September 2015

CAUT BriefingNote

Outsourcing

Increasingly, university and college administrators are contracting out their institutions' operational IT needs. Specifically, this means moving from an IT system with a server based at the institution with an in house IT support staff to a cloud based system outside the institution where most of the staff resources are provided by the cloud provider. Many institutions have already moved the operation and management of student email accounts to cloud providers and are increasingly keen to move academic staff emails, records and data to the cloud.

The decision of a university to outsource one or several services to cloud providers could have an impact on the privacy of all employees and students. When the university allows a third party provider of services access to employees' personal and professional data or to students' personal and *academic work* data for secondary uses, employees and students could have claims according to privacy laws.

Academic staff can challenge access to their professional and personal data by providers of cloud services based on their academic freedom and privacy rights determined by their collective agreement and by laws of general application.

CAUT is able to assist academic staff associations dealing with institutional officials or agents contemplating or executing members' data to a cloud provider.

What is the Cloud?

At its simplest, cloud computing refers to storing, accessing, and processing data and programs over the internet or external networks, rather than on local computer drives or networks. According to the National Institute of Standards and Technology:

*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management efforts or services providers interaction.**

The cloud is in effect a data centre, usually a building resembling a warehouse filled with servers. Some can be located a few kilometers away from your institution. Others can be located hundreds or thousands of kilometers from your institution.

---

* National Institute of Standards and Technology, Special Publication 800-145, September 2011, The NIST Definition of Cloud Computing, Part 2, page 2, available at: http://1.usa.gov/1umXAe3.

CAUT ACPPU

Canadian Association of University Teachers
Association canadienne des professeures et professeurs d'université
www.caut.ca

cope225sepb.ca

Why is the Cloud a Problem for Faculty?

Unrestricted access by a commercial cloud provider to academic staff data is a violation of academic freedom and privacy rights as defined by the collective agreement and the law.

Contractual provisions entered between the university/college and the cloud provider may give the provider the right to collect, data mine, and store an academic staff member's data for secondary purposes. By accepting these contractual provisions, the university or college in fact allows the provider to create employee profiles and to monetize the data collected.

The analysis of data is a major growth industry, subject to constant change with new methods and refinements accompanied by an absence of transparency on how data is being manipulated and commercialized. A provider's assurance that that it will not collect data to advertise to users or collect end-users' data for advertising or marketing purposes does not mean that the collected data would not be used for other types of commercial practices. For this reason, it is important that the contract limit the providers' access to faculty data solely for uses necessary to the provision of the outsourced services, i.e. defending the system against malware attacks or general system maintenance, etc.

Data centers run by US based corporations make faculties' data subject to the NSA's surveillance apparatus.

American surveillance and law enforcement agencies can require access to email and other records stored in any of the US based corporations' server farms, wherever in the world the server farm is located. The corporation is required to comply with the request and is not permitted to advise the affected individual or institution that their data is being accessed by the US government. Recent amendments to the *Patriot Act* and to other laws (pursuant to the *USA Freedom Act*) have curtailed the most egregious of the NSAs powers, but the law (including various Executive Orders) continues to permit US government officials to obtain computer and other records from service providers without notice to those affected. Even if they knew about a request, non US citizens do not have the same rights and protections to challenge those requests in the US courts responsible for deciding cases under the *Act.* And the minimal protections that do exist in the *Patriot Act* and other surveillance legislation does not apply to non US citizens.*

State surveillance of academic's work is a core breach of academic freedom. When the cloud provider is a US based corporation, faculty data automatically has less protection than it had under an internal, onsite system as a result of the legal framework of US government surveillance and monitoring. While the Canadian government has adopted a more invasive surveillance agenda recently, Canadian based data centres and cloud providers still offer better protection from surveillance, despite recent legislation, than a data centre operated by a US based provider.

Data stored at external data centers may be more vulnerable to data breaches than an onsite server for a number of reasons.

