Guidance from the Information Privacy Commissioner

One of the important risks identified in our evaluation of the proposed project to migrate faculty and staff e-communications to the Microsoft cloud is the university's capacity to meet its obligations under the *Freedom Information & Protection of Privacy Act (FIPPA)*. The legislative officer responsible for ensuring compliance with *FIPPA* is the Information & Privacy Commissioner of Ontario. Consequently, we have adopted the IPC's recommended *Privacy by Design* Framework and Foundational Principles as a guide to working through this project proposal. We are also very attentive to insights and perspectives that the IPC is able to provide on both the specifics of our approach and, more generally, issues about outsourcing services to US-based cloud providers.

During the project's consultation, views were expressed that the Ontario IPC and other government privacy commissioners do not represent the standard of privacy observation to which the university should aspire. As the investigator to whom the university is responsible in FIPPA matters, however, statements from the IPC provide important guidance on the expectations of privacy practice for which we are accountable. Consequently, in the material below, we wish to share comments of the IPC gleaned from correspondence that has come to the Committee's attention:

> *… I remain of the view that we cannot simply prohibit institutions from outsourcing to US corporations.*
>
> *…it is not realistic for organizations to take the approach of "locking down" their communications systems within a local or national geographical boundary. We live in an increasingly interconnected, Internet-driven global economy in which data is transferred and stored instantly on computer servers around the world.*
>
> *In response to your concerns that US law may present greater privacy risks to Canadians vis a vis the processing of their personal information by an American-based or owned communications service provider, I note that even assuming your analysis is entirely correct, prohibiting or restricting the outsourcing of email to US corporations may not provide sufficient practical benefits. Consider for example, that even if an institution were to continue to provide email services in-house or through a Canadian owned local corporation, emails sent to individuals in the US or emails sent within Canada to individuals using US service providers (e.g. Gmail, Yahoo, etc.) may still be subject to NSA surveillance under the USA PATRIOT Act and the FISA Amendment Act. In addition, it has been reported that Canadian communications service providers frequently route intra-Canada communications through the US. And local service providers and systems handling Canadian content may also be subject to remote attacks.*
>
> *Moreover, as recent media reports make abundantly clear, we cannot discount the very active role the Communications Security Establishment Canada (CSEC) appears to be playing in such surveillance programs. Not only does CSEC appear to have its own secretive metadata surveillance program – a program all Canadians urgently need to know more about – but CSEC appears to be complicit in working closely with the NSA to weaken encryption standards, spy on other countries, as well as exchange related personal information. Further, CSEC-related revelations are expected in the coming weeks.*

In this opaque and evolving context, it is difficult to evaluate the significance of any benefits that may be associated with trying to keep the processing of Canadian communications metadata and content in Canada.

Please note that in addition to requiring institutions to comply with the privacy and security requirements found in the Freedom of Information and Protection of Privacy Act*, I encourage all organizations to take a proactive, leadership approach to protecting privacy. In this regard, my office encourages voluntary adherence to the* Privacy by Design *Framework and Foundational Principles. This involves making privacy a top organizational priority from the outset, assembling an empowered project team, consulting with affected stakeholders, carrying out a thorough and iterative privacy impact assessment, applying risk-based controls, providing meaningful options and privacy enhancing-tools to users, documenting all pertinent decisions, and carrying out activities in an open and transparent manner.*

(Cavoukian, Ann, Information and Privacy Commissioner, Ontario, to Lisa Austin, Associate Professor, Faculty of Law, University of Toronto. 11 October 2013.)