Seeing Through the Cloud: National Jurisdiction and Location of Data, Servers, and Networks Still Matter in a Digitally Interconnected World

Heidi Bohaker, Lisa Austin, Andrew Clement and Stephanie Perrin.

Executive Summary

Moving to the Cloud? Many Canadian organizations are doing so, contracting with third party vendors to provide a wide range of digital services over the global Internet.

"Moving to the Cloud" really means creating content and storing the digital archives of information produced—including confidential, proprietary and deeply personal information—outside of your organization's physical control, on someone else's computers, somewhere else in the world.

In the short term, such extra-national outsourcing may appear to make financial sense, especially for those in the education sector who can access these services for little to no cost, at least for a limited period of time. But what are the broader and longer-term consequences of doing so?

The authors of this report undertook a year-long study to investigate the privacy implications of using services hosted in the global cloud where the data at issue would be stored or processed in another nation's jurisdiction, regardless of whether it was encrypted or not.[1] As academics from the humanities, law, and information studies, we were drawn to this question following Edward Snowden's 2013 release of documents which revealed the sweeping extent of domestic state surveillance activities by the United States, especially those targeting "non-US" persons. We could not reconcile this information with claims that data faced a "similar risk" from such surveillance regardless of where in the world it was stored or processed.

In our research, we examined relevant statutes, constitutional doctrine, and other case law in Canada and the USA, investigated the history of transborder data flows and current North America Internet traffic patterns, and studied decisions by Canada's major public universities to use Google Apps for Education or Microsoft Office 365,

[1] Our research was funded by Canada's Office of the Privacy Commissioner's Contributions Program, 2014-2015. This document is the executive summary for our public report. Detailed research reports are listed as appendices at the end of the public report and are also available for download as pdf files from our project website: http://ecommoutsourcing.ischool.utoronto.ca/.

suites of eCommunications and collaboration software (which includes email, messaging, telephony, video-conferencing and document creation, editing and storage).

Such systems are particularly sensitive with respect to privacy concerns because they are archives of conversations and ideas that are internal to organizations, such as intellectual property, strategic planning, confidential employee medical and performance issues and research and development data. These digital archives also contain *metadata*, or data about content, the "to" and "from" of a message and dates of creation and modification that themselves reveal significant personal information.

Based on our research, we found that for sensitive digital data **national jurisdiction matters: where in the world your data is located affects which third parties can legally access it, and on what terms.** Governments around the world can and do legally access digital data; the important question is *access on what standards*? When Canadians store their data, for example, in the United States, their data can be accessed by United States government authorities on standards that would be unconstitutional if applied within Canada. Nor can Canadians expect that United States constitutional standards will apply to them. Furthermore, specific US legislation explicitly provides a lower level of privacy protection to the digital data of non-US persons.[2]

Canadians and Canadian organizations have significantly better legal privacy protection from state surveillance when their data are processed, stored, routed or more generally kept exclusively within Canadian jurisdiction than elsewhere. This protection extends to valuable intellectual property which is also vulnerable to industrial espionage from state surveillance in foreign jurisdictions. Canadians have significantly more options to address data protection concerns through their own courts, legal reform and the electoral process.

Organizations should plan their use of externally-hosted services carefully, based upon a thorough analysis of the data to be processed or stored extra-nationally. For content that is intended for sale or dissemination globally (for example, movies, books, music) or for records whose data classification is "public," the use of globally-provisioned cloud-based hosted services may be an appropriate choice.

However, for data classified as personal, confidential or otherwise sensitive, moving to the global Cloud requires Canadians or those living in Canada to forfeit their rights and

[2] For the full legal report, see Lisa Austin and Daniel Carens-Nedelsky, "Why Jurisdiction Still Matters," available as a pdf file at http://ecommoutsourcing.ischool.utoronto.ca/.

protections as citizens and residents—particularly their constitutional protections—in the name of potential savings that may be realized from extra-national outsourcing. The expectation of privacy in law is not only a human right; the Supreme Court of Canada has repeatedly affirmed that it is also necessary to preserve a free and democratic society. Control over one's personal information is required to maintain individual autonomy and dignity which are crucial social values; by restricting the right of the government to pry into the lives of its citizens, democracies protect fundamental freedoms.

Based on the findings of our research, we strongly recommend that:

1. Canadian organizations should not outsource eCommunications services beyond Canadian jurisdiction until adequate measures for ensuring legal and constitutional protections equivalent to those in Canada are in place.
2. When considering eCommunications options, including outsourcing, organizations should conduct thorough and transparent Privacy Impact Assessments (PIAs) and Threat Risk Assessments (TRAs), taking into account constitutional and other protections provided under Canadian law, as well as the risks of using services hosted in foreign jurisdictions. The "similar risk" assertion should no longer be used in PIAs to support extra-national outsourcing.
3. Organizations that have already outsourced to companies that place data outside Canadian jurisdiction should revisit these decisions in light of the deeply flawed "similar risk" assertion and what is now known about, for example, mass surveillance practices in the USA. Organizations should consider the risk of similar practices occurring in other countries.

There is an urgent need in Canada for a combination of technical, policy and legal expertise to conduct further research in this area and to develop new regulatory and IT solutions in order to safely realize the benefits of cloud computing technologies. These could include everything from amendments to and enforcement of existing privacy laws, to regulations that keep domestic Internet traffic from leaking out to the global Internet, to international treaties on data protection and improved encryption technologies. Making an informed decision about moving to the cloud requires seeing through it, to the reality of existing national jurisdictions and state surveillance practices with which we still live.