https://thevarsity.ca/2017/07/31/data-in-a-foreign-land/

HED: Data in a foreign land

DEK: U of T's email outage and the privacy implications of sending data abroad

Published: 31 July 2017

Byline: Josie Kao

On April 28, U of T suspended its UTmail+ service for students and alumni for what was supposed to be a five-day transfer of data from the US to Canada. The transfer did not go as planned. Students and alumni unexpectedly lost access to their accounts for an entire week. Suddenly, the data that many considered to be ever-present was gone.

This unexpected transfer failure brought attention to the university's eCommunications systems. Collectively, students, staff, faculty, and alumni conduct an incredibly vast amount of correspondence through these email services; is this data as secure as people are led to believe? Data is something that we might think to be ubiquitous — at least, that's what the term 'the cloud' might lead us to believe. But data has a physical root: it is stored on servers across the world, and for years, U of T's email data was stored in the US.

Sending data abroad

In 2011, U of T decided to outsource email services to Microsoft. Most current U of T students only know of the current UTmail+ system, but at the time, the choice to sign on with Microsoft was an important one. As the old email system became increasingly outdated, U of T was faced with two options.

The first option would have required the school to build and maintain its own servers. In his report titled "Report #2 and Recommendations, Student e-Communications Services," U of T's Chief Information Officer (CIO) at the time, Robert Cook, estimated this would cost the university around $1.44 million.

The other option, outsourcing to Microsoft, was free. The university eventually chose this option.

With the decision to let Microsoft run its eCommunications services, U of T was putting its data in American hands bound by American laws. This arrangement prompts one of the biggest questions in the world of data security: what happens when data travels across borders?

Much of Canadians' data is both routed through and stored in the US, yet no one really knows the privacy implications of this. In 2015, a team of U of T researchers led by faculty members Heidi Bohaker, Lisa Austin, Andrew Clement, and Stephanie Perrin released a report titled "Seeing Through the Cloud," which investigated what happens to Canadians' data while abroad. The report concluded that there were areas of concern regarding the status of international data storage.

"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," the report states.

While data travels outside Canadian borders, it is not clear whether it is protected by any constitution at all.

The report recommended that universities refrain from outsourcing "eCommunications services beyond Canadian jurisdiction until adequate measures for ensuring legal and constitutional protections equivalent to those in Canada are in place."

Two years after the report was released, Microsoft moved the university's data back to Canada. Clement, a professor in the Faculty of Information at U of T, described it as a positive step.

"I'm pleased that U of T has done that," Clement told *The Varsity*. "But there's still a question as to whether the US government can put pressure in various ways… onto Microsoft to get what is held in Canada."

The university also acknowledged these risks when the decision to outsource its data was made in 2011. In the Privacy Impact Assessment (PIA) conducted before the move, U of T conceded that "US authorities can request records of individual users, including emails, access logs and other personal information. In some cases the University will have no way of knowing if and

when this is happening." Despite this admission, the probability of this risk taking place was noted as "low" and its impact as "medium."

Of course, American whistleblower Edward Snowden revealed in 2013 that the United States National Security Agency (NSA) did conduct extensive surveillance on internet users outside of the US. But in a blog post published by Microsoft President and Chief Legal Officer Brad Smith shortly after the Snowden leaks, Smith said, "We do not provide any government with direct access to emails or instant messages. Full stop."

Smith went on to explain that, though his company does get information requests from the government, "When we receive such a demand, we review it and, if obligated to we comply. We do not provide any government with the technical capability to access user content directly or by itself."

After the Snowden revelations, Microsoft petitioned the US Justice Department to let them reveal more on the nature of the NSA's requests. They wanted to "share publicly more complete information about how [they] handle national security requests for customer information."

The Justice Department responded by allowing Microsoft and other companies to reveal the number of requests that each receives, but it did not go so far as allowing them to reveal what information was being collected.

In 2016, Microsoft reported a total of 61,409 requests from law enforcement, which was down from 74,311 requests in 2015.

Despite this, U of T continues to have great faith in eCommunications services. "There's nothing to suggest that we are under surveillance," Althea Blackburn-Evans, Director of Media Relations at U of T, told *The Varsity*.

"We do practice something called 'Privacy by Design,' which is a set of principles set out by Ontario's previous privacy commissioner," Blackburn-Evans said. "[We] are very proactive about that."

The principles of Privacy by Design (PbD) focus on preventative measures. As the first principle states, "PbD does not wait for privacy risks to materialize, nor does it offer remedies for

resolving privacy infractions once they have occurred — it aims to prevent them from occurring."

That being said, it is unlikely that anyone can perpetually prevent any lapses from happening. Microsoft also adheres to PbD principles, yet it found its networks susceptible to security breaches as recently as May 2017, during the 'WannaCry' ransomware attacks. Attackers were able to take control of over 200,000 computers running Microsoft's software by exploiting a vulnerability discovered later by the NSA.

While observance of PbD is a useful step in protecting data, there are no clear guidelines for dealing with privacy breaches if and when they occur.

Microsoft and the UTmail+ transfer

Despite its vulnerabilities, the university's relationship with Microsoft is still very strong. When Microsoft built two new data centres in Canada in 2016, U of T's eCommunications data was moved back into the country a year later. "The move [was] entirely about offering the full value of Microsoft 365 to everybody at U of T," said Blackburn-Evans.

