IN THE MATTER OF AN ARBITRATION

BETWEEN:

Laurentian University Faculty Association

("the Union")

-and –

Laurentian University

("the Employer")

RE:	Grievance No 2017-18, regarding Google, Gmail and IT Code of Conduct Policy
DATE AND LOCATION OF HEARING:	Jan 24 & 25, June 25, Nov 29, 30, 2018, April 24 and Sept. 18, 2019.
SOLE ARBITRATOR:	Brian Etherington
APPEARANCES FOR THE UNION:	David Wright, Counsel Linda St Pierre, Chief Steward
APPEARANCES FOR THE EMPLOYER:	Daniel Michaluk, Counsel Matin Fazelpour, Counsel Luc Roy, CIO Shawn Frappier, HR Mgr.

AWARD

Introduction

This award deals with a policy grievance filed by the Association on June 22/17 (exh 1). The main issue raised by the grievance is whether the employer has violated the provisions of the collective agreement concerning the protection of the academic freedom and privacy rights of faculty members (article 3.10) by moving from its own internal email system to Gmail. The grievance also alleged violation of the provisions of articles 2.30 (Existing Practices) and 3.20. However those latter grounds were abandoned during the hearing. The remedies sought were an order requiring the Administration to take actions to cease the transition to Gmail and to implement a "Canadian email system that complies with the collective agreement. It also sought an order that members be made whole for any losses suffered as a result of the Administration's failure implement a patch to the former system and the impact the new system would have on the members' access to their documents and productivity.

The dispute over the transformation of the email system actually began back in 2013 when the employer began to plan to move the student email system to Gmail. In late 2014 the employer began discussing doing the same thing with faculty email. That led to various exchanges between the parties, including discussion of provisions of

Google contracts for applications for education, but despite the union's objection the employer eventually proceeded with the move to Gmail for faculty email.

The most fundamental issue with the terms of the contracts for the association was the fact the contract was with a U.S. based provider and the storage of the data for the system would be in the United States. To the association this meant that the system offered less protection for the protection of the privacy rights of its members than they would enjoy if the service were to be provided by a company with storage on Canadian servers. The union said it accepted that email itself was not a perfect communication system in terms of ensuring privacy. It accepted that there were privacy risks in doing anything by email in any kind of online system. However, it takes the position that privacy rights can be enhanced by not using an American provider or a provider that uses US based servers for storage. The Association also had concerns about Google and Gmail being known for data mining.

The Association accepted that the Canadian government has the ability to access data legally and has methods to do that, but argued that there are greater constitutional and other legal protections for users when the data is stored in Canada. It submitted that the legal restrictions on the Canadian government are greater than those on the U.S. government in the United States. It takes the position that the US government can access data in that country on broader grounds than those available to the Canadian government in Canada. It also argued that the legal protections for data are lower for non-U.S. nationals than for U.S. nationals with respect to data storage in the U.S.

On Oct. 9/15 Ms St Pierre sent a memorandum to Luc Roy (CIO) setting out LUFA's general and specific concerns with the proposed Google contract (Exh 5). Mr Roy responded in a memorandum sent on March 31/16 (exh 6). That memorandum did not alleviate the concerns of the association. Discussions continued between the employer and the association that seemed to acknowledge it needed the association's agreement. But in the end the employer moved to Gmail without union agreement. The union initially submitted this was a violation of the collective agreement on existing practices in article 2.30. That provision provides that prior to modifying any working conditions not covered by the collective agreement, but possessed by all members of the bargaining unit, the employer agrees to give notice of such change to the union and give it the opportunity to make representations to the employer through the Joint Consultative Committee prior to implementing any change. After such representation the employer has the right to proceed without consent providing the change is urgent and reasonable.

The union relies on article 3.10.6 of the agreement. It provides that the parties agree that members have a right to privacy, consistent with the traditions of Academic Freedom and the provisions of that article (3.10). The union contends that this clause is a recognition that faculty members have particular privacy interests tied to academic freedom that are different than non-academics or other types of employees. This arises from the fact that academics often engage in research that is in sensitive areas that might be considered to be questionable by governments. It gave as an example a political scientist doing research on terrorism or a psychologist doing research on pedophilia. It noted that the rest of article 3.10 sets out other academic freedom concerns, and pointed

especially to 3.10.2 regarding freedom in teaching, research and scholarship, and the freedom to express one's opinion about the university, its administration and the system in which one works. It argued that a robust protection of academic freedom and privacy rights associated with that are not achieved through the Google contracts for Gmail using a U.S. based company with U.S. based servers.

The union argued it is not enough to say there are inherent risks in all email systems, when the employer has an obligation to take steps to reduce those risks in the interests of protecting the privacy of faculty members to ensure academic freedom.

The employer takes the position that it made a necessary and reasonable change that is expressly permitted by the collective agreement, an agreement that gives it the express right to "determine the manner in which and the level at which facilities and services are provided to Members." (art. 3.20.1) Further it submitted that it engaged in a very lengthy dialogue with the union, and to the extent it might have been required to engage in such a dialogue prior to change, it did so to the point it could no longer afford to continue. It also contended that after significant delay in attempting to win over the union to its position, the university acted in urgency and in compliance with art. 2.30.1 and 2.30.2.

The employer noted that prior to the change in 2017 the university provided faculty with an email service called Groupwise. Copies of emails sent and received by faculty on that system were stored on computers owned by the university and kept in a room that was part of the IT department at the university. But for every copy of a Groupwise email sent or received by a faculty member and stored in the IT room there

was one or more other copies held by other parties to the email communication and beyond the control of the university. Emails in that system also need to transit the internet in unencrypted plain text to reach another party who was not using the Laurentian Groupwise system.

The university took the first step towards change in 2013 when it launched Google's "G Suite for Education" to its students. This is a set of productivity tools that are developed and hosted by Google, including email, an electronic classroom app, spreadsheet, word processing, and calendar tools, and a storage space called Google Drive to allow storage on the Google cloud. The cloud allows for storage on Google servers in eight countries, including the U.S., Chile, Ireland, Netherlands, Finland, Belgium, Taiwan and Singapore. The move for students to that system in 2013 was driven by necessity due to lack of storage in the Groupwise system. However, the problem of insufficient storage continued after the students were moved off the system. By 2015 the employer realized the performance of the Groupwise system was faltering and needed to change, and the association itself was complaining about the performance of that system. The employer decided that it had to move to a new on premises solution or move faculty and staff to Google's cloud based system. It opted for the latter solution because: it provided the service and performance faculty were demanding; it integrated well with other applications that could be used by both faculty and students; it came with unlimited storage removing the need for continued archiving; it has strong and arguably superior security fundamentals compared to any on premises solution; it was more cost effective to have a single email system; and there was no licence fee or hardware costs.

The employer also noted that by moving to Google it was following a trend that began in 2006 with Lakehead outsourcing to Google. By the time of the hearing there were at least 8 Canadian universities that had moved their email systems to Gmail. A significant number of others use Microsoft's cloud based product (Office 365). In explaining its move, the employer noted it came only after an exhaustive dialogue with the union starting as early as December of 2014, but leading no where in 2015, and resulting in a note from Ms St Pierre on behalf of the association on April 27/16 that stated she was reiterating the union's position that "members need to be provided with a reasonable email service. We have received complaints that recent changes to Novell have resulted in poor email service."

That communication resulted in further meetings between the parties in the fall of 2016 and discussions about possible resolutions in 2017 but to no avail. The university finally proceeded with its plan in June of 2017, over 2 and a half years after it started its dialogue with the union.

The employer takes the position that article 3.20.1 is key because the university promises to provide services which support the discharge of member duties but also reserves to the employer the "power to determine the manner in which and the level at which facilities and services are provided to Members." It also pointes to 3.20.4 because it requires the employer to provide a computer that is networked but fails to include any kind of particular security requirements or even a general security requirement. The employer notes that is in contrast to other parts of article 3.2 in which the parties have particular terms dealing with security, i.e., the requirement that offices must be

"securable". It submits this shows what the parties left out of article 3.20.4 but also shows they understood that security is never absolute. It submitted these are specific collective agreement provisions that ought to matter more than general promises in the agreement about academic freedom or privacy.

In direct response to the union claims about privacy concerns, the employer took the position that the move to Gmail is not associated with an increased risk of lawful access by the U.S. government or other foreign governments. It noted that Groupwise emails were already greatly exposed to the U.S. government and other foreign governments. It further contended that if there is any increased risk of lawful access by the U.S. government that increment is theoretical and immaterial. It argued that the union's case was based on "security theatre" rather than security reality. It said real security risks, such as the risk of hacking by outsiders, are real and fundamental and should be addressed by security fundamentals, a goal that is supported by the move to Google. It asked me to dismiss the grievance.

Evidence

The association's first witness was its Chief Steward, Ms Linda St. Pierre. She has been the chief steward of the union since 2009. She filed the grievance in this matter on behalf of the union on June 22/17. She said she first raised concerns about a possible move to Google for email service for faculty in 2013 when the student email system was moved to Google. She met with Mr Roy at that time to ask if the employer had any plans to do the same with faculty email. She said Roy told them there was no plan to do so at

that time but if they were to change their mind on that they would notify the union and seek its agreement on that. She said she was unsure of the timing of that meeting other than it was sometime in 2013 when the student system was changed.

Sometime later she was contacted by Roy to tell her that the employer was then looking at moving to Google for email service for faculty. Roy told her he would follow up on that discussion with the union and would give it a copy of a contract proposal from Google. They later had an email exchange with Ms St Pierre sending a brief email on Dec 13/14 to Roy and Emilie Cameron (formerly an HR Director for the university) stating that she had discussed such a move to Google with CAUT and now had some concerns, and Roy responding by email on Jan 7/15 with access to a sample agreement with Google from another university. St Pierre said the union had no internal expertise on the impact of a change to Google for email service and she wanted to consult with the Canadian Association of University Teachers (CAUT) and the LUFA executive. She then had discussions with Ms Paula Turtle, legal counsel for CAUT. She was advised that a move to Gmail would bring about some changes to the system but they would not be positive. After providing the sample Google agreement from another university to Ms Turtle, they got a response from her listing concerns that CAUT had pointed out with the proposed agreement provisions. Ms St Pierre then prepared a memorandum to reflect the advice she had received from CAUT about the potential negative impacts of the Gmail proposal (exh 5 – Oct. 9/15). She said the union's primary concern was the fact there would be data storage in the U.S. and that would make it subject to the Patriot Act, legislation that provides the U.S. Government with broad surveillance powers and thus

limits the privacy rights of faculty members using the email system. It took the position that there was better protection under the Canadian legal system. Ms St Pierre admitted she had no expertise in the area of email systems and IT.

Mr Roy responded to the concerns expressed by LUFA about the move to Gmail in a memorandum sent to Ms St Pierre on March 31/16 (exh 6). His responses did not satisfy LUFA's concerns. However, on April 6/16 Roy sent another email to St Pierre thanking her for clarifying her position that opting for Gmail was not a good option, pointing again to his point by point response to her concerns in exhibit 6, and expressing the hope that they could find a way to offer Gmail to the faculty at Laurentian and stating he was available for questions and discussion.

They then had a follow up meeting where Roy went over his responses with St Pierre. Also at the meeting were Ms Cameron, and Dean Havlovic of the Faculty of Management. St Pierre informed Roy at the meeting that she had put his responses to Ms Turtle at CAUT and LUFA felt that Roy's responses did not solve any of their concerns. They then asked Roy where he thought he might be able to get some changes from Google with respect to the U.S. Patriot Act. St Pierre said Roy tiptoed around and reiterated his earlier responses. She said Cameron asked Roy if he had any room to negotiate with Google and Roy said no, the Google agreement was a take it or leave it deal. St Pierre told the others that it made the meeting a pointless exercise if there was no way to address LUFA's concerns. She also informed others at the meeting that if that was the case LUFA could not agree to the shift to Gmail based on the concerns stated in her earlier memorandum based on CAUT advice. Roy then stated that the contract that

the memo from St Pierre was based on was no longer the contract that Google was proposing. St Pierre then expressed frustration and asked to have the new Google contract and told them she would review it to see if it addressed any of the LUFA concerns. St Pierre said that was where they left matters at the end of the meeting and the employer did not say they were moving to Gmail at that time, just that it was one of the options they were considering.

That meeting was sometime between April 6/16 and the fall of 2016. St Pierre said she did not sense any urgency on the part of the employer at that time. She said that she never received a copy of the new Google agreement referred to by Roy until the preparation for the arbitration hearing. When asked if she had ever told Roy about LUFA's position on the ability of the employer to move to Gmail without LUFA consent, St Pierre said that was dealt with in her first meeting with Roy in 2013 about the student system moving to Gmail. She said Roy told her that he had no intention of going down the road of moving the faculty email to Gmail at that point, but if he did decide to go in that direction it would be with the agreement of LUFA. She said neither Roy, nor anyone else from the university, ever told her otherwise, until a later email exchange with Emilie Cameron. Until that email exchange she felt both parties were of the view that there would have to be agreement on the change because article 2.30 applied to this issue (and then 3.10 post negotiation). St Pierre said she also received a written communication from Roy that indicated the need for LUFA agreement. She was referring to an email exchange on April 27/16 between Roy and Dr Persinger, a faculty member who had complained to Roy about the problems with the Groupwise email system. In that email,

copied to St Pierre and several others, Roy told Persinger that the employer had a solution, Google Mail, but it would compromise the current LUFA agreement. The email also stated that they had no alternative at that point but were continuing to look at other solutions (exh 9). St Pierre expressed the view in her response that the employer had an obligation to provide an email system that was quick and reliable and does not violate members' rights under the collective agreement, and stated the employer could not leverage members' complaints to create pressure on LUFA to accept breaches of the collective agreement. She testified that she felt the administration had other options apart from Gmail but were trying to shift blame to LUFA for its email problems.

There was a further meeting to discuss the Gmail issue on October 26/16. At this point the administration was making it clear they wanted to move to Gmail for faculty email and wanted a discussion to see if there could be agreement to move to Gmail. Despite having a few meetings on that issue they failed to reach any agreement. On March 22/17, St Pierre sent an email to Cameron (exh 11) to clarify LUFA's position that there needed to be agreement by LUFA prior to a switch to Gmail and any move to Gmail without agreement would result in a grievance.

The matter was referred to mediation in April of 2017 but it was not resolved. The employer then implemented the move to Gmail and the grievance at issue herein was filed in response.

When the move to another email system was first discussed by Roy and St Pierre in 2013 as a result of the student system moving to Gmail, Roy said the old Groupwise email system would eventually become obsolete and have to be replaced. However, at

some later juncture, when the Groupwise system was hacked, Roy told St Pierre that they could possibly implement a patch to fix bugs in the Groupwise system but that would cost $150,000. She said they had limited discussion of that option in 2013 but it was not one Roy considered viable and he noted that Gmail would be free and said that was a primary factor for him. However, Roy also told her that he felt that Gmail could keep the email system safer than anything he could provide under the old Laurentian email system as he had a limited budget to protect the security of email.

St Pierre said she also discussed other alternative email systems with Roy, including discussing switching to an email system based in Canada. Roy told her that he had estimated the cost of moving to a Canadian based system at $50,000, as compared to no cost for Gmail.

St Pierre said most of LUFA executive used the Laurentian email system for email, but her and her administrative assistant used Go Daddy email for LUFA business. She said when she took over as Chief Steward the former holder of that office told her it was important not to use the Laurentian email system to communicate with LUFA members. St Pierre did not want to use her personal email as she wanted to have separation between her personal and professional life, so she began looking at alternatives to find a system that allowed her to get off of the employer system but had a large capacity for storage. The only one she found that had unlimited storage for emails was Go Daddy. She acknowledged that Go Daddy was based in the United States, but said that at the time she chose it she had no awareness or information on where email was stored or where email systems were based.

St Pierre has now developed awareness and concerns about secure storage. She has contacted Go Daddy and asked it how she might download her emails to a local computer so she could keep them securely. Go Daddy said she could not do this, as she had several hundred folders and that would present a barrier to trying to switch over to local storage. She said she then looked into switching back to a Laurentian University based server. However, when she looked into that the administration told her that they had changed LUFA's password and they could not give them a new password. This made it clear to her that the administration had full control over passwords for Laurentian University based accounts. So LUFA then hired two computer science students to assist them in switching over and downloading all of LUFA's emails to a file storage system to be purchased by LUFA that encrypts all emails they send and receive. She said they were also looking at switching into another email system known as ProtonMail at the time of the hearing. They were also looking at switching to a Sudbury based server system for LUFA email. She said they were still seeking a final solution to get their files and email off of Laurentian servers and off of U.S. based servers.

