Letter to the Provost about new draft Information Security policy and Email Migration

October 20, 2015

Professor Cheryl Regehr
Provost and Vice-President
University of Toronto
Simcoe Hall, Room 225
27 King's College Circle
Toronto, ON. M5S 1A1

Dear Professor Regehr:

I am writing to you regarding two important and linked matters: first, the proposed new draft policy on *Information Security and the Protection of Digital Assets* (also known more generally as the "Cyber Risk" policy) being developed by the Vice-President University Operations and second, the proposal to migrate ecommunications (including email) for academic staff at the U of T to a third party vendor.

I want to start by acknowledging your efforts to date in seeking input from UTFA and the University community more widely on these matters. As an Association, we of course agree that the U of T needs good policies, procedures, and practices in place to safeguard digital information and records, and to provide for effective ecommunications.

UTFA's primary overarching concern pertains to both of these initiatives, and has to do with the significant risk that academic freedom (as described in both Article 5 of the UTFA Memorandum of Agreement as well as in the Mission and Purpose statements of the University of Toronto) and privacy rights for academic staff (largely informal at present) will be undermined. I am sure you would agree that for academic freedom to prevail in the University, colleagues must enjoy appropriate levels of autonomy in the accumulation, management, and circulation of their professional records – whether related to teaching, research or creative and professional undertakings, and whether the files or data are stored in electronic form or otherwise. Thus, some measure of privacy and protection against improper

surveillance and seizure of those records – including by the University administration or by external parties, including domestic and foreign governments – is in order. None of us would accept, for instance, casual monitoring of our University email by members of the Administration.

Quoting from a November 2013 letter to you on this matter: *"While faculty and librarians are indeed employees of the University of Toronto, the employment relation of academic staff is quite distinct in that, in order for academic staff to enjoy the robust academic freedom on which the excellence of the U of T depends, we must retain control over our professional records and correspondence, electronic and otherwise. Moreover, in many instances, important matters of intellectual property may be involved in electronic correspondence."* And yet, the **U of T does not have a privacy policy that governs access to and control over academic records (electronic or otherwise) generated by academic staff and that specifies the responsibilities of the University to uphold the highest standards of protections for professional privacy when it comes to custody and control of those records**. Numerous peer institutions have such policies. We have repeatedly offered to negotiate such a policy on an expedited basis. In fact, I note in this context that our November 2013 letter expressing concerns about the proposal to outsource ecommunications went altogether unanswered by your office.

With regard to ecommunications, we understand that the University administration is now in a position to select from among the bids from prospective third party vendors. As we expressed to you in our letter of November 25 2013, *"…we consider any change to the administration of, access to, and control over faculty and librarian email [or ecommunications more generally] to be a change in the conditions of academic work for those we represent and therefore a matter of concern to UTFA. This is all the more so given the potentially significant implications of this or any similar migration for issues of: (i) academic freedom; (ii) privacy and security of academic records and correspondence; and (iii) control, management and ownership of intellectual property."*

Now, with the proposal to centralize the management of digital assets, the need for a privacy policy is made even more evident. **Academic staff at U of T deserve a policy making their rights to privacy and control over access to their academic records strong and explicit, commensurate with the quality and importance of the work they do, and with the central importance of academic freedom in underpinning this University's deserved reputation for excellence. UTFA's view is that such a policy must be in place prior to any outsourcing of ecommunications to a third party vendor. We will strenuously resist attempts to move in the opposite order.** We are waiting for your response to our repeated overtures.

With regard to the proposed so-called "Cyber Risk" policy, we are pleased to provide you with some input subject to the proviso that we reserve the right to challenge the policy in its final form and with the aforementioned concern about this policy being advanced in the absence of a strong policy foundation featuring explicit rights to professional privacy for academic staff.

UTFA's primary concerns regarding the proposed Cyber Risk policy can be organized into three broad areas:

i. **academic implications of the policy;**
ii. **collegial consultations leading to finalization and eventual approval of the policy; and**
iii. **the relationship between existing IT and digital asset management provisions at the unit and divisional levels on the one hand, and the new architecture of IT and digital asset management envisioned by the policy on the other, including genuinely and**

appropriately collegial input to and oversight of new administrative authorities arising from the new policy.

While the proposed Cyber Risk policy has clear administrative and technical dimensions, it is important to recognize that this policy also has important academic implications, not least since it pertains in part to the secure storage and communication of electronic information generated by and relevant to the research, teaching, and professional activities undertaken by academic staff at U of T. Thus, the policy and should be developed and implemented in this light. Specifically, decisions and/or policies for the protection and management of digital assets may bear on the academic freedom rights of individuals and groups (e.g., if decisions on management of digital assets alter customary and formal rights of academics to control access to their electronic records pertaining to teaching and research). Yet the central importance of maintaining academic freedom is not recognized in the draft policy. We believe that one of the underlying rationales of this proposed policy ought to be to uphold academic freedom in the management of IT and digital assets, and that this should be made explicit. We know that some of the concerns about the proposed policy being expressed by various units from around the University deal directly or indirectly with this fundamental issue in questioning the need for increasing the centralization of management and authority when it comes to digital assets and information security.

We also understand that wider consultations are now underway pertaining to the proposed Cyber Risk policy. We applaud and encourage efforts to seek input from the U of T academic community on this policy, and on the issues to which it pertains. Given the significance of the proposed policy to the University's academic mission, we specifically support calls to **strike a more formal and representative committee with appropriate academic membership in order to consider feedback and finalize the policy, and to record and make available some record of deliberations pertaining to the policy.** These calls seem reasonable as a way to ensure that the process of developing this policy adheres to existing standards of collegial governance where academic policies are concerned.