Bo Wandschneider, who was recently hired as the university's new CIO, echoed Blackburn-Evans' sentiments, positioning the decision in terms of streamlining the service for students.

"What we were trying to do is create a richer experience for the students by having them in the same environment that the faculty and staff are in," Wandschneider told *The Varsity*.

But the move to bring everyone together did not go as planned, as issues with the transfer caused a delay of two additional days. The problems forced Microsoft to eventually "[escalate] the severity of the UTmail+ service issues to CRITICAL," according to a U of T update.

When asked about what went wrong with the transfer, Blackburn-Evans stated that it was "a complicated migration, there were over 200,000 accounts being transferred and some issues arose that weren't anticipated. The issue was on Microsoft's end and they were working around the clock to fix it."

Clement described the delay as "outrageous" and "really damaging."

“These systems are complex, so things do go awry, but this is one of the biggest failures that I can think of and they’ve shown that they couldn’t handle it,” said Clement. “They knew they were going to do this, they had time to prepare and so on. So I think it really draws into question any claims that they want to make about how well they’re handling their email.”

Microsoft wouldn’t comment on U of T’s customer account. “What we can say is that Microsoft is committed to maintaining the highest customer satisfaction and ensuring all customers realize the value of Microsoft’s products and services. Microsoft continues to engage with key customers to ensure that any opportunity or risk is flagged and managed in a timely matter,” Sean O’Brien, a Microsoft spokesperson, told *The Varsity*.

When asked whether the university had any misgivings about Microsoft after the transfer, Wandschneider stated that it didn’t and that there was nothing that the university was concerned about. “Whenever we go into any of these agreements where we move to cloud services, we conduct a risk assessment and we evaluate all the risks associated with being in the cloud,” Wandschneider said. “We make sure that all their systems and our systems are up to the standards that we expect and that we are protecting the privacy and confidentiality of our user community.”

The complexity of The Cloud

The most recent PIA from the university, released in early 2017, tries to address some of the risks of outsourcing. It purports to have avoided the issue of foreign surveillance since the data has moved back to Canada.

“Canadian Microsoft Data Centers are now located in Toronto and Quebec City…The data will therefore be subject to Canadian law,” states the PIA. “[This] addresses many of the questions that had arisen during consultation prior to 2016 with respect to U.S. storage of data.”

However, even if all of the university’s data is stored in Canada, there is still the problem of boomerang routing. This phenomenon occurs when data is transmitted over borders, sometimes unnecessarily, before being stored in the home country. Clement’s report, “Canadian internet ‘boomerang’ traffic and Mass NSA Surveillance,” notes that “a great deal of Canadian domestic

Internet communications boomerang through the United States and are subject to NSA surveillance."

The 2017 PIA also attempts to address this issue by noting that encryption in transit will be applied to the university's data. "This is expected to acceptably reduce risks from foreign government use of 'boomerang routing,'" it reads.

Clement recently developed a tool to plot out where data goes and the NSA interception points it runs into along the way. IXmaps.ca was made for people to see how their data is routed all over the world and how it is therefore is at a greater risk.

"I would say that it needs to be stored and routed within Canada," said Clement. "Particularly as the United States goes increasingly rogue in terms of its compliance with usual legal international norms under the Trump administration, there's a greater risk."

If the U of T community's data either travels through or is stored in the US, and the NSA has the capability to intercept it, this raises urgent concerns.

"U of T students coming from all over the world, coming from many of the so-called Muslim countries, many students are politically active, some of them will be at a relatively high risk of being of interest to the US government," Clement noted. "We don't know how far the US government can reach into these US corporate databases overseas."

Yet these risks do not only apply to international students: the NSA has admitted to wanting to "collect it all." Even data that is not necessarily a threat to the US has and may continue to be collected.

Moving forward

So how can the university ensure that it is protecting its email services? One obvious solution would be to stop outsourcing eCommunications services and start managing them closer to home.

U of T first decided to outsource to Microsoft because it was the free option. Now the university is locked into the system, and it is becoming clear that the risks were greater than anticipated.

“It’s a general aphorism about when you get something for free, you are the product. In this case it’s the students who are the product that’s being sold,” said Clement. “So you’ve been sold to Microsoft and the university has saved its money.”

However, Wandschneider said that the university was not currently looking for other routes. “We’ve done our due diligence and I’m really happy with where the data is residing,” he stated.

If the university is to remain with Microsoft, there are still other ways that the privacy of students is ensured. One of the strongest options would be to take it to the government.

British Columbia exemplifies how to use legislation to protect against foreign surveillance. BC’s Freedom of Information and Protection of Privacy Act states that “a public body must ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada,” with some exceptions.

This law requires schools in BC, including the University of British Columbia, to develop their own eCommunications system, known as BC-net. This system is run entirely within the province, and as such, would protect against some of the risks of foreign surveillance facing U of T.

“Seeing Through the Cloud” supports the BC-net model, suggesting that other “higher education and/or broader public sectors outside of British Columbia could reap similar financial benefits while ensuring privacy protection for their eCommunications systems.”

As the university community continues to debate the costs of outsourcing, U of T is preparing to move staff and faculty emails to the Microsoft service as well. And as more and more data is moved around the world, the university and its student community will soon confront what it means for their collective privacy.