In cross examination Ms St Pierre acknowledged that her Phd is in Neuroscience and she has never studied Computer Science, Data Security or Canadian National Security Law at the post secondary level. Nor did she have any work experience in the fields of IT, Data Security, National Security Law, or the negotiation of commercial contracts with technology vendors. She also acknowledged that she did not know anything about where Google stores data related to its email systems other than the United States. She said LUFA was not claiming the other countries where Google stores

data outside of the United States were a threat to the privacy rights of LUFA members. She said the grievance was about having an email system based outside of Canada and concerns about the U.S. Patriot Act and what it exposes LUFA members to in terms of access by the U.S. government to their data. She said she did not know to what extent their CAUT counsel had explained that other countries were viewed as threats. The main message was that Canadian storage and systems would give LUFA members access to a Canadian system and Canadian law regarding protection of their privacy.

St Pierre acknowledged that LUFA deferred to experts who advised them on the threats presented by the employer move to Gmail and they fully supported that position. She admitted the union lacked the knowledge to make such assessments internally. She agreed that Gmail was the primary concern of the grievance, although Google Docs was raised earlier by Roy, and both that app and Google Drive are now available for faculty use. But Roy said the Google Docs and Drive apps would not be made mandatory so they were not a primary concern when they were announced by the employer in December of 2014. She indicated that if Google Docs or Google Drive were to be made mandatory for faculty for file storage then LUFA would object. She acknowledged there was no grievance filed when the Google Docs and Drive apps were made available to faculty members for use in December of 2014, despite the fact data stored in those apps is stored all over the world. She said the reason for that was that use of those apps was left up to the members, who could also choose to use LUNET Drive to store their data. St Pierre believed that LUFA's position was that as long as members could choose what

apps they used for data storage there was not a problem with those other Google apps being made available to LUFA members.

St Pierre noted that LUFA members do not have any choice when it comes to the use of Gmail for the purpose of communicating with students. She agreed that faculty can choose to use email for a wide variety of communications with students, other faculty, administrators, research collaborators, and family and friends. She agreed that not all emails are of equal sensitivity or importance. St Pierre agreed that faculty do often have choices concerning the method of communication they use with different parties, but said she believed the university had a policy requiring faculty to use the university email system when communicating by email with students on university business. She acknowledged there was no policy preventing faculty from communicating by fax, telephone, regular mail or courier. However, she noted that faxes and phone calls often went over the internet today, and also noted that in today's world people generally use email as the primary means of communication. She also noted that there could be 200 people in a class and it is not feasible to communicate with all of them by telephone. She agreed that email was a tool of convenience that the employer has agreed to provide

St Pierre agreed that faculty often use email to communicate with people who are outside of Laurentian University and that such recipients of faculty email are outside of the Laurentian email system. She also agreed that such recipients may be highly secure or very insecure in terms of that person's email system. She further admitted there was nothing the employer could do to control for that risk although she believed they had some measures to protect Laurentian users from incoming emails. However, St Pierre

admitted that the security practices of the non-Laurentian senders and recipients of emails communicating with faculty members were beyond the control of the university. She also agreed that the email systems of non-Laurentian senders and receivers of emails communicating with LUFA members may be housed in the U.S. or other foreign countries. It cannot control where the outside communicators store their emails.

St Pierre said she was not sure if the Groupwise system emails were encrypted. She recalled Roy telling her that any outside email were subject to the lack of security of the outside senders and receivers of email and the issues of security that come with communication over the Internet. She acknowledged that it was common for faculty to email with other faculty at other universities. She said she was aware that some other universities used Gmail for faculty but other than Lakehead she was not sure which ones used Gmail and which used Microsoft Office 365. Employer counsel advised her that the following schools all used Gmail: Lakehead, Alberta, UPEI, Ryerson, Memorial, York, Nipissing, and Laurentian. She was not sure if the faculty at all those universities used email in a similar fashion to email at Laurentian. She could not say if email usage at Laurentian was more sensitive than at the other seven universities using Gmail. She was not aware what system was being used by the following schools that are currently using Microsoft email: New Brunswick, Toronto, Carleton, Queens, Dalhousie, Manitoba, Concordia, Guelph, Western, Brock, Waterloo, Calgary, McGill, OCAD, Ottawa, Windsor, Trent.

St Pierre was asked about what it was that frustrated LUFA members in terms of the operation of the old Novell email system as referenced in the grievance in exhibit 1.

She said this related to some other grievances about upgrades to the Novell email caused by the system timing out. The union had concerns that the administration was not putting in a security patch and the system was being hacked. She said she was unclear about whether this grievance was about the old system timing out or the lack of a security patch but thought it was primarily about privacy concerns. She said that after upgrade attempts to the Novell system there had been complaints from LUFA members about the system timing out and concerns that it was not working well. She said those complaints about the old system not working well came around the time she sent the email to Roy on April 27/16 (exh 9). She received a flurry of complaints from members at that time. She said she received a message of concern that LUFA was standing in the way of changing the email to Google.

She was uncertain of the number of complaints she received from members. However she agreed that there were persistent problems with the old Novell system being experienced by members at that time. She was uncertain of how serious the problems were. She said she was concerned about the timing of these complaints from members arriving at the same time that the employer was pushing for the move to Gmail and telling members that LUFA was the problem by not agreeing to the move. However, she agreed there was a problem with the email that had to be fixed. She also agreed that the employer fixed the problem by going to Gmail but pointed out that it chose Gmail instead of a Canadian based solution and that caused the grievance. But she admitted that Gmail had not been slow or subject to crashes.

St Pierre said she received some notice from Mr Frappier prior to the June 22/17 announcement by Mr Roy that it was migrating from Groupwise to Gmail for faculty email. She said that she had some discussion with counsel about mediation before they filed the grievance on June 22/17. She said she first had discussions with Frappier and Farah about the possibility of moving to Gmail sometime between 2013 and 2015. She was not certain of the timing but agreed with the suggestion it was possible that it was in the spring or early summer of 2013 that it was first discussed with Roy. When asked about the 3.5 year delay between that first discussion and filing a grievance St Pierre noted that they were informed it was only being done for students at the outset and the employer was exploring options for faculty email, one of which was Gmail. She was asked about her email to Roy and Cameron on Dec. 13/14, stating that she had checked the amended contract with Google with CAUT and her initial optimism was squashed. She said she had heard from somewhere that Google had amended its Gmail agreements in a way that would address LUFA concerns about privacy. She had told Roy she would send the latest Google agreement to CAUT for comment but she had heard back that the changes to the agreement were not favourable to address LUFA's concerns.

St Pierre said that LUFA did not file a grievance when the employer had announced that Google Drive was available to faculty in December of 2014, because they were told use of Google Drive was purely voluntary. Faculty were not required to use it. She also noted that Roy did not tell her prior to that Dec. 13/14 email that the employer was moving to Gmail for faculty. What he had told her earlier in 2014 was that the

employer was considering Gmail as one of several options for dealing with faculty email in the future.

St Pierre noted that the email exchange in exhibit 7 concluded with her suggesting they aim to meet at the end of the month (January 2015) but she said it took her several weeks or months to get the latest the version of the Google agreement and get detailed feedback from CAUT counsel on that agreement. She said she thought there were delays on both sides and LUFA did not provide the memorandum to Roy on the advice it received from CAUT until October 9 of 2015. She said she simply presented the data provided by CAUT to Mr Roy and did not fully understand it. She said that she had asked Roy and Cameron if they had any negotiating power to get Google to make changes to address LUFA's concerns and at that point Roy told her he had given LUFA the wrong contract, and there was a different Google agreement that they were going to sign. She said the memorandum of Oct. 9/15 gave details of the LUFA concerns because Roy had asked them to be specific as to their concerns with the Google agreement. However, she said the concerns raised in that memorandum are similar to those raised in the grievance in June of 2017.

St Pierre received Roy's memorandum responding to LUFA concerns about Gmail on March 31/16 (exh. 6). It was pointed out to St Pierre that, although she said Roy told her there was a different Google agreement other than the McMaster one she had been given earlier but she never received any agreement other than that McMaster agreement, an email from Roy on Feb 23/16 contained a link to the updated general Google agreement that was being considered by the employer. St Pierre said she never

clicked on that link but simply forwarded Roy's memorandum to CAUT counsel and left it to her to consider the contents including the proposed agreement link. She said she had asked Ms Cameron for the Laurentian agreement but she never received that agreement. St Pierre contended she was told in a meeting with Roy that there was a specific agreement for Laurentian but she did not receive one.

St Pierre said that she went to a meeting with Roy and Cameron and Dean Havelovis, prepared to discuss the McMaster agreement with the memo from CAUT counsel on its deficiencies. She was upset when she was told at that meeting that the McMaster agreement was not the Laurentian agreement because they had obtained CAUT advice on the McMaster agreement. When she asked Roy if they could negotiate changes to the Laurentian agreement he said no, but he was hoping he could use persuasion to get LUFA to agree as it was a take it or leave it proposal by Google. She said she was only told that it was a take it or leave it contract after she had obtained CAUT advice on the McMaster contract concerning changes that should be sought to address their concerns. She said that at the time of the meeting in April of 2016 with Roy and Cameron she still thought there was a separate Google agreement that was different from the general Google agreement because Roy had told her there was a Laurentian agreement that was different than the McMaster agreement.

St Pierre noted that Roy said several times that email was not a secure form of communication whether the system was based in the U.S. or Canada, noting that email could be compromised by law enforcement in Canada. She responded that LUFA relied on CAUT counsel with regard to differences between Canadian and U.S. based systems

with respect to privacy concerns. She said she was frustrated at that meeting on April 27/16 because they had been given the wrong contract to give to CAUT for legal advice. But she said that LUFA obtained two valuable pieces of information at the meeting: they had been given the wrong contract and they could not negotiate changes to the Google contract for Gmail. But there was no resolution.

It was put to St Pierre that the follow up meeting with Dean Havelovis was later the same day. She said that could be the case. It was put to her that the administration had reached out to try to schedule a further JCC meeting on email issues between the parties through the summer of 2016 but that LUFA was not available due to its office being closed to members from June 13 to July 4, 2016 and vacations taken by LUFA staff. St Pierre said she was aware there were some attempts to get a meeting in the summer of 2016, but said there were scheduling difficulties on both sides. The employer introduced an email invitation to schedule a JCC meeting on Gmail issues sometime in September 2016. It was dated August 19/16. It was sent by the Exec. Asst. to the Provost to St Pierre and her administrative assistant and the president of LUFA. This ultimately led to a meeting on November of 2/16 after a September meeting was scheduled but cancelled by LUFA.

St Pierre attended that meeting with Ketchen and LUFA vice president Goreham. Roy, Cameron, Carol McAuley, and Sheila Cote-Meek attended for the employer. The meeting involved discussion of LUFA concerns with Gmail including some discussion of issues arising from the U.S. Patriot Act. Roy asserted that Canada had legislation similar to the Patriot Act. St Pierre said that LUFA checked on that later and found that the

Canadian law allowed for better protection of privacy. There was also discussion of some of the terms of the Google agreement, including whether they allowed for data mining. There was also discussion of how the Northern Ontario School of Medicine (NOSM) resolved privacy issues concerning its use of Gmail as a possible middle ground. There was some discussion of possible settlement on the basis of a model they could agree upon but they were unable to resolve it. The employer then discussed the timing of its rollout of Gmail. It wanted a spring 2017 rollout (in April or May) and thus wanted a signed agreement with LUFA as quickly as possible to allow for that. There was some further discussion in the spring of 2017 around acceptance of a NOSM type of system as a solution but that was ultimately not accepted and in June of 2017 the employer announced the move to Gmail.

St Pierre had expressed one of LUFA's concerns about the security of Gmail as arising from the fact that the agreement required Google to provide 'reasonable security', no less protective than security standards at facilities where it stores and processes its own information of a similar type. Her memorandum of Oct 9/15 expressed concerns as to whether Google has information or data to store that is comparable to highly sensitive or potentially controversial academic research data. In that respect LUFA had concerns that its promise of reasonable security did not address the particular needs of academics. St Pierre agreed that Google was a leading technology company and was known to be among the most innovative companies in the world. She agreed that it conducts research to support its innovation as a world leader in its field. She also agreed that it likely had highly confidential information that underlies its innovation and its research. She agreed

that information like their latest search algorithms would be a great secret as would the coding for its latest software. She also agreed that Google possessed data that rose to the same level of sensitivity and importance as academic research data. But she said she was uncertain about how it stored other people's data. She continued to maintain there were differences between academic research data and other forms of data in terms of the sensitivity of the information.

The memorandum of LUFA concerns about the Gmail agreement (exhibit 5) included a problem with Google's acceptable use policy in that it included an obligation on the part of users to not use the email to encourage the violation of the legal rights of others. It was pointed out to St Pierre that the Laurentian acceptable use policy for email users that has been in place since 2013 included the same prohibition on members using LU mail to violate the legal rights of others or to promote or encourage illegal activity. She confirmed that no grievance had been filed by LUFA against that policy.

When asked about the move to GoDaddy for LUFA email, St Pierre said that LUFA had first explored the possibility of having separate phone lines and email systems that were not connected at all to the Laurentian system. She said that at first Bell told them they could do that but later said it was not possible. So they decided to try to get away from Laurentian email and met with a local computer services retailer to discuss moving to a new email platform. However, they currently remained with Go Daddy which has servers in the United States. St Pierre said this concerned her because it meant their email was subject to the Patriot Act, and they were still looking for an alternative but they wanted to take the time to get it right when they moved to a new system. But

she said there principle concern when they moved to Go Daddy was to get off of the LU system for LUFA business. When asked if this affected what she wrote in her email she said it did not. She was then asked if this lack of impact on what she wrote in emails was due to the fact the risk to her privacy was too small to be real. She said no, and added that if they have members with risky research then the risk is real. But she admitted that she had not had any incidents with her communications with LUFA members, and said it was not the type of communication that triggers the same level of concern.

The Association's second witness was Professor Andrew Clement. He has the title of Professor Emeritus in the Faculty of Information at the University of Toronto. He was retained by the Association to provide an independent expert report with respect to the risks, if any, to the privacy interests of Laurentian faculty members resulting from the decision of Laurentian University to transition to the use of Gmail for its email services. (exhibit 22). In his retainer letter he was asked to provide a report that responds to the following questions:

1. What are the best practices for organizations, including universities, which are considering changes to the IT systems and email services respecting potential impacts on the privacy interest of the users of such systems and services?

2. What is the difference between informational privacy and security?

3. Is there an inherent security risk in the use of email and if so, how does that impact on users privacy and are there measures that can be taken to mitigate against such privacy impacts?

4. Does a member of a faculty at a Canadian university, who has the protection of academic freedom, have any distinct or enhanced privacy interests compared to other types of employees? If so, please describe such interests.

5. What risks to faculty members' privacy interest, if any, result from a Canadian university providing email services to its faculty through a company such as Google which stores those emails on servers located in the country other than Canada. Are there particular privacy interests raised if emails are stored on servers located in the US?

6. Are the privacy interests of members of faculty at a Canadian university enhanced by the university providing its email services to its faculty through a company which stores those emails on servers located in Canada?

7. Are you aware of whether other Canadian universities provide email services to their faculty members directly or through companies which store emails on servers located in Canada? If so, please detail; and

8. To your knowledge are there any enhanced privacy protections associated with Gmail compared to other email services such as Microsoft services?

The employer did not challenge Prof. Clement's qualification as an expert but reserved the right to challenge the scope of his expertise. Prof. Clement had been a Full Professor in the Faculty of Information Studies at the University of Toronto from 1998 to 2015, and was an Assoc. Professor in that faculty from 1989 to 1998. He taught courses in the area of Information Systems and Information Policy for 25 years. He taught in the graduate program and had an active research program through those years. In the decade prior to the hearing his research had focussed on privacy and surveillance related to information systems. His research has been supported by an extensive series of research grants from funding agencies such as the Privacy Commissioner and the SSHRC.

In 2012 he served at the Interim Director of the Knowledge Media Design Institute at the U of Toronto. At the same time he was the Interim Director of the Collaborative Graduate Program in Knowledge Media Design at U of Toronto. In 2004

he was an Academic Visitor at the Oxford Internet Institute at Oxford University. This was another interdisciplinary institution focused on various social and policy issues around the internet and the use of digital media. Clement noted that a number of universities have set up such institutions to address issues related to the use of the internet and digital media and way those issues cut across several disciplines within the university.