The cloud storage itself may be breached by hackers, as was the case with the iPhone hacking scandal, where celebrities' private photos were accessed and released. Other risks of cloud storage include increased vulnerability to inadvertent data release, which can result from common practices, like employees accessing their employer's system through insecure personal mobile applications. Furthermore, due to the sheer magnitude of the data storage in cloud-based systems, a malicious attack on one cloud customer can enable access to other cloud customers using the service.

---

* An arbitration decision was rendered on August 26, 2015 between the Nova Scotia Government and General Employees Union and Dalhousie University. In this case, the NSGEU challenged Dalhousie University's decision to contract with Microsoft Inc. to provide e mail and collaboration tools that would result in personal information of employees being stored outside of Canada, contrary to Nova Scotia's *Personal Information International Disclosure Protection Act* (PIIDPA). The arbitrator dismissed the grievance, finding that the outsourcing in this case did not contravene the PIIDPA. The case was argued solely on the basis of whether the PIIDPA had been violated, and the arbitrator did not consider academic freedom or privacy language that is contained collective agreements for academic staff. However, CAUT is concerned about the arbitrator's conclusions, because by allowing the University to outsource its contract to a US based server with data centres located around the world, the affected employees have lost control over their data.

What Can Faculty Associations Do About It? Get Access to the Contract!

When administrators are considering migrating academic staff data and records to the cloud, the number one priority of academic staff associations should be to get access to the contract being negotiated by the administration and provider. The contract will set out vital language about the level of security (e.g. is data encrypted while stored, is it encrypted when transmitted?) to level of access the provider is entitled to academic staff data (e.g. can the provider mine faculty data in order to sell it to marketing companies?). The contract will also contain or refer to the Terms of Use that end users (academic staff) will be required to accept in order to access to the outsourced services (data storage, electronic communications or other).

Many administrators will cite privacy concerns and/or the competitive economic advantage of the provider in order to forestall access to the contract. Academic staff associations should be prepared to agree to reasonable confidentiality pledges with regard to the content of the contract if necessary in order to access the contract. The increased use of computers and various electronic resources by faculty in conducting their work makes the language of the contract a key frontline in the protection of academic freedom. The devil truly is the details; so access to the contract is essential to ensure faculty data and communications is being rigorously protected.

Once academic staff associations are able to access the contract, below is an incomplete list of the kinds of issues we have seen in some contracts that would require specific attention.

Security of Data

The contract should specify actual, specific security standard, as opposed to a pledge to adhere to *industry standard* security practices, or standards for *similar* information. The contract should also require the encryption of data (storage and transmission), and compulsory and expeditious notification of data breaches.

Access to Data by Provider

There should be a prohibition on all data mining, including the creation of any type of end user profiles. The confidentiality of data should meet Tri-Council research integrity standards. However, a prohibition on data mining is insufficient. Access to faculty data by the provider must be limited to access necessary for the purposes of system maintenance such as defending the system against malware or email spam.

Location of Data

There should be a prohibition on extra-territorial storage. Server farms must be within Canada in order to ensure that communications are not subject to NSA surveillance, which may also be contrary to Tri-Council or other research standards that require confidentiality of sensitive research data.

Paramountcy of Contract between Institution & Provider

Many contracts reference an outside document (such as Google's privacy policy), that can override the terms and conditions of the contract between the provider and the institution, and which can be amended in the future without notice to customers or users. For example, the contract between the institution and provider may not permit data mining; however, the privacy policy (or future versions of the privacy policy) may allow data mining.

Ownership of Data

The contract must specify that intellectual property rights remain with the institution and users.

Amendments to Contract

The contract should specify that amendments to the contract require approval of the parties — do not accept language that allow provider to unilaterally alter the terms of the contract.

Jurisdiction & Governing Law

The contract should specify that the legal jurisdiction for resolving disputes is the home jurisdiction of the institution.