March 24, 2016

From: Sergio Rodriguez, Director, Information Services
To: All Schulich School of Medicine & Dentistry faculty members
RE: Western Email Migration to Office 365 – Option to defer until Canadian data centres are available

Western’s current email system (for @uwo.ca addresses), known as Convergence, is lacking a modern feature set and is not well supported by its manufacturer. Recognizing that email is still a key system within the University environment, Western University’s Information Technology Services (ITS) undertook an initiative to find a replacement for Convergence.

A comprehensive review led to a contract between Western and Microsoft for the use of Microsoft’s cloud-based email and collaboration platform known as Office 365.

As part of the implementation of this system, Western recently announced that it will be moving existing @uwo.ca email accounts for faculty and staff beginning in May 2016.

Since this system is ‘cloud-based’, meaning that the servers that store and transmit the data for the service exist outside of Western’s premises, a Privacy Impact Assessment (PIA) was carried out by Western ITS, Legal Counsel & the Privacy Office to vet the security of the system and to ensure reasonable steps were taken to protect the privacy of Western users.

Some members of the University community have expressed concern about Western email account data residing in US based servers due to the fact that in doing so, they would be subject to the US surveillance apparatus.

The University is aware of and sensitive to these concerns. In response, Western is offering faculty members a one-time option to defer moving their accounts to Office 365 until Microsoft has servers available in Canada. This option is designed to provide those who may be concerned about the US surveillance apparatus potentially having access to their email data, an alternative that may provide more privacy protection by having the servers reside in Canada and under Canadian law and jurisdiction.

Implications for your consideration when deciding whether or not to defer:

- The main benefit of not deferring is the ability to take advantage of the Office 365 features immediately, including more reliability (Microsoft guarantees 99.9% uptime), a 50 Gb mailbox, ability to connect a mobile device easily and the ability to share a calendaring system with students and staff who are also on the Office 365 system; This may be especially important to faculty who use the Western system as their primary email account.
By not deferring (and therefore having data stored on US servers until Canadian servers are available), individuals are acknowledging and accepting an additional risk in terms of not having Canadian law as an additional potential layer of protection with regards to privacy.

It is important to note that when Canadian servers are available, Microsoft will be moving all Western accounts to Canada including those which migrated initially to the US based servers. While Microsoft has previously stated that these servers will be available some time in 2016, as of this writing, the exact timing of their availability or when Western’s data may be moved is not known.

It must be acknowledged that there is additional risk with having Western email system data stored in servers in the US rather than in Canada. The following considerations will help in contextualizing this additional risk:

- Type of data in question. The type of data being discussed is primarily user-created content (a user’s email messages, calendar items, etc.). Microsoft will never store nor validate Western user IDs and passwords. This validation will continue to occur at Western.

- All pertinent University policies and guidelines including those related to security, privacy, and collective agreement obligations continue to apply regardless of where the service is hosted.

- Western recognizes that it is not guaranteed that ‘user data’ will not leave North America; this would apply whether the service is hosted in the US or Canada. This means that ‘Since user data is stored in foreign jurisdictions (principally, the United States), it is subject to the laws of those jurisdictions including laws, which permit a government to access it.’ (Microsoft Office 365 Privacy Impact Assessment, P. 13).

- Having data stored on Canadian servers may provide additional protection while the data is at rest (i.e. not in transit from its source to its destination). In Canada, individuals are afforded protection from unreasonable search and seizure by our Constitution which would not apply if the data is stored outside of Canada. Page 13 of the PIA articulates two important notes regarding this matter:
  - Canadian authorities also have the ability to legally intercept electronic information. The PIA states that ‘International and domestic instruments also permit or require Canadian authorities to share intercepted e-communications with authorities in the United States and other foreign countries.”
  - Western has determined that the probability of being subjected to US foreign surveillance court orders to be very low.
• Our geographic location and the way that internet based communications are routed does not guarantee that when messages travel from source to destination, they will not travel through the US, making them subject to an US surveillance program called UPSTREAM in which the US National Security Agency collects data as it moves through the internet - even if the service is hosted in Canada. The PIA references a report titled "Canadian Internet ‘Boomerang’ Traffic and Mass NSA Surveillance: Responding to Privacy and Network Sovereignty Challenges" which provides further details on this phenomenon.

• The overall assessment by the subject matter experts at Western (Privacy Office, Legal Counsel and Western ITS) found that ‘Microsoft’s physical and logical controls align with University security and privacy obligations and that any remaining risks should be mitigated or limited…” (Microsoft Office 365 Privacy Impact Assessment, P. 2) and while they acknowledge additional risk of government surveillance, they view the risk as having a low probability (P.14).

• Email is not generally considered a secure method of communication, regardless of where the system is hosted. As such, it is best to find alternative means to communicate private/confidential or sensitive information. Western has committed to making an internal secure file sharing mechanism available this spring as an alternative to using email for such cases.

The decision to defer moving the Western account until Canadian data centres are available is personal and its implications, including the considerations set out above should be weighed carefully. If any faculty member would like to discuss any specific situation or areas of concern further, Schulich Information Services is happy to discuss and provide guidance.