He had numerous research grants from the Federal Privacy Commissioner in the decade prior to the hearing. A number of them dealt with privacy and surveillance in digital media. He pointed to a grant from that office for 2014-15 for a project entitled "Assessing Privacy Risks When Considering Extra-National Outsourcing of E-communications". He said that a lot of what is in his expert report for this proceeding draws on the results of that study. He said that 2014-15 study emerged from his experience with the decision by the U of Toronto on a proposal in 2013 to outsource email for faculty and staff that ultimately resulted in adopting a Microsoft product, Office 365. At that time the servers for that product were hosted in the US. Clement noted that e-communication outsourcing is an attempt to cover the breadth of office services. It is not limited to email but extends to a range of other collaborative and online services like Calendar and Document Creator. Thus email is a prominent part of the package but it covers a broader set of communications applications. Clement said the U of Toronto proposal in 2013 to outsource these communications caught his eye because of his research since 2008 looking at privacy and surveillance risks associated with storage and routing of information through the US and risks that arise from that by reason of what we

were learning about the surveillance capabilities that the National Security Agency (NSA) had installed within the main routing centres of the internet. The U of Toronto held a number of consultation sessions with faculty and staff to consider whether they should do what the university proposed and to prepare them for it. He noted that the U of Toronto had already moved over to Office 365 for student email. Clement attended a public town hall meeting on these issues and raised questions about privacy risks that were being recognized in 2013. He noted that the news since 2013 has been full of revelations by Edward Snowden, who handed over a number of NSA documents to reporters that confirmed what those who followed surveillance concerns had suspected, but lacked evidence of. After the public town hall session on the U of Toronto proposal, Clement convened a teach-in at his faculty and invited the former head of Microsoft Europe and Canadian email outsourcing to discuss the issues. Clement said that received a lot of attention from a number of his colleagues at U of Toronto, including Prof. Lisa Austen from the Law Faculty. Prof Austin was on the U of Toronto committee that was reviewing the proposal to move the faculty and staff email system to Office 365.

As a result of the discussions concerning the U of Toronto proposal, Clement, Austin and a third colleague from History, made a research proposal to study the outsourcing of e-communications to an out of country provider. At that point both Google and Microsoft were making contracts to provide these services for free in universities. Clement said as part of their study he and his colleagues looked at what other universities were doing in the hopes of providing an informed basis for assessing what to do with e-communications. They got funding for this project and had Prof Austin

do a legal analysis of risks to Canadian data by virtue of storage or transit through the US. Clement noted that at that time the prevailing view was that Canadian data faced similar risks in the US to those it faced in Canada so there was no additional risk. But Prof Austin provided a paper in the appendix to their report that took the position that the prevailing view of similar risks to systems based in Canada and the US was flawed. Their study resulted in one main report with several appendices.

Prof. Clement pointed to the following 2015 publications as very relevant to the issues in dispute herein: Clement & Obar, "Canadian Internet 'Boomerang' Traffic and Mass NSA Surveillance: Responding to Privacy and Network Sovereignty Challenges," Chapter 1 in Michael Geist (ed), *Law, Privacy and Surveillance in Canada in the Post Snowden Era*, University of Ottawa Press, 2015, pp 13-44; and Bohaker, Austin, Clement, and Perrin, "Seeing Through the Cloud: National Jurisdiction and Location of Data, Servers, and Networks Still Matter in a Digitally Interconnected World," e-Communication Outsourcing Final Report, U or Toronto, Sept. 2015.

He also referred to: Clement, "Addressing Mass State Surveillance Through Transparency and Network Sovereignty, Within a Framework of International Human Rights Law – a Canadian perspective." Chinese Journal of Journalism and Communication Studies, Vol. 23, Special Issue on Internet Governance, 2016 (p 31-52); and Clement, "NSA Surveillance: Exploring the Geographies of Internet Interception," Proceedings of the iConference 2014, Berlin. The latter article looked at the routes that data may take to go from a home device to servers. In 2013 he co-authored Obar and Clement, Internet Surveillance and Boomerang Routing: A Call for Canadian Network

Sovereignty (July 1, 2013), Proceedings of the Technology & Emerging Media Track – Annual Conference of the Canadian Communication Association (Victoria, June 5-7, 2012). He said these papers demonstrate that he was already well sensitized to looking at where data in information systems went and the surveillance risks that it goes through in that journey.

An extensive list of academic presentations from 2013 to 2015 showed that Clement was involved in a number of presentations to academic audiences about internet surveillance after Edward Snowden's revelations. He noted that most of these looked at issues of the exposure of data on the internet to surveillance by the Five Eyes countries. He noted that all of the Five Eye countries have some standing mechanism for doing such surveillance. Clement said that he developed a research tool to help search through the documents revealed by Snowden to further reveal the forms of state surveillance and the risks for ecommunication data. Clement said that his co-author in the study on the risks of outsourcing ecommunications to companies in other countries, Prof. Austin, showed that the data in such communications were more at risk when they left the country because they lost the constitutional protections they enjoyed in Canada.

Clement confirmed he has been researching and writing on privacy and surveillance concerns with respect to digital media and ecommunications since 1992. He published several papers on that topic between 1992 and 1995. He noted that he is still doing research and writing on that topic today, and co-wrote an opinion piece on that topic published in the Globe & Mail on April 23/18, entitled "Facebook: a mass media micro-surveillance monopoly". He noted that just prior to the hearing he had submitted a

new research proposal and is the principal investigator for another grant application to the Privacy Commissioner's Office.

Clement testified that as a result of the teach-in and consultation held by the U of Toronto committee looking at the outsourcing of U of Toronto email for faculty and staff, the Committee was split on whether to proceed with the move to Microsoft's Office 365, due to data privacy concerns. In 2014 as result of this split the Provost decided to stop the pending agreement with Microsoft and redo the RFP process for an email provider. The process did not insist on Canadian sites for the servers but the system had to be free. Google, Microsoft and a third company responded to the RFP. In 2016 they announced they were going with Microsoft Office 365, but that company had opened two new data server centers in Toronto and Quebec. The Provost referred to that new development as a factor as to why U of Toronto went with Office 365. Clement testified that he believed his work on privacy risks had an impact on the second RFP process and the ultimate location of the Microsoft servers.

Clement noted that his expert report for this hearing relied heavily on the 2015 research study, Seeing Through the Cloud: National Jurisdiction and Location of Data, Servers, and Networks Still Matter in a Digitally Interconnected World, co-authored with Profs. Bohaker, Austin and Perrin (exh 27) ("STTC"). That study looked at decisions by Canada's major public universities to use Google apps for education or Microsoft office 365. It found that 21 Canadian universities had outsourced student email to foreign providers, either Google or Microsoft, exclusively. At the time of the study these companies hosted their services in the United States as well as several other countries

around the globe, but not in Canada. To assess the privacy risks of outsourcing such communications, the study looked at relevant statutes, constitutional doctrine, and other caselaw in Canada and the United States, investigating the history of transborder data flows and current North American Internet traffic patterns. The study found that contrary to widespread misconceptions over cloud computing, national jurisdiction still matters, and where in the world your data is located affects which third parties can legally access it, and on what terms. The study also concluded that the ”similar risk” argument that many universities relied on to justify outsourcing their email to U.S. servers, that the risks from US state surveillance were similar to that in Canada, was fallacious.

Based on their year-long research study the co-authors of STTC came to the following conclusions and recommendations:

> -For sensitive digital data national jurisdiction matters: where your data is located affects which third parties can legally access it and on what terms. For example when Canadians store their data in the U.S. it can be accessed by US government authorities on standards that would be unconstitutional if applied within Canada. Also Canadians outside the U.S. cannot expect the U.S. constitutional standards will apply to them. As well, specific U.S. legislation explicitly provides a lower level of privacy protection to the digital data of non-US persons.
>
> -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. 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 protections, particularly their constitutional protections, in the name of potential cost savings that may result from extra-national outsourcing.
>
> - The authors recommended that:

> - Canadian organizations should not outsource eCommunications services beyond Canadian jurisdiction until adequate measures to ensure legal and constitutional protections equivalent to those in Canada are in place;
>
> - When considering e-Communications options, 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 and the risks of using services hosted in foreign jurisdictions.
>
> - Organizations that have already outsourced to providers that place data outside Canadian jurisdiction should revisit those decisions in light of the deeply flawed 'similar risk' assertion and what is now known about mass surveillance practices in the U.S. and possible similar practices in other countries.

Clement acknowledged that he relied heavily on the work and opinion of Prof. Austin with respect the greater risks to privacy and lesser protection for privacy rights for Canadian citizens and residents when their data is stored in the US as opposed to Canada. He noted that Austin's work and conclusions are set out in Austin and Carens-Nedelsky, "Why Jurisdiction Still Matters," (May 31, 2015) (exhibit 28, at p. 3-4).

In the first part of his expert report Clement addressed the question of best practices for organizations considering changes to IT systems and email services respecting potential impacts on the privacy interests of users of such systems and services. He identified four best practices that should be followed in such circumstances. He emphasized the importance of (1) competitive tendering to enable it to assess all the options available before choosing the best one in light of various relevant factors such as cost, privacy, security, user interface, etc. This process allows the organization to look at other factors apart from cost and weigh them against each other. (2) A threat and risk

assessment process (TRA) ensures there will be analysis of all the ways in which a system could be vulnerable, including types of break-ins or interception by third parties including state surveillance agencies. (3) A privacy impact assessment (PIA) is widely recommended when an IT system handles personal information. This is something inherent in an organizational email service because it handles very personal and highly sensitive information affecting a user's privacy rights. PIAs identify potential privacy risks of new systems and help to eliminate or reduce those risks. Privacy risks can arise in a variety of ways including insider access or interception by foreign government agencies when data is outside of Canada. Several universities in Canada that were studied regarding the outsourcing of email in "Seeing through the cloud" prepared PIA reports. Clement noted that the provincial government requires this to be done recognizing that they may have a fiduciary-like responsibility to protect the privacy of individual users. (4) Stakeholder consultations are common for organizations like universities that favour collegial of collective decision-making. This provides a voice for those affected to raise concerns and suggest ways to improve the proposed service. Clement noted that this was done by University of Toronto when it was considering moving to Microsoft Office 365 and they held consultations and town hall sessions with stakeholders.

Professor Clement was given a number of relevant documents related to Laurentian's move to Gmail to review in providing his expert opinion report. One of those documents was the opening statement of employer counsel in this matter describing the process used by the employer to move to Gmail. Clement was asked whether based

on that description the employer had engaged in best practices in its move to Gmail. The employer objected to the question to Clement on the basis of lack of relevance and that there was not an adequate foundation for the question. It argued that the main issue was not one of process or whether the employer engaged in due diligence but was more about whether the move to Gmail was improper because it infringed on privacy interests of members due to the risks to privacy rights it created.

I ruled against the objection on the basis that it was arguably relevant. I noted that one of the issues in the grievance was whether the employer had complied with its obligations regarding consultation and reasonableness under article 2.30 prior to changing existing practices. I also noted that the employer had raised and described the process it had followed in its opening statement so the union was entitled to question that process. I note that at this juncture in the hearing the association had not abandoned its allegation of a breach of article 2.30 regarding changes to existing practices.

Clement noted that the employer had extensive discussions with the faculty association prior to moving to Gmail, and he agreed that was a form of consultation but said it was not the form he would regard as best practice. He saw no evidence of a PIA or TRA or a competitive RFP in the description of the discussions or process followed prior to adoption of Gmail.

Prof. Clement explained the distinction between informational privacy and security. He said these terms are often improperly conflated. Security measures are to ensure that only authorized parties have access to the information or data and protect against unauthorized access. But privacy deals with the matter of who can access

personal information and under what circumstances. Thus a facility or system may be seen as secure because there is no unauthorized access allowed but it may be seen to be lacking in privacy of personal information because of who has authority to access an individual's personal information. Thus personal information may be held in highly 'secure' systems, but individuals may still regard them as highly privacy invasive due to the parties that are authorized to access their data in that system. For example, in the case of Gmail, U.S. security and law enforcement agencies seeking access to Canadians' data held in US based servers are relatively unfettered by the laws that protect Americans' data. Thus in some cases security measures designed to protect personal information may in themselves pose additional privacy challenges. Clement noted that in such cases privacy commissioners in Canada have typically applied a four-part balancing of interests test to determine whether the security measures are appropriate. Under that test the following factors are analyzed: Necessity – there must be a clearly defined necessity for the use of the measure in relation to a pressing societal concern; Proportionality – the measure must be carefully targeted and tailored suitably so that it is seen as reasonably proportionate to the privacy of the individual that is being curtailed; Effectiveness – the measure must be shown to be empirically effective at treating the issue and connected to solving the problem; and Minimal Impairment – that the measure be the least invasive alternative available. This test was identified as a Canadian standard taken from the Canadian Privacy Commissioner's website.

Clement relied on the Austin paper for his knowledge and statements on the meaning of security and how it differs from privacy. He relied on documents released by

Snowden with respect to what analysts use to decide whether to access particular personal information. He said on of the tests used was whether the person was a U.S. citizen in the U.S. or not. If they were not then the analyst had more access under laws providing them with authority to access such information.

Prof Clement accepted that there are inherent risks of using email generally, including risks that arise from its complexity and geographic scope. He noted that the transporter system for emails offers many points at which messages can be covertly monitored and intercepted. There are also risks of hacking in any system. For that reason no absolute security guarantees can be given. However, he said there are numerous ways to reduce these risks along the way, measures to be adopted appropriate to the circumstances to make email more secure. He also took the position that under FIPPA the university bears a responsibility to adopt best practices to assess and mitigate these risks. He took the position that in addition to administrative and technical measures the university should also take steps to ensure that communications are not unnecessarily exposed to foreign jurisdictions and associated security intelligence agencies. He noted that a significant proportion of university email involves senders and receivers who are both on campus. For those emails storing and routing it through the US and putting it in the hands of a US corporation adds significant privacy risks that can be avoided with on campus hosting. He also took the view that hosting servers within Canada offered similar benefits, especially if near campus. He took the position that both in terms of legal jurisdiction and the extent to which Canadian law and protections are effective, there is an enhancement to privacy protection if email servers are kept in Canada. He said if the

servers are in the US than Canadian data is considered to be foreign and thus not subject to US protections for privacy. He said that as long as the servers are kept within Canada that reduces the risk of interception because of the limited geographic scope and removing the risk of such date going abroad for storage.

Prof Clement was asked if a member of a faculty at a Canadian university, who has the protection of academic freedom, has any distinct or enhanced privacy interests compared to other types of employees. He said that generally when employees use an an employer email service they lose some of the privacy rights they enjoy as a citizen, because they are communicating via employer owned equipment for work duties. However, in his view faculty members at a Canadian university are not considered employees in the same way, because such institutions are unique in their adherence to the principle of academic freedom to ensure that faculty can engage in independent critical thought and expression without fear of sanction. He views the protection of private communication from unwanted access by those in positions of power who may take exception to faculty opinions or lines of research as an essential aspect of academic freedom. He also expressed the view that the responsibility of Canadian universities to protect faculty communication is heightened in the current political climate of strong controversies over government policies. He noted that in that current climate there may be faculty members in Canadian universities whose academic and social networks or even their country of origin may be regarded as threatening by the U.S. administration. Prof. Clement referenced one of the conclusions from Seeing Through the Cloud on this concern:

> The choice of e-Communications provider should be made in full consideration of the impact of extra-national outsourcing on the mission and purpose of universities, on teaching and research activities and of the staff and students to uphold the principle of academic freedom. (p. 22)

Clement also noted that the threat to secrecy of faculty members can be done on a number of bases, starting with their names, their associations, and their country of origin. He said there are a lot of ways in which an individual can be found to be suspicious with consequences for their privacy. He said that the Snowden documents revealed that the screening of communications is based on the use of trigger words and social connections or who one is communicating with. He noted that even if emails are encrypted the header and email addresses cannot be encrypted. He said this meant there were a lot or ways in which academic communications can put someone at risk. He also noted that the use of data analytics technologies is common in web applications for the National Security Agency. He noted that these technologies allow them to use words, phrases or email addresses for analysis, and when they show up in a data stream that becomes a trigger to pull those communications out and build a data stream for further analysis. He gave as an example the use of the work 'jihad' as revealed in the Snowden documents. Thus if an academic was doing research on 'jihad' and used it in emails, that could trigger the analytic technology screen.

Clement said these types of concerns could impact on academic freedom by raising questions about whether faculty have to be careful about the terms you use in emails or documents in order to protect themselves or grad students (and possibly Muslim students) to ensure they do not become the subjects of surveillance.

