corporations," Faculty of Information, November 16, 2013.

users can learn to use this and whether relying upon individual habits in this way ensures privacy and security practices as an institutional default.

- Transport-layer encryption (like that used to secure online banking) can protect the connection between individual user and the server, such as when individuals remotely access their email. However, whoever provides this encryption can be legally compelled to cooperate with state authorities and decrypt. Therefore legal jurisdiction is important to the effectiveness of such a mitigation strategy.

The risk is not low.

- Snowden's revelations of programs like MUSCULAR show that the NSA has targeted the data centres of large internet companies without their knowledge or cooperation.[12]
- Microsoft has provided assurances that the customer data of their enterprise customers has never been disclosed for national security purposes. However, despite being requested, they have not officially confirmed that this includes metadata and traffic data. Therefore some of this information may have been disclosed. As the committee heard, metadata can be as revealing as content data.[13]
- There is no law reform proposal on the table in the US that prevents the bulk collection of data associated with non-US persons. To the contrary, we have every indication that the NSA believes that it must collect the "haystack" in order to find the "needle".
- Even if the average personal risk, aggregated over all individuals potentially affected, is not large, given the nature of what happens to people who do get caught in a state security net, the consequences can be devastating.
- The *nature* of the risk is also important. Under FIPPA, the University is prohibited from disclosing our communications data to US authorities of any kind.[14] This ensures that US authorities must seek the cooperation of Canadian authorities for access to our data, and those Canadian authorities are bound by the Canadian constitution. The risk that our data can be accessed on standards that fall far below Canadian constitutional standards is not simply a "cost" with the same status as other costs and benefits to be balanced in this proposal – our constitution provides us with the basic framework that tells us how to weigh and balance costs and benefits.

Institutional Leadership

The University needs to provide national leadership.

- As Professor Clement wrote to the committee: "It hardly seems prudent for a notable institution such as U of T, with a duty to provide public leadership and so valuing its public reputation, to be seen siding at this point with the NSA and announcing its helplessness or indifference in the face of unfettered state surveillance. That would be a great public disservice during this formative period in the public debate over the appropriate role of surveillance in a democratic society."[15]
- Although a number of other Universities in Canada have adopted either the Google or Microsoft email platforms, these decisions were made prior to the Snowden revelations.

[12] Washington Post, "Microsoft, suspecting NSA spying, to ramp up efforts to encrypt its Internet traffic" (November 26) http://www.washingtonpost.com/business/technology/microsoft-suspecting-nsa-spying-to-ramp-up-efforts-to-encrypt-its-internet-traffic/2013/11/26/44236b48-56a9-11e3-8304-caf30787c0a9_story.html).

[13] See Heidi Bohaker, "States, Power, and Information Technology: Perspectives from History" Teach-in on University e-Services Outsourcing to U.S. Corporations, November 16, 2013.

[14] S.42 of FIPPA.

[15] Email from Andrew Clement (January 8).

There are reasonable alternatives.

- The committee very briefly discussed alternatives to O365, and looked at some very preliminary cost figures.[16] On the basis of this it is clear that there are reasonable alternatives that are worth exploring in detail. These include providing an in-house solution as well as looking at Canadian providers. Microsoft has also recently announced that it will allow cloud customers to store data outside the US, so the University could also consider the possibility of a Canadian-hosted O365 alternative.
- The committee received several submissions from faculty members and departments across the campus specifically requesting that the University fully look at the alternatives.[17]
- In her letter to Professor Andrew Clement, Ontario's Information and Privacy Commissioner, Ann Cavoukian, stated: "In ensuring compliance with FIPPA, institutions considering or revisiting outsourcing information handling should consider which service providers offer greater security, transparency and privacy in the handling of communications."[18]
- Looking at alternatives is also consistent with the spirit of public procurement policies. We recognize that these policies do not formally apply here because O365 is being offered to the University free of charge, and we appreciate that the University has a strong, long-standing, relationship with Microsoft. However, given that the length of the contract is relatively short, that there are significant exit costs, that the choice of encryption solutions (which will cost money) is path-dependent on this decision, and that there may be other future implications for University choices regarding document storage, collaboration tools, and integrated communications, the spirit of these procurement policies is still engaged. It is important that the University carefully consider choices that create dependencies on a single vendor that might limit future strategic decisions.

Educating community members is important, but should not take the place of institutional solutions.

- We need to do more to educate our community about the risks associated with using email for some types of communication so that people may make informed individual decisions. However, such education should not offload our institutional responsibility to seek an email solution that offers the University the best level of default privacy and security that is reasonably possible.
- As Stephanie Perrin wrote to the committee:

> "Simply telling faculty, staff and students their data will be held in the US is not a mitigation, you need to advise them of the risks. Does every first year student realize that if they mention (in their email to friends) using drugs on the weekend, even in code, they are of interest to the US Drug Enforcement Agency? We have plenty of examples of individuals being stopped at the border for less. I would suggest that faculty, staff, and students don't understand information flow, despite (in the case of students) their comfort with information systems, because in most cases these days they have grown up with computers. The mere fact they are posting nonsense on Facebook does not absolve the University, at least in my view, of a responsibility to advise all parties of the basics of data mining in 2014. We won't speculate about 2020 for the moment.
>
> The university itself runs activities (e.g., The Ischool's own LGBT lecture series) which could expose foreign faculty and students to problems when they return home to, for instance, West Africa or Russia (but the list of countries and potential employers is long with respect to this particular risk). In my view, turning a blind eye to potential risk to all email users from intelligence activities strikes at the heart of academic freedom. It is hard to anticipate

[16] See: *Alternative Hosting Options*.

[17] Letters from: UTFA (Nov 25, 2013), History (Nov 18, 2013), Geography (December 17, 2013), Law (December 20, 2013), Centre of Criminology and Sociolegal Studies (January 6, 2014), Faculty of Information (January 9, 2014).

[18] Letter from Commissioner Cavoukian to Andrew Clement (October 29, 2013).

> all potential risks with such a huge collection of data, without holding a multi-stakeholder workshop and encouraging an informed group to contemplate possible risks."[19]

We need to offer <u>all</u> of our faculty and staff excellent communications tools.

- The opt-out solution is not attractive. The committee as a whole has been convinced that our current email system is simply not sustainable in the long term. As a world-class research institution we should be able to tell our faculty and staff that we are offering them the best option available from a set of reasonable alternatives. We are not in a position to do this without a more thorough look at alternatives.
- The fact that faculty and staff use a variety of cloud computing tools should indicate to us how valuable it is for us to ensure that we provide them with the best and most secure tools possible. We cannot do this without a more thorough look at alternatives.

A formal cost-benefit analysis must be carried out.

- As Dean Seamus Ross, of the Faculty of Information, pointed out to the committee, a full options appraisal/cost-benefit analysis is essential to ensuring that any decision is based upon "transparent, accountable, and well-founded consideration of the issues."[20]
- This is particularly important given the way that the O365 proposal has evolved over the past several months. Figures claimed for cost saving have varied and not been well substantiated. There is no recommendation in the majority report to adopt any of its features beyond email and calendaring, providing additional features will involve costs, maintaining an in-house email and calendaring option for faculty and staff who opt-out will involve costs, any encryption solutions adopted will add significant costs, and we do not yet have any details of the encryption solutions being proposed.

[19] Letter from Stephanie Perrin (January 8, 2014).

[20] Letter from Dean Seamus Ross, Faculty of Information (January 9, 2014).