With regard to the specific content of the policy, we do have additional concerns, some of which echo sentiments that have been made and continue to be conveyed from various academic units and individual faculty and librarians from around the University. Broadly, while the policy is relatively long on the introduction of new standards of security in the management of IT and digital assets by the Vice-President University Operations, it is comparatively short on how these standards will be met within units and divisions and thus how the policy will be implemented. This speaks more generally to the thrust of the policy which places a new burden on academic units to comply with standards that are promulgated primarily by the Office of the Vice-President University Operations. **Would it be possible for the VPUO and the Chief Information Officer to work more closely with those staff (academic and otherwise) involved in the design and implementation of existing IT and digital management procedures and practices in order to ensure more input from around the University when it comes to appropriate standards and procedures?** Close collaboration of this kind will help to ensure that the policy and its implementation are sensitive and responsive to the diverse needs and forms of expertise that exist across the institution.

We also see some potential issues with the role of the Office of the VPUO in the implementation of the policy. The draft policy calls for establishment of an Information and Security Council (ISC) to help oversee implementation of the policy, and specifically to advise the VPUO on "appropriate Procedures, Standards, and Guidelines…". The ISC is envisioned as a broadly representative committee with "expert" membership to be determined by the VPUO. While the need for expert advice from this or some similar

committee is not in question, it would also seem appropriate for the policy to elaborate on criteria used to ensure the ISC will indeed be representative, that the ISC deliberations will be accountable to the wider University community, and that the membership of the committee reflects relevant *academic* as well as technical expertise.

There are also potential concerns with the scope and oversight of emergency authority that the draft policy envisions being vested in the Office of the VPUO. The policy now reads: *" In the event of an emergency situation that threatens the University's Digital Assets, the VPUO shall have full authority to enact emergency response measures that shut down the risk or mitigate further damage to Digital Assets and to protect the University community. Actions taken by the VPUO under this Emergency Authority shall be reported to the Information Security Council and in the VPUO's annual report to Governing Council via the Audit Committee."* Some emergency powers of this sort might well be appropriate given digital security threats, but wielded improperly, these powers themselves run the risk of becoming a serious concern. **What requirements, for instance, are in place to notify potentially affected academic staff before or after the enactment of emergency measures to communicate the character of and rationale for the measures? Why are there no appeal or review rights envisioned in the policy to ensure accountability in the exercise of this authority? What steps will be taken to ensure that academic freedom and privacy (within the University community as well as outside it) will be upheld and prioritized in the event of any need to invoke these emergency powers?**

In sum, we have been hearing from numerous colleagues and units around the University on these matters, on the record and off, expressing concerns about the proposed policy and the proposal to outsource ecommunications. As you know, several colleagues collaborated on the excellent report "*Seeing Through the Cloud: National Jurisdiction and Location of Data, Servers, and Networks Still Matter in a Digitally Interconnected World*"[1] and released it publicly on September 15 2015 at a wellattended event supported by UTFA. We owe these colleagues our thanks. Their report raises serious concerns and documents the important differences between national jurisdictions when it comes to privacy rights and protections against government surveillance. Because of the contrast between Canadian and other national jurisdictions when it comes to privacy rights and protections, and because Canadians largely forfeit those rights and protections when it comes to data stored in other jurisdictions, there are important distinctions between domestic and third party vendors when it comes to protections against surveillance of electronic correspondence and records by foreign governments and, for that matter, other public and private entities. As you know, the recent EU "safe harbor" court ruling pertaining to the security of personal data of European citizens stored in the United States indicates that contractual assurances by US companies such as Microsoft and Google about protecting privacy are no obstacle to US government surveillance. Given the fluid landscape of international law in these areas, revelations about the extent of government surveillance, and the critical issue of what protections can and cannot be contained in a contract with a third party vendor pertaining to ecommunications, a University policy that lays out what responsibilities the University administration is prepared to assume to protect the privacy and security of academic records as a condition of academic freedom at the U of T is absolutely vital.

The lack of a policy making explicit the specifically academic rights to privacy for academic staff is a serious policy gap that predates both the proposed migration of ecommunications to a third party vendor, and also the proposed Cyber Risk policy. But both initiatives highlight the urgent need for a new privacy policy to form part of the context in which management of electronic records, communications, and assets takes place. One would expect, for instance, that any contract with a third party vendor pertaining to the management of ecommunications would reference such a policy and the need to uphold

the privacy rights of academic staff. And I stress here that the issue is not personal privacy (although that is important too), but specifically academic, professional privacy rights and provisions. As you know, UTFA proposed new privacy language for inclusion in the Memorandum of Agreement during the Special Joint Advisory Committee (SJAC) process. The Administration rejected that language outright. But, crucially, the SJAC agreement does include agreement that significant, Universitywide terms and conditions of employment as they are expressed in existing or new policies must be negotiated with UTFA. It is UTFA's view that the proposal to migrate ecommunications to a third party vendor and the proposed Cyber Risk policy are highly likely if not certain to result in unilateral alteration of the landscape of existing, informal and customary privacy and custody rights of academic staff. We cannot allow that to happen.

I and other members of UTFA's leadership are ready to meet with you at your earliest convenience to initiate steps toward formulation of a privacy policy that can meet the changing needs of our University. I look forward to hearing from you.

Sincerely,

Scott Prudham
Professor, University of Toronto
President, UTFA

cc. Scott Mabury
Meric Gertler

[1] The report is available at http://ecommoutsourcing.ischool.utoronto.ca

File attachments:
Letter to the Provost about new draft Information Security policy and Email Migration

---