Prof Clement then addressed the issue of what risks to faculty members' privacy interests result from a Canadian university providing email services to its faculty through a company that stores emails on servers located in a country other than Canada, and whether there were particular privacy concerns raised if emails are stored in the U.S.. He noted that once the data of Canadian faculty leaves the country it loses Canadian legal and constitutional protections. When in the US it is treated as foreign and does not enjoy the protections afforded to US persons. He noted that in the US it also becomes subject to surveillance by the NSA, and according to the Snowden documents the NSA has partnered with Google and 8 other major US tech companies to provide direct access to the servers of these companies through the PRISM surveillance program. He said he was unsure of the status of that agreement today. He also noted that under s. 702 of the Foreign Intelligence Surveillance Act Amendments Act (FISAA) the NSA can obtain authorization for broad interception powers without the need for individual warrants. Clement also noted that the NSA has used that legislation for implementation of its "Upstream" surveillance programs that allow for the interception of bulk data flowing through switching centres of major internet service providers. He took the position that there were grounds to support the belief that the NSA has a sufficient number of intercept points to allow it to monitor nearly all email passing through the US. He said both the PRISM and Upstream programs enabled it to scan emails in bulk and assemble secret dossiers on a large number of individuals. He said the NSA had been doing this since the early 2000's. He said that by placing interceptors or scanners in 18 switching centres it can scan close to 100 percent of all emails in the US. He also noted that to the extent the

emails are stored on servers in other countries it becomes subject to the laws of those countries and is exposed to further risks of foreign surveillance.

Clement was then asked if the privacy interests of faculty at Canadian universities could be enhanced by the university providing its email services to its faculty through a company that stores those emails on servers located in Canada. He said the answer was yes presuming that other security and privacy protections/risks remained comparable. Storing emails on servers in Canada meant they remain under the protection of Canadian privacy laws and privacy rights under the Charter of Rights and Freedoms. He said it also made it more likely that they would remain under protection of Canadian law when in transit between sender and receiver if they are both in Canada. He admitted that for it to stay in Canada throughout it would require that all of the sender and receiver, and the cloud server for the network, would have to be in Canada and the email would have to be routed through a switching centre in Canada.

Clement noted that in 2015, when they conducted the outsourcing study, 14 Canadian universities provided their faculty with email services that were hosted in Canada. He noted that these included the BC universities that were subject to British Columbia's Freedom of Information and Privacy Act (FIPPA). That act was amended in 2004 to require Canadian storage of personal data held by pubic sector institutions. Clement also stated that Microsoft had recently established two data centres in Canada, which provided the University of Toronto with justification for completing its move of faculty and staff email to Office 365 after a prior proposal to move to that company was halted by the Provost following objections to extra-territorial outsourcing.

Clement was asked whether there were any enhanced privacy protections associated with Gmail compared to other email services such as Microsoft's service. He said he was not aware of any such enhanced privacy protection offered by Google as compared to Microsoft. He noted that Microsoft had set up two Canadian data centres to apparently address some of the privacy concerns expressed by Canadian universities and also noted that Microsoft might also be more privacy protective than Google because the latter's business model is largely based on collecting and monetizing personal information whereas Microsoft's is based on selling software services. Thus Google has a greater incentive to collect and analyse personal data. Ultimately his conclusion was that all other variables being equal, universities that provided email service themselves or obtained those services from companies with servers in Canada would result in better protection with regard to privacy interests and academic freedom and any threat that surveillance poses to faculty and students.

In cross-examination, Prof Clement agreed that his expert opinion report relied heavily on the findings of himself and his three co-authors in *Seeing Through the Cloud, supra.* He admitted that he expressed opinions on legal matters in his expert report but said when he did so he was relying on the findings and conclusions of his co-authors with legal expertise in the area of privacy, Prof. Lisa Austin of the U of Toronto Faculty of Law and Dr Stephanie Perrin, who he described as an internationally recognized privacy expert. He noted that Dr Perrin had been a civil servant in the Federal Government for many years and was a lead proponent of the enactment of PIPEDA in the 1990's. He said that his opinions about national jurisdiction and the consequences for legal protection of

privacy interests that flowed from data leaving Canada were shared with his co-authors of Seeing Through the Cloud. He acknowledged that he was not an expert on the law and he deferred to Prof Austin and Dr Perrin on legal issues but he added that he had discussed the issues arising from the impact of national jurisdiction on privacy protection with Prof. Austin a great deal.

When it was pointed out that the rationale for many of his statements on legal protections in his expert report were not contained in the report, he replied that one had to look to the *Seeing Through the Cloud* report for that rationale. When it was pointed out to Clement that the *Seeing Through the Cloud* paper recognized that the Charter did not restrict the U.S. government from looking at Canadians' data, he said that was correct but it did restrict the reach of Canadian agencies when responding to requests from the US authorities for access to Canadian data. He accepted that the Charter did not apply to the US government and said that was understandable.

Prof Clement agreed with the suggestion that a highly secure data system does a good job of protecting information from unauthorized access to data. He agreed that unauthorized access can be by outsiders who have no right to access but force their way in. He said that would include hackers but noted that this term can include "white hat hackers" who contend they are not a threat to security. He also noted that the NSA claim they are not hackers because they claim they have authorized access. He said the FISA Amendment Act of 2008 was enacted to retroactively render legal what the NSA was doing with respect to scanning and intercepting emails and give legal immunity to the

telecoms that had been giving access to the NSA. But he agreed that hackers pose a significant threat to university email systems.

Clement also agreed with the suggestion that the threat of unauthorized access by a hacker was a risk that he presumed to remain comparable in his answer to question 6 about the enhancement of privacy interest protection if the email provider has servers located in Canada. However, he admitted that he had no knowledge of the old Novell email system and the new Gmail system at Laurentian with respect to the threats from hackers in both systems. Clement also agreed that unauthorized hackers can also include inside users who go beyond their authorized access to the system. It was put to Clement that the threat of unauthorized access by the inside user was also one of those threats or risks that he had to assume were comparable to sustain his answer to question 6 in his report. He replied that such a risk did not have to be absolutely comparable to maintain there was less risk from an email provider with servers located in Canada. He said there had to be a weighing of the various threats to decide on comparability. However Clement said that he had not assumed any differences between the two types of systems with respect to insider threats of unauthorized access.

However, he agreed there could be a very insecure email system that is located solely within Canada. He further agreed that there was a hypothesis that insider threats or risks are greater for an in house email system versus a cloud-based system. But he also said you could have an on premises system with a very committed IT staff to protect against insider threats and could also have less committed staff with no community commitment in a larger cloud based system. Clement said he would not presume a

greater insider threat in either type of system, but he accepted that the insider threat was a very complicated problem for IT staff to deal with and noted that it would show up on any PIA or TRA threat assessment if properly done. He acknowledged that threats from both hackers and insiders should be taken into consideration when considering security measures, including physical security and access measures, technical security measures and administrative security measures. Clement also accepted that the Canadian Charter did not bind hackers and malicious insiders and did not protect university email systems from those individuals. He acknowledged that protection from those threats can only come from reasonable security measures.

Clement also accepted that his definition of security referred to protection from unauthorized access or disruption but should have included protection from loss of data. He agreed that a lost laptop with unencrypted emails on it presented a security problem. He said he did not assess that threat with respect tot the old Groupwise Laurentian email system. He agreed that a responsible university should assess the risks of a lost laptop by imposing reasonable security measures. He further agreed that one way to address that problem is to have a system in which emails are not stored as emails at all. He also agreed that one way to protect against the problem of the lost laptop is to not put emails on the laptop at all. One way to do this is to have the emails stored in the cloud on a Google server and accessed using the Internet. When asked if the loss of a local device as compared to storage of emails in the Cloud were things that he had to assume were equal for his answer to question 6, Clement said no he had assumed that one would have

measures to protect against data loss for both systems, one with storage in Canada and one with storage outside of Canada.

Prof Clement agreed that his expert report was in part about the risk of surveillance by foreign intelligence agencies. He said he was interested in what these agencies do in terms of signal intelligence surveillance of electronic signals and systems typically used by foreign targets. He described it as spying on electronic communications. He noted that many countries do this, including the U.S., Canada, Great Britain, New Zealand, Australia, China and Russia. Clement identified foreign and signal intelligence programs or legislation as parts of a country's national security program. He did not take issue with the fact that countries have foreign and signal intelligence programs but he thinks that the extent to which they have taken such programs is questionable. He admitted he had never worked for such an organization so had no first hand knowledge of how they worked, but said he had learned a lot about those issues by studying the Snowden documents with respect to U.S. foreign intelligence agencies. He said these documents were a main source of his information on how U.S. foreign intelligence surveillance works but he has also read extensively on other sources about the operation of the NSA and foreign intelligence.

He described the Snowden documents as raw documents with no descriptions of their contents for the layperson. However, he noted there has been no challenge to the claims made in the documents or their authority. No one has disputed that they exist. He acknowledged there had been some dispute about these documents but there has been

general agreement on the capacity of the NSA to intercept a large portion of Internet traffic that goes through the U.S.

Prof Clement has written about the NSA program known as 'Upstream' in his 2016 – 2017 paper titled "Addressing mass state surveillance through transparency and network sovereignty, within a framework of international human rights law – a Canadian perspective", Chinese Journal of Journalism and Communication Studies, p 31-52. (exh 30, tab 1). Page 6 of the article contains a slide from the Snowden documents referring to two of the main programs that the NSA used to scan and monitor and collect electronic data, Upstream and PRISM. Upstream allows them to screen and collect communications while they are in transit between the sender and receiver. PRISM enabled the collection from the servers of U.S. service providers. The slide noted that s. 702 of the FISA Amendment Act authorized both types of surveillance and collection by the NSA. In this paper Clement claimed that Canadians needed to be better protected from the NSA Upstream program. In the paper Clement argues that Canadian communications should be directed away from the NSA programs by trying to ensure that email systems are both stored and routed only within Canadian territory. He said his argument was based on data and study. His data was derived from the International Exchange MAP platform, known as IXMAP. He described an international exchange as analogous to a telephone exchange, referring to the points where there is an exchange of information over fibre optic cables. In 2012 there were 85 IX's in the US and only two public ones in Canada, Toronto and Ottawa. Today there are 10 in Canada. Clement said

one of the purposes of this paper was to show the consequences of the tremendous imbalance in Internet infrastructure. He said that imbalance continues to exist today.

Clement's 2016 paper concluded that the infrastructure imbalance caused a lot of Canadian Internet traffic to boomerang through the U.S. even where sender and receiver and email servers were all in Canada. He said the amount of boomerang traffic into the U.S. depended on a number of factors such as where the fibre optic cable was laid, and the infrastructure and decisions made by Internet service providers. He said the example of an email in the U of Toronto system from himself to a U of Toronto colleague being routed through transmission lines and a U.S. IX was not caused by infrastructure but rather resulted from a decision made by an Internet provider and different companies in the system. So in fact boomerang traffic is not caused solely by the infrastructure imbalance. It results from a number of factors. In the 2016 paper he found that 28% of same country Canadian communications followed a boomerang pattern or routing through the U.S. (from 2009 to 2016). He agreed that there was still a significant pattern of Canadian electronic communications going on a boomerang route through the U.S. He also found in 2016 that 81% of communications between Canada and third countries were routed through the U.S. He agreed with the suggestion that while these figures were not limited to email traffic we could infer that emails would follow a similar pattern. He agreed that an email from an on campus email system user to someone in a third country was likely to be routed through the U.S.

Clement noted that there is a Greater Toronto Area Internet web that makes it more likely that for universities in the GTA email between them are more likely to be

routed within Canada. But he agreed that for emails between on premises servers at one university to on premises servers in another university a significant portion of that email will be routed through the U.S. He still maintained that universities are special to a certain extent because some have been unique in developing their own system to keep traffic in this country. But he agreed that the main reason he wrote the paper was to point to the importance of national sovereignty with respect to the internet usage and to point to the risks presented by the routing of data and in particular the potential impact on privacy interests of boomerang routing of internet traffic. It was to bring the international routing of data on the internet into a human rights framework and call for an international order for internet governance.

Clement was asked if his paper in fact recognized that the localization of email system cannot solve the problem of internet surveillance because one cannot keep such communications solely inside of single countries, that being inherently contrary to the nature of the Internet as a global environment. Clement replied that if one wants to maintain email and Internet communication within a framework of international law then having it travel through the US undermines that objective. He asserted that privacy regulation and protection in Canada has been comparable to that which is in place in Europe. He said his central point was to call for the creation of a robust law of communications that can be relied upon to protect our rights.

Clement identified PRISM as a program used by the NSA to collect data directly from the servers of the ISPs, but said that the Upstream programs that enable the interception of data in transit have an even wider reach than PRISM and the telephony

meta-data collection programs of the NSA and are arguably the most challenging to human rights (exh 30, tab 1, p 5-6). He clarified that by "wider reach" he meant that it potentially captures all of the Internet traffic, including all of the traffic between the servers of the ISPs and Internet transactions apart from the traffic of the ISPs. He said it was worse than PRISM with respect to its wider range of communication interceptions but said it might be less intrusive in that it required that the packets of data intercepted had to be reassembled. He said he did not intend to say one was worse than the other in terms of being a threat to privacy interests. When asked if he stood by his statement in 2016 that Upstream was a bigger threat to human rights, he said it presented a bigger risk for people whose activities were most likely to draw the attention of the foreign surveillance agencies. When asked if Upstream was a bigger concern for academics he said he would not say that but instead said those programs were both equally concerning.

Clement agreed that if the employer had the on campus email system that LUFA desired and someone sent an email from that system to the US it would transit through the US and be subjected to the risk of collection by Upstream. He said he was not aware of the percentage of Laurentian faculty emails that went to or from the US. But he was aware that there were a number of Canadian universities that had moved to email systems that were hosted by US companies with servers in the US and agreed that communications between Laurentian faculty (even assuming an on campus email server) and people at those universities will go to the U.S. He said if the other school was using Microsoft 365 because it now had servers in Canada then the email was less likely to go to the US. However, he noted that due to the routing practices of Canadian ISPs, if the

university used Bell or Telus as an ISP, then the data is likely to be routed through the U.S. He also agreed that his paper listing of the other Canadian universities that had moved to Microsoft 365 did not indicate whether the email systems for those schools were using only the Canadian servers or possible using other servers.

Clement agreed that emails sent by Laurentian users from an on campus email server to persons in a third country will often transfer through the U.S. while in transit. He did not know how much of Laurentian emails were with persons in a third country. He also agreed that email sent by a Laurentian faculty member to another Canadian University would regularly be routed through the U.S., by his estimate somewhere between 25 and 30% of the time. He said that email sent intra- campus does not have to go off campus and thus is generally not exposed to Upstream. But he agreed that the purpose of a university email system is to enable faculty and students to communicate with anyone in the world and thus be able to reach anyone globally from their office almost instantaneously.

Clement agreed that email message content can be encrypted when an email is sent. This means that the data is encoded to protect against unauthorized access while it is transit. While encryption can be broken or circumvented that is not easy to do. In his paper on "Canadian Internet Boomerang Traffic …" (exh 29, p. 32), Clement described the development of encryption as valuable and necessary but said this alone was not sufficient to adequately address the threat of surveillance by state security agencies. Clement did not appear to take issue with a document the employer presented on Email Encryption FAQs (Exh 30, tab 3). That document made the point that all Gmail is

encrypted while in transit but can only be guaranteed as protected by encryption throughout the transit where both the email providers of the sender and the recipient support TLS encryption. Thus email from google user to google user is protected by encryption. Encryption for data while it is stored on a system's servers is different from transit transcription so that transit encryption does not protect from surveillance by PRISM. Clement said he did believe that more email systems today were implementing email encryption due to the Snowden revelations.

Clement said he had no reason to dispute the claim in a NY Times article of June 23/17 that Google Gmail has more than 1.2 billion users and that Google announced it would no longer scan users' gmail for targeted advertising purposes. He agreed that to the extent that Laurentian Gmail users communicated with others who also used Gmail they could expect those emails to be encrypted and relatively immune from Upstream, at least more so than if it was not encrypted. Clement also did not dispute the claim in a Tech Crunch article from 2018 (exh 30, tab 5) that Google's G Suite for Education had 70 million users around the world.

Prof Clement was asked about the reference in his expert report (at p. 7) to Canadian data becoming subject to surveillance by the NSA when it leaves Canada and losing Canadian legal and constitutional protections when in the US. He made the statement that based on revelations in the Snowden documents that under the PRISM program the NSA has 'partnered' with Google and 8 other major US tech companies to provide 'direct access to their services for conducting its surveillance operations. However, he agreed with the suggestion that this access was authorized by section 702 of

the FISAAA, and added he thought it was also authorized by the Patriot Act. He also agreed that the use of the term 'partnered' might imply mutual intention and consent and acknowledged that in fact the access given to the NSA was actually a matter of complying with section 702 and agreed that the ISPs take the position they were compelled to provide access and did not do so willingly.

Clement agreed that the release of the Snowden documents provided information on NSA activities that were formerly secret. He was not sure if it led to the further declassification of information by the NSA. He said he understood that although Snowden handed over classified documents to the media those documents remained classified. However, he did not agree that the release of the Snowden documents led to greater transparency at the NSA. Rather he said it led to greater attention being paid to the NSA and the Director of National Intelligence being required to provide greater context for what the NSA was doing.

Clement agreed that one body that gave more transparency to NSA activities was the Privacy and Civil Liberties Oversight Board (PCLOB), which has a mandate to oversee the NSA's FISA activities. When shown the legislation that created the PCLOB and set out its functions and mandate (42 USC 2000ee) Clements noted that he had not seen that legislation before. He said he was aware of the PCLOB and its function of overseeing the NSA's FISA activity, but had not been aware prior to the hearing that it was an independent agency. He said he was not surprised to learn that the PCLOB had access to classified documents, or that it was comprised of a Chair and four other members selected by the President with the advice and consent of the Senate. The

legislation also indicates the members of PCLOB are expected to be bipartisan and chosen solely on the basis of qualifications and experience and expertise in the areas of civil liberties and privacy, without regard to political affiliation. Clements said he would expect that to be the case in terms of the legislated criteria but he also recognized the possibility of a discrepancy between what should be the case and what actually exists in fact with respect to bipartisanship.

Clement was somewhat sceptical of the ability of PCLOB to provide effective oversight of the NSA and other agencies. When asked if reading the statute setting out the composition, selection criteria and mandate of the PCLOB had changed his views, Clement said that was not the case. He based his views in part on the recent experience of the appointment of a new U.S. Supreme Court Justice (Kavanaugh) that led him to question the neutrality of appointments, but said his scepticism was not based solely on that appointment and he had it prior to that incident. He said this was highly contextual area and statements by officials on these issues cannot always be viewed as accurate. He said officials have on some occasions blatantly lied in statements made to Congress. Clement said he did not question the sincerity of attempts to establish oversight mechanisms. He said he was also initially sceptical of Snowden in the same way but came to trust his revelations as he came to learn more about his background. Clement trusted Snowden as a more reliable reporter that the Director of National Intelligence.

Clement said he was not aware that PCLOB held public hearings into Snowden but said that was consistent with its mandate. He was not aware that PCLOB had found that the program called 'Bulk Telephony' was unlawful, but he was aware that program

was revealed by the Snowden documents and was declared unlawful after those revelations. He was not aware that PCLOB recommended that the Bulk Telephony program be discontinued. He said this could help to change his views on the effectiveness of PCLOB. He said he was not specifically aware of the fact that PCLOB had studied PRISM and Upstream as well but he would have expected it to do so. He has not read the report of the PCLOB on the Surveillance Program Operated Pursuant to Section 702 of the FISA, July 2, 2014 (exh 30, tab 8) and was not aware of it in any detail prior to the hearing.

On page 22 of the above noted report, PCLOB notes that Section 702 authorizes the targeting of non U.S. persons only if they possess or are expected to receive or likely to communicate foreign intelligence information. When asked if he was aware of this limitation on targeting of non-US persons, Clement said he understood that was the rationale for such targeting. When it was pointed out that this limitation is set out in 50 USC s. 1881a (a) (exh 30, tab 6), Clement said he had not seen the legislation before but was aware of it. He agreed that the authorization of surveillance under section 702 applies to a program of surveillance and not warrants for specific individuals. He said that was why his report referred to the NSA being allowed to operate without individual warrants when conducting such electronic surveillance. He agreed as well that this was why the term "programmatic surveillance" is sometimes used to refer to surveillance under s. 702 of FISA. But Clements also agreed that in order for there to be a s. 702 surveillance program there has to be a Court authorization of the program by a FISA court, known as a Foreign Intelligence Surveillance Court (FISC). He also said he was

aware that a FISC authorization is based on a certification given by the Attorney General and the Director of National Intelligence.

Clement also said he was aware that there were core requirements to be included and satisfied in a certification for a FISA surveillance order but was not aware of a requirement that it be consistent with the 4th amendment of the US Constitution. He said he was generally aware that the authorities were required to report on any non-compliance with FISA orders. He was also aware that, once s. 702 acquisition has been authorised by a FISC order, the acquisition is done by the sending of directives to the ISPs (exh 30, tab 8, p 32). He said he also had a general understanding that the ISP's can challenge a FISC order in court.

Clement was asked several questions about excerpts from a PCLOB hearing held on March 19/14 (exh 30, tab 9). That excerpt described the use of PRISM and Upstream under a FISC order and the fact that such a data search is targeted by the use of selectors like phone numbers or email addresses. Clement said the excerpts referred only to those two types of selectors but he said that targeting could be broadened by using other selectors like mac address or IP address. When it was put to him that s 702 surveillance orders are limited to identified persons he noted that mac and IP addresses can be linked to persons as well. He said that the way a person can be targeted can be quite broad. He also said that the hearing excerpts assumed that the authorities were complying fully with the FISA in terms of their choosing of selectors according to the wording of the statute, with a goal of acquiring foreign intelligence.

Prof Clement was asked if he accepted that the U.S. collection of the data of non-U.S. persons was constrained by the requirements of s. 702 of the FISA. He said he believed that there was still illegal activity going on because he was not aware of new oversight mechanisms to protect against that. He was not confident that existing oversight mechanisms can be relied on based on their public mandate because there is so much obfuscation regarding current practices and outright lying by the surveillance agencies. He suggested the employer here was asking us to put all of our faith and trust in the FISC as a secret court with no adversarial process. Clements said we need a more open execution of the processes under the FISC. He suggested that with the Snowden documents we can begin to form opinions outside of what is provided by the FISC. He said one of the reasons for his scepticism about exiting oversight mechanisms was the testimony of James Clapper in 2013 to a Senate committee. He was asked by a senator if there was collection on masse of surveillance of Americans and his reply was, 'no not wittingly'. Then a few months later Snowden released his documents and Clapper was called back to testify and asked about his earlier answer. He said his reply had been the least untruthful thing he could say. He said that type of answer makes him sceptical of any claims that are made about the effectiveness of FISA processes. For that reason he does not think that reasonable people should take at face value assurances that when their data is going though communication channels in the U.S. it is safe from NSA access.

The excerpts from the PCLOB hearing referred to above (exh 30, tab 9) also revealed that the NSA has to meet the statutory requirement of having a valid and FISC approved foreign intelligence rationale for targeting particular communications or data in

addition to identifying the target as a non-US person reasonably believed to be abroad. Prof Clement said he was aware of that requirement but said there remained questions raised about whether that rationale requirement could be relied upon because of the problems raised by whistleblowers like Snowden and others. He said he was also aware of the fact that the targeting rationales being used by the NSA are reviewed regularly by the Director of National Intelligence and the Justice Dept., but he was not aware that they were reviewed every 60 days. He said he understood there were audits and spot checks of that activity that were required. He acknowledged however that his knowledge of compliance oversight of the NSA was limited, but noted that much of it was secret until recently.

Prof. Clement was asked about his knowledge of Presidential Policy Directive PPD-28, issued by President Obama on January 17/14 (Exh 30, tab 11). He said he was aware that President Obama issued some kind of directive in response to the Snowden documents but was not familiar with the specifics of the document. He was informed that this directive was retained by the Trump administration. The directive is made to the US intelligence agencies including the NSA and is intended to address the privacy concerns raised by US surveillance of non-US persons and required that they only take actions that are properly authorized under statute or executive order in accordance with applicable statutes. Clement was not aware that it made express statements about the protection of privacy interests of non-US persons and required that signals intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate

privacy interests in the handling of their personal information. Clement was not aware of the specific principles set out in this policy directive or the specific directives concerning adherence to those principles. He was simply aware that the President had issued some assurances concerning intelligence agency activities. He was also not specifically aware that the directive made the PCLOB responsible for oversight of compliance with the directive by US agencies but he had a general understanding in that regard.

Prof Clement said he was not aware that the PCLOB had issued an implementation report on this directive that was recently declassified. However, he said he was aware that the US and the EU had entered into an EU-US Privacy Shield Agreement. He agreed that it was an important agreement with commitments that enabled the protection of personal data that flows from the EU into the US for commercial purposes, and it renewed annually. The employer introduced the first annual report issued under the Privacy Shield (exh 30, tab 12). That report identifies PPD-28 and FISA section 702 as the US legal rules that are particularly relevant for the compliance with the Privacy Shield. Clement agreed that it appeared that the EU was relying on PPD-28 to ensure adequate protection of the privacy interests of EU citizens. He said however, that he did not agree with such reliance on PPD-28 and said there were people who did not think this was sufficient, although he admitted that there were some EU officials who regarded this as adequate. He said he believed there were some challenges to the Privacy Shield going on now. Clement thought that a prudent person with options to not send data to the US should explore those options.

Prof Clement's 2016 paper, "Addressing Mass State Surveillance Through Transparency and Network Sovereignty …" (Exh 30, tab 1) identified 13 Necessary and Proportionate Principles as part of an international human rights law response to concerns about state surveillance of internet communications. He said these principles were identified and issued by a Coalition of Privacy Experts in 2013 after the Snowden revelations. He said they are principles for judging the appropriateness, legality or justness of surveillance of Internet communications by intelligence agency operations. He described it as an attempt to recognize the need for surveillance but to bring it within international norms for human rights and privacy.

Prof Clement said the transparency principle suggests that individuals should be given information about surveillance so they can make choices about how they use the Internet. He agreed that the purpose of this principle is for user choice to be able to mitigate the impact on personal privacy from surveillance of the Internet. He also agreed that in the US some ISPs have lobbied for greater transparency and identified Google as a leader in that respect. It was the first ISP company to issue a transparency report on requests that had been made by intelligence agencies for access. Google did this in part in response to the use of the word 'partnered' by the NSA. Google's report for 2018 and prior years was issued on Nov. 13/18 (exh 30, tab 10). The employer produced the part of that report that dealt with US national security requests for access. Prof Clement said he did not look at this report for the purposes of preparing his expert report, but said he had referred to it in the past and relied on it as a model for Canadian telecom companies to follow.

Clement agreed that the content requests in fact tracked PRISM requests and when it requested tracking of an email account it was like a switch being flicked on that email account that allowed the NSA to capture everything to and from that account. He agreed that the reporting was done for 6-month periods. The report for July to Dec. 2017 suggested the largest number of users affected by such a request was 65, 499 out of a total number of Google users of Gmail of 1.2 billion.

Prof. Clement agreed that Canada has its own signals intelligence agency known as the Communications Security Establishment (CSE, or CSEC). It operates under powers given to it under the National Defence Act. It is not permitted to direct surveillance at citizens of Canada. However, it is allowed to target a foreign person or entity who is communicating with a Canadian citizen. Thus a Canadian researcher of terrorism who is communicating with a foreign target may have their communications intercepted. However, Prof Clement noted that a Canadian person having such communications is protected by the Charter with respect to CSE surveillance of their communications. He said this was the point about privacy protections made by Prof Austin in her article claiming that territorial nationality matters when it comes to Internet communications and IPS providers.

Prof Clement was taken to a tweet he sent out on Sept. 22/14 in which he sated that CSEC (now CSE) spying was a secretive, extensive, and out of control. He also tweeted a link to a video about the extent of the CSEC spying of online communications. That video warns that CSEC can collect and analyze an individual's private communications data without a warrant and can include their emails and phone activity.

It warns that it shares Canadians data a with foreign spy agencies as well. He stated that this tweet was a repeat of a tweet by Open Media. When asked if he believed that tweet when he sent it out he said that he did. However, he noted that at the time of the hearing there was a new bill to change the oversight of CSE, Bill 59. He said this was a change from 2014 in that the new Bill was an attempt, for the first time, to bring Parliamentary oversight to the activities of the CSE. Clement said that up to this time the CSE was the only signals surveillance agency that was not overseen by Parliament or some government agency. He said there was no real equivalent to the PCLOB in Canada. The CSE has a Commissioner but that person has no authority to make a binding recommendation and the office has shown no transparency and reports only to the Minister of National Defence. The Minister of National Defence authorizes programmatic surveillance on his or her own. Clement agreed that after the Snowden revelations the US does have more oversight of signals communications surveillance than Canada in a formal mechanistic sense. However he said that in a practical sense in terms of the risk of running afoul of state security agencies he did not know which country was better. However, he asserted that if we believe that the Charter still applies to protect individual privacy rights regardless of oversight of the CSE, then the Canadian person is still protected by the Charter with respect to access to his or her data as long as it stays in Canada.

To clarify, Prof Clement stated that if one has an email system that operates solely in Canada then ones data is at risk from whatever the CSE is doing. But if an email system has servers in the US then the Canadian user has the risk of both CSEC problems

and the added risk of US agency surveillance. Clement said he did not have a strong basis for trust and he is suspicious of surveillance unless he has good evidence on compliance with oversight. He also conceded that the CSEC and the NSA and other 5 Eyes agencies work very closely together and to try to separate them out is difficult since they share so much surveillance information.

Clement was asked if he subscribed to a theory of 'trust no one' for data security. He said he did not go that far, but believed that trust had to be earned and we should avoid adding extra risk if it is possible to do so. He also said he believed more or less all of what was said in the Open Media video on CSEC that was played at the hearing during his cross-examination. He agreed that the book of essays entitled "Law, Privacy and Surveillance in Canada in the Post-Snowden Era (2015, U of Ottawa Press, edited by Michael Geist) was an authoritative resource for looking at the law and policy of surveillance in Canada. The employer introduced a Chapter from that book written by Prof. Craig Forcese entitled "Law, Logarithms, and Liberties: Legal Issues Arising from CSE's Metadata Collection Initiatives". Prof Clement had read the paper before and said Prof Forcese was a well-recognized authority on National Security Law. He said the paper focused on the metadata surveillance program of the CSE. He noted that Snowden had leaked some details about the CSE program. He noted that this program was used by CSEC to find out who was communicating with who over the Internet. Prof Clement agreed that one of the thesis presented in this paper is that the CSEC metadata surveillance program was a violation of the Charter (at p. 149, exh. 30, tab 13). He said he agreed with that view.

Clement was also asked about the fact that Prof. Austin, in her paper "Why Jurisdiction Still Matters" (Exh 28), under the heading Legal and Practical Risks, acknowledges that access to private communications by CSEC in contravention of the Charter is a practical risk for Canadians given the weak oversight of Canadian spy agencies (at page 31). Prof Clement said he agreed with that view. However the Austin paper goes on to suggest that because such a claim accepts the proposition that Canadian agencies are likely acting illegally with little actual evidence it is too speculative to accept as presenting similar risk to US surveillance for data stored or transmitted in the US. It was put to him that the risk of illegal surveillance by the CSEC could not be both a practical risk and a speculative risk. Clement replied that there could be some ambiguity about whether there is a practical risk, and agreed one could not be sure of the extent of such risks. He said he did not accept that it was wrong to make decisions based on a practical risk because it would endorse illegality. He said he thought that in the case of uncertainty about the degree to which the CSE is acting illegally and the scope of such activity, that would not make added exposure to US based signals intelligence surveillance an insignificant increase in risk to privacy. Clements noted that Austin was saying it is wrong in principle to make decisions based on an assumption that CSEC is acting illegally. When asked if this put principle above practicality, Clements said one had to consider the various elements of risk. One element is that CSEC may be acting illegally in accessing data through meta data programs. But that element does not mean there is no reason to give up keeping ones email in Canada to avoid the added U.S. risks. He said Austin is saying there may be risks of state surveillance even if one has local

email systems but that is not a justification for adding the risk of going to the US with email.

Prof Clement agreed however, that if you are a Canadian researcher on a local email system who communicates with foreign sources then you really ought to take precautions to protect your email from CSEC if you are at the extreme of communicating with individuals who are risky in terms of attracting surveillance. He said that should not be the case if communicating with foreign sources who are not identified as a risk. He also agreed that if a Canadian researcher does research on terrorism they should take steps to protect themselves from CSEC and agreed there were devices for doing that, albeit devices that are less convenient than regular email. Finally, Prof Clement agreed that, as stated on page 3 of his paper "Addressing Mass State Surveillance …" (Exh 30, tab 1) he wrote that paper from the perspective of a privacy advocate with an interest in privacy protection for university faculty members. He said he was still a privacy advocate at the time of his testimony.

In re-direct Clement acknowledged that although the CSEC is not allowed to direct its surveillance at Canadians in Canada, when an individual's communications come to the surface through searches directed elsewhere that will result in analysts reading their communications content. Thus the limitation in its mandate does not preclude the ability to intercept much larger quantities of information beyond that which it was initially directed towards. He noted as well that there have been statements by public officials in the US that much of the collection of data by the NSA was not the result of direct surveillance.

With respect to the Google report for access by surveillance agencies as of 2018, Clement noted that the report for July 2017 to Dec. 2017 showed that only 500 to 599 requests for access resulted in up to 65,499 user accounts being accessed pursuant to those requests. This showed that a single request can result in the targeting of a large number of accounts.

With respect to questions on the necessary and proportionate principles for an international human rights law approach, Clements testified that the primary intention of the principles was to provide a framework for how security agencies would be regulated under international law. It was not to enable individuals to make decisions about their own data and how they would communicate. He said the latter would only be a very small part of what the principles were intended to achieve.

With respect to encryption of emails by Google, Clement said that this does increase the standard for email providers but he was pretty sure that Microsoft was doing this as well. He said that in the period since the Snowden revelations there has been a big move toward TLS to ensure better privacy protection.

Prof Clement noted during cross that he relied on the legal opinions of Prof. Lisa Austin for the legal aspects of his expert report on the risks of using an email provider with servers in the US. He noted that the argument of Prof Austin that he relied on in his report was later published in a peer reviewed law journal article. Prof Clement also noted that when he and his co-authors published Seeing Through the Cloud, they invited contributions from others who were interested in the topics covered in that report, as for example from the U of Toronto's IT officer. They also solicited responses from a

number of recognized experts on their website. He said those were put up on their website. One of those responses was from Konrad Von Finkelstein. He was the former Chair of the Federal Competition Bureau and the Chair of the CRTC. Von Finkelstein made glowing remarks about their report and endorsed their claims about the similar risk argument before criticizing other parts of their arguments.

Following the completion of the evidence on Prof. Clement's expert report (exh 26), the association filed a motion to have a supplementary report by Prof. Clements on the adequacy and thoroughness of the processes used by the employer to assess potential impacts on the privacy interests of users prior to moving to Gmail for the faculty at Laurentian. The employer objected to the introduction of such a supplementary report on the grounds of the lack of an evidential foundation for such an opinion by Dr Clement, and the fact its contents appeared to cover similar ground to evidence given by Dr Clement in his initial report and his direct testimony. After some submissions and discussion the motion to introduce a supplementary expert report was withdrawn and a new exhibit (33) containing all documents that the employer considered prior to its decision to move the faculty email system to Gmail was introduced into evidence on consent.

Argument

Union

The association began by asserting that although the details of the case can be seen as complicated, for example the technical details of how email works and is

transmitted and stored, this case is really quite simple. We all accept that the use of email poses both privacy and security risks. That is because anyone you send an email to can then send it on to someone else. As well we all know that email can be hacked by state and private actors. It submitted that the employer position was that email is inherently unsafe and poses privacy risks in any event so everything goes. But the association maintains that the evidence is clear that measures can be taken to make the use of email safer and more private. And one of the ways to make privacy and security stronger is by storing the data within Canada using Canadian based servers.

The association acknowledges that even when this is done it is not immune from privacy violations. But it argues that is not a reason to do whatever you want or to fail to consider which email provider is to be used for better protection of privacy interests. It submits that the employer has an obligation to take steps to manage and mitigate the risk to privacy that exists in email and that can be done by storing data on site or by using only service providers who store the data in Canada. It made an analogy to the situation of the physical university campus and the fact that it can become a less safe place to be after dark with respect to increased risks of an assault due to darkness. But the university can still take steps to try to minimize those risks, such as putting up streetlights. The union asserted that in the case of its email decision the university has failed to put up the streetlights. It submitted that it failed to even consider using a Canadian based service provider and said that by failing to do so it had increased the privacy risks of using university email. It contended that there are options to try to limit those risks, such as Microsoft that has located servers in Canada. It noted that other universities such as the

University of Toronto have opted for that service provider. The association argues that by failing to move to that type of service provider it has failed to take adequate steps to give consideration to the protection for the privacy rights of LUFA members in article 3.10.6.

Article 3.10.6 is as follows:

> The Parties agree that Members have a right to privacy, consistent with the traditions of Academic Freedom and the provisions of this Article.

Thus the collective agreement ties the privacy right to another right of fundamental importance in a university environment: academic freedom. The collective agreement provides a robust right to academic freedom in article 3.10.1 and 3.10.2:

3.10.1

In addition to their legal rights as citizens, Members have the right to academic freedom. Academic freedom is the right to search for truth, knowledge and understanding and to express freely what one believes. The University as an institution and the community of its scholars have a duty to protect and defend the search for knowledge and truth by all that inquire, teach, offer professional library service and learn under its auspices. They shall be free to carry out research and to publish its results, free to teach, to discuss and to criticize both the University and the wider society it serves.

3.10.2

Academic freedom includes the right, without restriction by prescribed doctrine, to freedom in teaching, freedom in research and scholarship including the right to disseminate and publish the results thereof; freedom to produce and perform creative works; freedom to acquire, preserve, and provide access to document material in all formats; freedom to participate in professional and representative academic bodies; freedom to engage in service to the institution and the community; and freedom to express one's opinion about the University, its administration, and the system in which one works.

Academic freedom does not confer legal immunity. It requires the acknowledgment of the work of others and the acceptance of responsibility for one's own beliefs and utterances.

The union noted that these clauses do not qualify the right to privacy by saying it refers to a right that is deemed to be more affordable or at the reasonable discretion of the employer. It submitted that because it is protected as an element or component within the context of academic freedom one cannot read into that right some kind of discretionary control or limitation for the employer. Rather it contends that the employer has an obligation to take all appropriate steps to protect the privacy of the members of the bargaining unit.

The association contended that the central point of this case is that despite the risks to privacy that are inherent in the use of email, it can be made less risky by taking appropriate measures. It argued that the fact that risk is inherent does not mean that the employer should not take reasonable steps to limit the risks.

The union acknowledged that Dr Clement had a rigorous cross examination and it was interesting to learn from it, but there was a danger in getting caught up in the complex detail of trying to figure out the precise nature of the risk to non-U.S. persons in having data stored on U.S. based servers, and the rights of non-US nationals with data on those servers. It contended that such precise details are not relevant because at the end of the day the evidence of Dr Clement supported the fundamental point that regardless of how much protection the US regulation offers to Canadians who have data on US servers and the precise limits of that protection, it is less than the protection offered to Canadian academics when the data is stored in Canada. It also argued that non-US nationals do not have the constitutional protections that US nationals have in the US. And they do not

have the protection that Canadian nationals have in Canada under the Canadian constitution. It contended that for the US government or any government to legitimately access the data of a Canadian academic stored in servers in Canada there is one legal process under Canadian law that has to be followed and they are subject to Canadian rights under the Charter with respect to unreasonable search and seizure. They do not have that protection if data is stored in the US. It argued that it is the limits on legitimate access that are important because there is little that can be done with respect to illegal access by state or non-state actors other than to try to build security measures into the system.

The association submitted that it may well be that Dr Clement was concerned about the fact that Canadian security agencies may break the rules and access Canadian's internet data illegally and urged adoption of stronger protection rights to guard against that. He is an advocate for setting up a system that gives the strongest and most appropriate privacy protections to prevent illegal access. But that does not mean that protections for Canadian's data being stored in Canada are not greater than if that data is stored in the US.

The union also argued that when one steps away from the details it does not matter what are the precise terms on which the US government can and does access information on US servers. What matters is that Canadians have less protection if their data is stored on servers in the US than if it is stored in Canada. It contended that Prof Clement's evidence on that was not shaken.

The union noted that Dr Clement's expert report addressed both procedural and substantive requirements to ensure appropriate protection of privacy in selecting an email system. On the procedural point it referred me to his responses to Question 1 concerning 'best practices' and his evidence on the importance of carrying out a proper Threat Risk Assessment (TRA) and Privacy Impact Assessment (PIA) and the reasons why they are important. It also referred to his comments on the importance of stakeholder consultations. It asked me accept Clement's view that while email has inherent security risks such that no absolute security guarantees can be given there are numerous ways to significantly reduce privacy risks and under FIPPA the university bears a clear responsibility to adopt best practices to assess and reduce such risks. That includes the need to ensure that email communications are not unnecessarily exposed to foreign jurisdictions and associated security agencies. It also urged me to accept that while employees generally lose some privacy rights when they use an employer's email service, faculty members are not viewed as normal employees because universities are unique in their adherence to academic freedom to ensure that faculty members can engage in independent critical thought and expression without fear of sanction. Clement offered the view that the protection of private communication from unwanted access by those in powerful positions who may take exception to the faculty member's views or research is an essential aspect of academic freedom.

Further the association asked me to accept Dr Clement's view that once the data of faculty members leaves the country it loses the constitution protection for privacy that it enjoys if kept in Canada and stored on servers located in Canada by providers such as

Microsoft. It also pointed to his view that the Canadian data, when stored in the US does not enjoy the protection granted to the data of U.S. persons. It also asked that I take note of the fact that 14 universities in Canada had provided their faculty with email services provided by Microsoft that now has servers located in Canada. Finally, it asked me to note Dr Clement's reasons for finding that Microsoft's email services for Canadian universities were more privacy protective than Gmail.

Dr Clement stated that his expert report was based very heavily on the report he did with several other scholars entitled "Seeing Through the Cloud" (exh 27) and in particular the legal opinion of Prof. Lisa Austin from the Faculty of Law at the University of Toronto. On page one of that report the authors found that they could not reconcile the Snowden revelations in 2013, showing the sweeping extent of US domestic surveillance activities targeting non-US persons, with the claim that data faced a similar risk from such surveillance regardless of where in the world it was stored or processed. It went on to conclude that, based on the authors' research, for sensitive digital data national jurisdiction matters, and 'where in the world your data is located affects which third parties can legally access it and on what terms.' (at p 2). The authors concluded, "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." (at p. 2). It contended that Dr Clement was not shaken on that during his cross-examination.

For its arguments on why there is less protection for Canadians whose data is stored in the US or other countries, the association pointed to the paper entitled "Why

Jurisdiction Still Matters" by Prof Austin et al (exh 28) and the following findings at p. 3 & 4 of that paper:

> -US authorities can access Canadian persons communications that are within US jurisdiction on statutory standards that are lower than those that apply within Canada and would be unconstitutional if applied within Canada.
> - US constitutional law does not apply when US authorities access Canadian persons communications data within US jurisdiction has long as the Canadian person remains outside the US;
>
> - Even if US constitutional law did apply, Canadian constitutional law offers more privacy protection to communications data;
>
> -Although Canadian authorities may share information with US authorities in some circumstances, both the collection of this information and its sharing is subject to Canadian law and Canadian constitutional standards.
>
> -Mutual Legal Assistance Treaties ensure that the constitutional norms of the assisting countries are applied. Therefore US authorities obtaining Canadian personal information through the MLAT process are subject to stricter norms than US authorities obtaining Canadian personal information within US jurisdiction.

Thus the union accepts there will always be other types of risks and limits to privacy for communications sent by emails, such as the risk of hackers or that data will be sent on to others etc, but there is still a greater risk if the data is used and stored inside the US. The risk that a Canadian agency may act improperly does not provide a reason to not act to reduce other risks. As well it argues that the fact there may be some protection for foreign nationals with data stored in the US does not mean there are not greater protections when such data is stored in Canada and is not a reason for failing to take measures to maximize privacy protection for email.

The association submits that the collective agreement places an obligation on the employer to maximize privacy protection, especially when there are cost effective options

available. Thus it argues the employer failed by moving to Gmail because it does not offer the best privacy protection and increases the risk to members' privacy in their use of email.

The union also agues that the employer used a flawed process in failing to properly assess or consider the risks to privacy of Gmail. It asserts that it also failed to do a proper TRA and PIA. On that point it referred me to the documents found in exhibit 33, the documents the employer states that it considered with respect to its decision to move to Gmail. It noted these included the PIAs done by the University of Alberta, Ryerson and Memorial (exh 33, tabs 4, 5 & 6). It submits that the closest thing that this employer has to a PIA are the slide presentations found at tabs 1 & 2 of exhibit 33. Tab 1 is entitled "Gmail Migration Proposal" and tab 2 is entitled "Cloud Email" and appears to be a progression on tab 1. However these slide presentations are radically different than what the other universities did as PIAs. The PIAs done by the other universities show a thorough consideration of privacy risks (see for example the Ryerson PIA, tab 4 of exh 33, at p. 15-16 where the risks of storage by Gmail in the US is addressed directly). That PIA also showed extensive consultation with all stakeholders, whereas in this case there was only discussion with LUFA. In addition, the Ryerson PIA showed they sought legal and subject matter expert advice on the impact of lawful-access treaties and warrantless searches or access. At the end of the day that university decided the risks were similar and decided to go with Google. But the PIA document at least showed that it went through a robust process, whereas the evidence we have in this case does not show a careful or thorough process.

The association also pointed to the PIA done by Memorial University in Newfoundland prior to adopting Gmail as another example of a thorough and robust PIA being done by a university prior to adoption of a new email system. On page 3 and 4 of that document (exh 33, tab 6), it refers to representatives of the university's Information Access and Privacy Protection Office meeting with the Office of the Information and Privacy Commissioner (OIPC) to present an overview of the project and committing to provide the OIPC with the completed PIA and invite feedback from that office. That PIA also identified and discussed the privacy risks involved in going with Google, with storage of data in the US as "significant, with little possibility of mitigation." At the end of the report the authors provided a summary of risks and mitigation measures to be undertaken in negotiating the contract with Google and also identified the need to educate users on security and privacy issues, communicate extensively with stakeholders during the move, and avoid a one size fits all contract with Google. It contrasts that approach with the lack of any PIA done by the employer here and it telling LUFA that it could not negotiate terms with Google. The union submitted that these two examples of a robust PIA demonstrate the type of best practices that are available and being used by other universities. It also referred to the process Dr Clement described as being used at the University of Toronto. Further, it noted that these documents show that this employer was aware of these processes but chose not to follow anything like that here.

With respect to measures taken by the employer, the union referred to its slide presentation on Cloud email (exh 33, tab 2). It noted that on a slide titled Privacy of Cloud Email, it states that the storage of emails is privy to acts of foreign entitites and

also sates that they have “the same right of access in Canada like US”. It also refers to Bill C-51 (Security of Canada Information Sharing Act) as being similar to the US Patriot Act. The union argued that these statements were simply wrong and notes that this failed to make reference to the privacy protections in the Canadian Charter available to faculty members if the data remains in Canada. The slide presentation also made no reference to the employer seeking expert advice or going to the Privacy Commissioner for input. The association also pointed to the slide on page 33 which showed some comparison of conditions between Microsoft Office 365 and Gmail with regard to mailbox size and costs. It also pointed to page 36, entitled ‘what we lose?’ That slide fails to refer to the enhanced legal protections for privacy that one gets by having email stored on Canadian servers and not subject to US surveillance measures. The union also noted that the slide on page 40 (that provided a summary of the presentation) failed to note the risk of access by the state including, US government access if storage is taken to the US. The union noted that the slide presentation failed to provide evidence of any kind of thorough and robust analysis by this employer of impact on privacy concerns, in sharp contrast to what was done by Memorial, Alberta, Ryerson and University of Toronto. All that was introduced by the employer was this slide show and the evidence of some consultation with LUFA

The union asked me to note that the employer did not call any evidence and it cannot ask me to presume such evidence exists when it chose not to call it. It submitted that the employer might ask me to find that there have to be reasonable limits with respect to what can be done to protect privacy, but it asserts that the obligation of the

employer under the collective agreement is to take all appropriate measures. It argues that to the extent they want to rely on reasonableness there is no evidence that the employer followed any process to ensure it would arrive at a reasonable result.

With respect to the employer's consultation with LUFA, the employer provided it with a copy of a Google contract it was considering and then later said that was the wrong one. Ultimately the union had the Google contract reviewed by the CAUT and it provided them with advice on problems it presented for the protection of members' interests. LUFA forwarded those concerns to the employer in October of 2015 and it received the employer's response on March 31/16 (exh 6). That response indicated that LUFA commented on the wrong contract and gave responses with respect to the updated contract. In the fall of 2016, the employer told LUFA it was seriously considering moving to Google for email for faculty. There was an email exchange and a meeting in November dealing with that communication and Ms St Pierre met with an employer representative who told her that cost was a big factor as there would be a $50,000 cost for moving to Microsoft.

The union also submits that the fact it was complaining that Groupwise was a problematic system that needed to be improved, does not allow the employer to say we do not care about protecting faculty members' privacy rights. Nor can the employer point to the fact that LUFA did not object to the move to Google Drive because that was not a mandatory application and faculty could choose not to use it. Gmail is a mandatory system for faculty to use for conducting university business and communicating with

students. Then in June of 2017 the employer announced that the faculty would now have to use Gmail

The union also points to the fact that there was an easily available option for the employer, to move to Microsoft for email services. It acknowledged that this option still entailed some privacy risks but those risks would be less serious than those with Gmail. The employer did not choose that option and did not do a robust assessment of risks to privacy entailed by either option. It submits that the consultation with LUFA was not a real consultation in that it ultimately told LUFA they had no choice. The union argues that it has both privacy and academic freedom rights under the collective agreement that have been violated by the move to Gmail.

The Union presented the following judicial and arbitral authorities in support of its argument: *McKinney v. University of Guelph*, [1990] 3 SCR *229; AUPE v University of Calgary*, 2008 CarswellAlta 678, [2008] Alta. LRBR 129; *University of Ottawa and APUO (Rancourt*), 2014 CarswellOnt 19219 (Foisy); *LUFA and Laurentian University (Selection of President) Gr)* (unpublished reasons of Arb Burkett, July 2017); *Lakehead University and LUFA*, 2009 CarswellOnt 7262, 184 LAC (4th) 338 (Carrier); and *NSG&GEU and Dalhousie University* (unpublished reasons of Arb. Outhouse, Aug. 26/15).

It relied on *McKinney, supra*, primarily for its strong statements of the meaning of academic freedom and its central importance to the mission of universities and their role as independent institutions in modern democratic society. The SCC identified the preservation of academic freedom as an objective of pressing and substantial importance

in our society in its analysis under section 1 of the Charter. The association relied on the *University of Calgary, supra*, for the point that universities are unique as places of employment because of their status as private, autonomous and self-governing institutions that receive public funding, but must always maintain their commitment to academic freedom and freedom of expression and thought so that they remain free to criticize government and other institutions in our society. The Alberta Labour Board identified the concepts of tenure and academic freedom as critical to the university's ability to carry out its role of maintaining a free marketplace of ideas where free expression and enquiry can take place unconstrained by state power. (at para 13 to 17). The union noted that in this case it is very important that the parties have agreed to recognize the protection of privacy as a right that is central to academic freedom.

The association relied on *Laurentian, supra,* for its recognition of the importance of consultation in the university collective agreement setting, given that such agreements reflect a unique set of priorities, including collegial governance and academic freedom. Although that case dealt with a violation of article 2.25.1, which provided an express reference to the desirability of consultation in the selection of senior academic administrators, the association relied on it for its recognition of the value of consultation and the importance of the observance of procedural rights. In this case the union says the failure of the employer to move to an email service with storage on Canadian servers is a violation of article 3.10.6. The move to Gmail fails to protect the privacy rights of LUFA members in a manner that is consistent with academic freedom. It argues that the fact there was a cost saving by moving to Google does not justify the overriding of

collective agreement rights. The agreement does not say to protect privacy rights as long as it can be done in a cost effective manner. Further, article 3.10.6 is not an article that gives a discretion to the employer with respect to what is reasonable or practical. Thus it requires the employer to get it right when it takes action affecting privacy rights and it failed to do so.

The association acknowledged that there are two existing arbitral decisions that dismiss grievances by faculty associations alleging a breach of collective agreement rights when the employer decided to move its email system for faculty to providers that are US based and may store data on servers based in the US. However it submitted that both decisions are quite distinguishable from the circumstances confronted in this case.

The first such decision was that of Arbitrator Carrier in *Lakehead University, supra.* In that case the union grieved against the move to Gmail for faculty email and alleged a violation of the academic freedom article, and a provision in the Rights and Responsibilities article (16.01.03) that recognized the members right to privacy in "their personal and professional communications and files, whether on paper or in electronic form". The association argues that the language at issue in that case was not as strong in its protection of privacy and academic freedom because it did not tie privacy rights into the right to academic freedom. It also argued a distinction on the basis that the employer argued the collective agreement at Lakehead did not obligate the employer to provide an email service for faculty, whereas there is no such issue in this case. Further the association notes that although the union in *Lakehead* called an expert witness to testify as to the risks of US state surveillance where email was stored in the US, the expertise of

that witness was focused on the risks to privacy of US anti-terrorism legislation and surveillance for U.S. residents as opposed to non-resident persons. A second expert, Prof Michael Geist also testified but his evidence focused on the risks of state surveillance and access by US agencies to email and data originating and residing inside Canada, either with or without the cooperation of Canadian surveillance agencies such as CSEC. Further, and perhaps most significantly, the arbitrator in *Lakehead* found that there was no clear and cogent evidence that any of the information or email originating within Lakehead University was reaching any of the servers situated within the U.S. He found that the best evidence he had was that email originating from Lakehead had, under Gmail, been routed to a Canadian server.

Further, the association in *Lakehead* argued that the rights and responsibilities article not only required the employer to provide an email service but also to ensure that all electronic communications would be private in all respects. That argument was found to be tantamount to an undertaking by the University to protect all faculty members from any form of intrusion or access either by the University itself or by any third party. The association herein submits that it recognizes that email has inherent privacy risks and it is not arguing for the employer having an obligation to ensure protection against any possible intervention. Rather LUFA is arguing for the recognition of a right to privacy that means you do not simply throw up your hands and say I cannot do anything to protect email communications, but rather the employer must take steps that are readily available to maximize the protection of privacy to the greatest extent possible. That includes the use of Canadian based servers because it decreases risks to privacy and thus

increases privacy rights. It noted that Arbitrator Carrier recognized this in his decision, that the provision protecting a right to privacy in electronic communications could not have been intended to provide absolute privacy and prevent all manner of intrusions as argued by the union in that case. Thus the union submits that both the facts and the union arguments are quite distinguishable from our case.

Finally, the union distinguished *Dalhousie University*, *supra* on the basis that the only issue before the arbitrator was whether the decision of the employer to move to Microsoft Office for email service with servers in the U.S. was a violation of provincial privacy legislation *(Personal Information International Disclosure Protection Act*). Thus the case turned on whether there was a violation of the Act and not a particular provision of the collective agreement. The main provisions at issue were subsections 5(1) and 5(2). The first subsection required a public body to ensure that all personal information in its custody or under its control (including a service provider's control) is stored only in Canada and accessed only in Canada, unless the head of the public body allows storage or access outside of Canada under ss. 5(2). This latter subsection allows the head of a public body to allow for storage or access to personal information outside of Canada if he/she "considers the storage or access to meet the necessary requirements of the public body's operation." The union noted that the statutory provision provided the head of a public body with built-in discretion to allow storage or access outside of Canada where it was reasonable to do so to meet the necessary requirements of the public body's operation. It also noted that in that case there was a lengthy and robust process of seeking service providers and doing a comprehensive privacy impact assessment and the

arbitrator found the President's decision to opt for Microsoft despite its US based servers to be reasonable when all factors, including cost savings and potential risks to privacy through state surveillance by US security agencies were considered.

In essence the association asserted that the *Dalhousie* decision was distinguishable because it did not deal with the limits of privacy protection under a collective agreement guarantee of protection for privacy as an important element of academic freedom. It actually only dealt with the interpretation and application of a specific section of privacy legislation prohibiting storage of, and allowing access to, personal information outside of Canada.

It concluded by pointing to the employer's failure to choose the option that was available to enhance privacy protection or to engage in an adequate process to assess the risks to privacy before the move to Gmail, resulting in a breach of article 3.10.6. It asked for a declaration of a violation of the collective agreement and an order that the employer implement a Canadian based email service under which data stays in Canada.

Employer

At the outset the employer noted that the association stated it was no longer asserting a breach of article 2.30 regarding existing practices. It noted that in a technical sense this is a case about whether a particular management right under article 3.20.1 prevails over the somewhat amorphous right to privacy and academic freedom under article 3.10 (and 3.10.6 in particular). It noted that the employer disputes what the privacy right under 3.10.6 means. Its primary position is that the right to privacy does

not apply to these circumstances given the management right under article 3.20.1. That provision includes the following statement:

> The Employer will determine by consideration of the financial resources of the University, the manner in which and the level at which facilities and services are provided to Members.

It takes the position that it has done nothing more than exercise its management rights in the manner contemplated by the parties under that provision of the agreement. The employer contends that this provision gives it the right to determine, taking into consideration financial resources and costs, the manner and level at which facilities and services are provided to members of faculty. It also refers to the wording that creates an obligation to maintain reasonable levels of various services, including technical services, and argues that it has provided reasonable levels of technical services in its move to Gmail. The employer notes that the association does not argue a breach of article 3.20.1. The employer position is that technical services given to members pursuant to management rights given to the University do not and cannot breach a member's privacy.

The employer notes that it did not exercise its management right until after a meeting of the Joint Consultative Committee and attempted settlement discussion that left it clear, by June of 2017, that the parties were in an intractable dispute about the planned move to Gmail.

In a non-technical sense the employer submits that this case is about principle, fear and misunderstanding. It points to the original grievance that includes a statement that LUFA has raised legitimate concerns about the risks to, and the impact this (the move to Gmail) will have on, the privacy rights of its members. Thus the grievance is

about a fear or a risk, not a certainty or any established breach of privacy. In argument the union used the term "danger" to describe the case based on the evidence and facts of the case.

The cross-examination of Dr Clement was an attempt to introduce evidence through the union's expert. LUFA asked me to disregard those facts because they are inconsistent with LUFA's fear and grievances. The employer submitted this was tantamount to asking me to ignore the facts and evidence. It submitted that this grievance has been brought by a local union without a full grasp of the issues, and an expert with a poor foundation for his views. It noted that Dr Clement stated that he defaults to suspicion in the absence of evidence.

The employer does not take the position that storage of data outside of Canada is not an issue to consider in making the decision on email service. However, it contends that the employer did consider it and recognized it as an ongoing concern with the change to cloud email. However, it said the issue is about whether that risk is greater or less than the old way of doing things with email. It argued this was a complex issue that must be addressed on the basis of facts and evidence, and not on the basis of fear. The employer asked me to note that it has never been accepted by an arbitrator or judge in Canada that the risk of moving to a cloud based system for email was unreasonable or unlawful. Further, it argued that LUFA has not proven it to be unreasonable in this case.

The employer noted that the union had made several arguments or attacks focusing on the process used by the employer, but argued that this is not really what the grievance was about. It noted that the fundamental issue raised by the union was that the

employer has contracted with Google, a US based provider with US based servers ensuring that storage for the system will be in the US. Thus the grievance is about the substance of the email system that has been adopted, not the process used to come to that decision. In that respect it noted that the union's request for remedy was for an order requiring the implementation of a Canadian based email system. Thus it submits that while the evidence about he consultation process may have some relevance, at best it is indirect evidence in terms of the substance of the privacy right and what is necessary for its protection. But the employer differs with the union about what the evidence on process demonstrates. The documents in exhibit 33 demonstrate what the employer looked at during the decision making process and show that it considered the very question that the association wanted it to consider regarding the risks to privacy presented by the move to Gmail and the risk of storage in the US. The employer submitted this was evident from the slide presentation on Cloud email (tab 2, exh. 33) and the documents it considered, including *Seeing Through the Cloud*, the report prepared by Dr Clement and his co-authors. It submitted that this met the concerns of the association with respect to the need for a PIA and TRA.

The employer submitted that the association appeared to be primarily concerned with the form of the employer's consideration or the risks presented by the move to Gmail and admitted its consideration of those risks did not appear in the form used by Ryerson and the University of Alberta. However, they looked at the same considerations. It argued that in essence this university, coming to the issue after the TRAs and PIAs had been done by several other Canadian universities, decided to look at

the risk assessments done by those other universities, and the arbitration decisions that had already looked at the same issues, and used those documents to help them consider the issues, assess the risk and make their decisions with that information. The employer took the position that there was nothing about the collection of documents it considered that shows robustness one way or the other. This employer did not do a detailed report like the other 3 universities whose reports were considered and included in exhibit 33, so it was not the PIA that Dr Clement contended was a "best practice". The employer submits that this failure was at best a failure to follow a best practice in the view of Prof Clement. But the employer submits that an employer can actually choose a reasonable system without following a "best practice" process, and the real issue in this arbitration is whether the email system adopted by the employer is in fact a violation of the collective agreement, even if it did not follow the best practice.

Further the employer took the position that the evidence of Ms St Pierre established the chronology of a long exhaustive dialogue between the association and the employer on the issue of how to replace its failing email system. It submitted this was the story of two parties talking past each other for much of the dialogue. However, the employer submitted that it was important to note that during the 3.5 years of the dialogue there were several meetings with discussion of contracts and the association taking the time to obtain legal advice from CAUT and providing the employer with written submissions on the union's concerns with the Google contract, including their privacy concerns. It noted as well that while this dialogue was going on there were numerous complaints by faculty members about the inadequacy of the existing Laurentian email

system, demonstrating the need for a new system. It noted as well that, as the dialogue over the new email system neared the end, the parties engaged in a formal mediation process but were unable to come to a consensus on what should be done.

The employer also pointed to the testimony of Ms St Pierre concerning LUFA's continued use of an email system provider (Go Daddy) that is based in the US with servers in the US. She also conceded that she did not have the technical expertise to understand the ins and outs of various email systems and relied heavily on the advice of CAUT. The employer suggested that much of her evidence on these points showed a lack of understanding of technicalities and a continued adherence to principle as opposed to practicality. It argued that the grievance arises from a principle focused misunderstanding rather than practical facts and evidence.

The employer submitted that the evidence of Dr Clement was similarly not able to prove the violation of the collective agreement asserted by the union. It summarized his key assertions of the impact of the move to Gmail as follows: there are inherent risks in use of email, but numerous ways to reduce risks and a university should take steps to ensure email communications are not unnecessarily exposed to foreign jurisdictions and security intelligence agencies; when Canadian data leaves Canada it loses Canadian legal and Charter protections and in the US does not enjoy the protections granted to US persons and becomes subject to the NSA; privacy interests of Canadian faculty members are enhanced by email services provided by a Canadian hosted provider "presuming other security and privacy protections/risks remain comparable"; and Microsoft email may be

more privacy protective than Gmail because it established two data storage centres in Canada.

The employer described the following opinions of Dr Clement as irrelevant: his opinion about best practices for an organization moving to a new email provider and whether the employer adhered to those best practices with respect to a TRA and a PIA (Q1); his opinion on the difference between privacy and security (Q. 2); and his answer to question 4 about the link between academic freedom and privacy protection, as not a matter that needs to be resolved base on expert evidence. On the answer to question 1, the employer contends this is a grievance about whether the substance of an employer decision violates a substantive right to privacy, and there is no longer an allegation of a breach of a procedural provision and the employer can arrive at an acceptable substantive decision despite a failure to follow best practices.

In addition the employer submits that the relevant risk opinions of Dr Clement should be given little weight due to his limited range of expertise, the limited foundation for his opinion and his admitted perspective as a self avowed privacy advocate. On the matter of limited expertise it argues that his opinion about legal and constitutional protections is beyond his expertise and he admitted that he had no legal training but deferred to the opinion of Prof. Lisa Austin to support his opinion on those matters. Further when Clement was taken through the US legislation that empowers and limits the NSA he admitted he was not familiar with that legislation and did not review it for the preparation of his report. The same was true for Presidential Policy Directive 28 issued in 2014 to place limits on the NSA surveillance of non-US persons.

Further the employer contended that Prof Clement's opinion about the risk of access by the NSA is weak as well as it was based on the Snowden disclosures of documents, but he had not read all of the documents disclosed by Snowden and he admitted that they were the subject of some debate and he had no special knowledge of the NSA or national security given his experience as a computer science professor and lack of experience in the field of national security. In addition, Prof Clement admitted that he had not read the July 2014 report of the PCLOB concerning its oversight mandate and controls over NSA surveillance activities. In addition the employer noted that the association had argued that the US did not have a legal framework that governed access to digital information by US agencies for non-US persons. It pointed out that this was incorrect, noting that there are greater checks and balances and oversight mechanisms in the US than there are for CSE activities in Canada, a fact admitted by Prof Clement. Thus the employer contended that both Dr Clement and the Association appeared to lack awareness and knowledge of legal regulation of such activity in both the US and Canada. It thus contended that Dr Clements lacked a proper foundation on which to base his opinions of the relative risks for privacy for email systems based in Canada and the US.

In addition, the employer noted that Dr Clement had described himself as a privacy advocate and said in relation to his views on Canadian and American security agencies that he was suspicious unless he had good evidence to the contrary. The employer described this admission of bias as very problematic given the witness's admission that he had no knowledge of foundational documents about the regulation of NSA surveillance.

The employer also criticized Prof Clement's opinions as being very qualified because he failed to speak at all to the actual relative risks of Gmail as compared to a local email system and simply presumed all other security and privacy threats to remain comparable. It submitted that this was the ultimate answer to the risks discussed in *Seeing Through the Cloud*. That report focussed on the one truth that the Canadian Charter does not apply to the US government and took the position that other relative risks do not matter. That is a very principled position and academic and artificial because in reality one cannot ignore the reality of the many other relevant and practical risks to privacy

So for example, Dr Clement assumed the risk of hacking to be comparable but he admitted he had no actual knowledge of the Laurentian email systems, old or new and their vulnerability to hacking. But he admitted that a lost laptop with unencrypted email messages located on it were a security problem for the old system. He also admitted that one way to protect against that risk was to have a system where emails are not stored on laptops. He also admitted that he had not studied the proportion of Laurentian emails sent from or to someone in the US. Further Clement assumed the risk of insider unauthorized access to emails to be equal in both the old and new Laurentian system, although he acknowledged there is a hypotheses that the risk of unauthorized insider access is greater when data is hosted in a community in which both users and IT administrators live and work.

Further the employer pointed to the fact that Dr Clement's own studies established that there is a significant risk of NSA surveillance associated with email that

is hosted within Canada. His own research findings on the routing of internet traffic done in 2016 showed that 28% of Canadian Internet traffic "boomeranged" through the US and 81% of transmissions between Canada and third countries transited through the US at some point. In his paper "Addressing Mass State Surveillance Through Transparency … " (Exh 30, tab 1, p. 5), Dr Clement argued that surveillance of communications in transit (by Upstream) was arguably a greater privacy problem than surveillance of stored data (via PRISM). In cross examination he explained that by "wider reach" he meant it could capture all internet traffic going to all servers and tech companies and also has access to lots of other Internet transactions that do not involve those nine large tech companies. When asked if this meant Upstream was worse than PRISM for privacy impact he answered "In one way yes in one way no". He admitted that it captures a wider spectrum of communications so is worse that way but not as bad in that it was harder from an analytical point of view to figure out what was going on with what was intercepted because data packets had to be reassembled. When asked if there was a greater risk from Upstream for some and generally equal risk otherwise he replied, people likely to be at risk are those likely to draw the ire of agencies, and if talking about academics, they were academics who do have human rights concerns and based on topics they are concerned with or topics they study or keywords they use. He seemed to suggest that Upstream was more risky for academics.

Dr Clement admitted that he did not look at any data about Laurentian email traffic routing that might suggest the risk associated with traffic routing would not persist if the employer were to continue to host email in Canada. Further he agreed that because

Gmail was encrypted, to the extent that LUFA members were sending email to other Gmail users (of which there are approximately 1.2 billion) those emails would be encrypted at both ends and relatively protected from Upstream collection while in transit as compared to an email system that lacked encryption.

The employer argued that Prof Clement gave evidence that undermined the argument found in Seeing Through the Cloud, that the loss of Charter protection caused by storage of emails in the US justified keeping the email stored in Canada. It noted that he testified that a Canadian researcher communicating with a terrorist located abroad may be a legitimate target for the CSE (Canadian signals intelligence agency). The Charter might protect that researcher from the CSE, but Prof Clement admitted that he had tweeted that CSE spying is secretive, expensive and out of control. Further he said he believed the video that he tweeted at that time that alleged that the CSE was engaged in illegal spying and agreed that the US had better surveillance oversight mechanisms than Canada (in a formal sense at least). Dr Clement also agreed with Prof Forcese's statement that CSE's metadata surveillance program may breach the Charter and ultimately agreed that access to private communications by the CSE is a "practical risk" to privacy.

However, when asked about Prof Austin saying it would be wrong to make a decision on the basis of practical risk, Dr Clement stated that "you have to consider the various elements of risk, one of which is that the CSE is acting illegally, the other that it has the means and capability of accessing metadata. But to say that Canadian agencies are acting illegally … that would then mean that there's no particular relevance to

keeping it in Canada and avoiding US surveillance. There can be an additive risk." The employer submits this shows that Dr Clement admitted to alleging illegality by CSE, yet in his statement in evidence he said that he cannot now accept his own prior assertion in this context because it would undermine the case for keeping email in Canada.

The employer contended that Prof Clement also attempted to downplay the risk of CSE unlawful access and the overall risk of surveillance in Canada. He appeared to agree with the suggestion that a Canadian researcher on a local premises email system, communicating with people who may be foreign targets, really ought to take steps to protect communications from CSE. Although he referred to it as an 'extreme example', he said there are additional steps one should take if researching on people who might be potential targets. But he also agreed that using other means, apart from employer email, is less convenient than using the workplace email.

The employer makes two primary legal arguments to support its contention there has been no violation of the collective agreement. First, it submits that the collective agreement obligations (art. 3.10.6) pertaining to privacy and academic freedom (art 3.10.1) do not apply, because the provision of email services for faculty is covered by the language of art. 3.20.1, and the association has not alleged any violation of that provision. Article 3.20.1 states as follows:

> The Employer acknowledges its responsibility to provide and maintain facilities, *services* and general working conditions, which support the *effective discharge* by full-time members of their responsibilities as specified in Article 5.15- Rights, Responsibilities and Duties of Academics. The Employer will determine by consideration of the financial resources of the University, the manner in which and the level at which facilities and services are provided to Members. Additionally, the Employer will provide, in a fair and equitable manner, at least a

> securable individual office for each full-time member and securable group offices exclusively for Session Members, ergonomically appropriate office furniture, appropriate lighting and ventilation, and will maintain reasonable levels of working space, secretarial and *other support* services, including telephones, *computing,* printing, duplicating, library services, *technical services,* Department/School resources, teaching and research assistance and laboratory space if required. (*emphasis* added by employer)

The employer contended that the rights of privacy and academic freedom under the agreement do not prevent the employer from selecting and implementing an email system that meets the 'reasonable level' of support services and computing or technical services required under art. 3.20.1. It submitted that this position is supported by the decision of Arbitrator Carrier in *Lakehead University, supra*. In that respect it also referred to the testimony of Ms St Pierre indicating that the move to Gmail did appear to solve the problem of poor email service under the former employer email system. It also noted that LUFA did not claim that it failed to provide a reasonable level of email service under article 3.20.1.

In further support of this argument the employer note that article 3.20.1 is a very specific grant of management authority and discretion to the employer as compared to a claim to a vey general right by the union. It argued that privacy and academic freedom are important rights but they have very little to do with what is actually at issue in this case. It argued that one does not actually breach privacy by implementing a new email system. It may raise privacy and security implications but it does not constitute an actual breach of privacy. It acknowledged that choices about privacy and security are integral to choosing an email system. However, it noted that the parties have agreed in art. 3.20.1 to give the employer a license to chose the "manner" by which email service is delivered,

a license to make choices about security and privacy/cost trade-offs that are inherent to the selection of technical services. It submitted that it was not feasible to give a license to choose the manner by which one delivers email services and a license to make judgements based on the employer's financial resources, without also giving license to make choices about the level of security protection to be purchased. It submits as well the specific grant of license with respect to technical and computing services prevails over the more general commitments made with respect to privacy and academic freedom. Further the employer argued that issues of academic freedom and privacy are not engaged by the provision of services that support the 'effective discharge' of faculty member duties.

In support of this argument the employer noted that it is supported by the findings of Arbitrator Carrier in *Lakehead University, supra*, (at para. 25). There he found that although the collective agreement provided an express right to "privacy in their personal and professional communications and files, whether on paper or in electronic form" to members, that right did not govern management's decision to outsource email to a US based provider. The arbitrator found that the guarantee to privacy could not be read as an undertaking by the University to protect all faculty members from any form of intrusion or access either by the university or by any third party. He doubted that such a comprehensive privacy in email was even technologically achievable or practical. He held that it was not an undertaking to protect a member's privacy in email from all manner of intrusion by third parties, but rather an acknowledgement that those rights to privacy exist and an undertaking that the university itself would not subvert or undermine

those rights. The employer argued that given that the Lakehead agreement lacked the employer supportive language of article 3.20.1 granting a license to the employer to choose the manner of delivery of email service, I should make the same finding about the relationship between the management right and the privacy right as was held in *Lakehead University.*

In the alternative the employer argues that if I find the right to privacy does apply despite the application of art. 3.20.1, I should find that is a right to reasonable security for university email and find that he association has not proven any breach of that right. It notes that a burden of justification can arise on a privacy grievance but only when management actions intrude upon an expectation of privacy, as for example with implementation of video surveillance, which then gives rise to a balancing of interests test to justify the intrusion. However there is no balancing of interests or justification required where the employer's actions are neutral and also legitimized or authorized under art. 3.20.1.

It argues that the union cannot prove any such intrusion, noting that there has never been any recognition in Canadian law, arbitral or otherwise, that the transfer of personal information to a foreign jurisdiction is by itself a breach of privacy. The employer notes this is the case despite the enactment of "blocking statutes" in BC ad Nova Scotia designed to block storage of private data outside of Canada. It notes that even those statutes have limits to allow such storage to deal with institutional realities and other factors. Further it noted that when individuals have challenged foreign transfers of personal information, Canadian privacy commissioners have held that such transfers are

not prohibited and the only issue is whether the personal information remains protected by "reasonable security measures". Thus in dismissing a complaint that challenged the outsourcing of a Ministry of Natural Resources database to an American provider, the Information and Privacy Commissioner of Ontario held that the privacy legislation did not prohibit provincial institutions from outsourcing services to a foreign provider on the basis that foreign law, including the US Patriot Act, may apply. The Commissioner noted that personal information may become subject to disclosure to law enforcement authorities, whether stored in the province or elsewhere. Thus the critical question for the institution is whether they have taken reasonable steps to protect the privacy and security of the records in their custody and control. (*Reviewing the Licensing Automation System of the Ministry of Natural Resources: A Special Investigation Report*, Information and Privacy Commissioner, Ontario (27 June 2012), at p. 5).

The employer submitted that the association argued here that the privacy right placed an obligation on the employer to take any readily available steps to minimize risks to privacy or make email safer. It argued that such a standard cannot apply because that would involve a standardless right and a boundless obligation to continue to take any available steps that would make protection better. It said the duty imposed cannot require the employer to always be doing better. It argued that as noted above the accepted legal standard is that of reasonableness or reasonable security measures, not an obligation to always take any measures available to make it better.

In addition the employer noted that the reasonable security measures standard is assessed based on all the circumstances, such as the sensitivity of the personal

information, the foreseeability of a privacy breach and resulting harm, the relevance of generally accepted or common practices in a particular sector or kind of activity, the medium and format of the record containing personal information, the prospect of criminal activity and the cost of security measures (*Twentieth Century Fox Film Corporation*, 2006 CanLII 37938 (BC IPC), at par. 80).

The employer also noted that one of the reasons challenges to foreign transfers of data have failed is that they only focus on the single risk of foreign security surveillance instead of looking at all the circumstances. There is also a reluctance to treat access by foreign governments pursuant to a foreign law as a security factor at all (given principles of comity). This has caused some privacy tribunals to draw an equivalence between Canadian and US law enforcement and intelligence regimes in terms of potential access to personal information. Thus in *Twentieth Century Fox Film, supra,* the BC Privacy Commissioner held that the geographic location of personal information which may change throughout the life cycle of a transaction is not determinative of threats to the security of the personal information. Thus while personal information located outside BC is subject to the laws that apply where it is found, the risk of such information being disclosed to government agencies is not a risk unique to US organizations. It also found that the risk presented by national security or law enforcement agencies is not necessarily greater outside of BC (at para 85 & 86). Similar views were expressed by the Ontario Privacy Commissioner in *Ministry of Natural Resources*, supra (at page 5).

The employer contended that the case law demonstrates that moving data outside of Canada is not per se unreasonable because of the potential for access by a foreign state

surveillance agency. The case appears to generally accept that access to data by foreign governments is but one of many risks to be considered in the assessment of such a move, but the employer notes that potential access by a foreign government by formal law is accepted, as demonstrated by the cases cited above.

The employer also pointed out that arbitrators have generally recognized that email is just a tool and is very difficult to make secure or completely private. It contends that this weighs heavily in favour of a very low security standard, because email is generally regarded as not being an appropriate means of sending or receiving any information that needs to be kept secure. It argued that portions of the evidence of both Clement and St Pierre support that view, and the findings of Arbitrator Carrier (in *Lakehead University, supra* at para 26) and Arbitrator Outhouse (in *Dalhousie University, supra,* at pages 90-91) both recognize the same point. The latter decision makes the following comment:

> Finally, it must be observed that email communications are far from being completely secure, even when hosted within Canada. They are subject to various forms of interception, hacking, sharing, etc.. The comparison of emails to postcards, although perhaps somewhat of an exaggeration, is not inapt. Certainly, any person who entrusts personal information to email, particularly their work email, cannot do so with a high expectation of privacy.

Thus the union has to prove that the employer failed to provide a reasonably secure email system taking into account the circumstance that email is something that is inherently insecure because it is a global communication system. The employer submits that the union has not attempted to establish a standard of reasonable security but instead has attempted to prove that one particular risk, that of access by US security agencies

caused by the change in data residency, is so serious that outsourcing to a US based provider is not possible without breaching member privacy. It submits that LUFA has failed to prove that this risk is so extreme that it prevails over all other risks given the testimony of Clement and St Pierre. The employer also noted that there were too many other very real and serious risks to email security to simplistically presume that all other risks were equal as was done by Dr Clement and LUFA.

The employer submitted that the legal argument on which *Seeing Through the Cloud* is based is far too simplistic and principled in nature. It is based on one simple premise: that the Charter protects Canadians from Canadian government access but not from American government access for data located in the US. But the relevance of that truth for violation of privacy is undermined by the following factors: the Charter does not protect against loss, hacking by outsiders, insider unauthorized access (all problems recognized by Dr Clement; the Charter is not protection against access by the US government to communications that boomerang in transit or otherwise through the US, a factor focused on by Dr Clement in one of his papers; the Charter is not protection against illegal Canadian government access to data, another factor that Dr Clement alleged in very strong terms in the past; whatever effective protection does arise from the Charter is supplanted by mechanisms like PPD-28 that are rooted in the shared interests of sovereign nations.

The employer argued that the union failed to prove even an incremental risk to security and privacy by moving to Gmail let alone that the move to Gmail failed to meet a reasonable standard. Further it noted that even proof of a risk is not proof of an actual

interference with privacy or academic freedom. It noted that we did not hear any evidence from faculty members with respect to any actual breach of their privacy or academic freedom. It submitted that the evidence we heard on actual communications and risks was to the contrary. It noted that the union's fears with respect to the risk of using a US based email system did not change the union's manner of communication with respect its own email system. Further both union witnesses acknowledged the low expectation of security with respect to email and the need to take steps to protect oneself with respect to the communication of sensitive data.

Finally the employer submitted that this case is not about academic freedom, but rather is about a misguided desire for a convenient tool for communication that is purported to be more secure but will never actually be secure enough for confidential communications because email is not a secure method. It argued the real solution to any problem with respect to privacy of sensitive information is to cause all LUFA members to think about the risks of email and the need to use an appropriate communication tool when required by the sensitive nature of the information. It submitted that it was a perfectly acceptable outcome to this matter to cause the faculty members and administrators to use simple caution in communicating sensitive information.

Reply

The association said it was not asking me to disregard any evidence, but submitted that a lot of evidence was simply not relevant to the issue. For instance, it asserted that the precise protections offered for the privacy of non-US residents under US law was not important. It submitted that at the end of the day the differences in risk to

privacy presented by a US based email system comes down to the Charter protections for the right to privacy for Canadians and a remedy for any breach of that right, which are lost when the data is stored in the US.

With respect to the evidence of Dr Clement, that for the purposes of his report he assumed that all other privacy risks were equal, he indicated he was assuming that the employer would take the other security measures necessary to deal with the other risks in both systems and if that was done you were left with there being one additional risk added by going to the US for the storage of data. Further it contended that this not a case where the employer showed that they got some added protections in the US so that these would have to be balanced against the added risk of US storage. It argued that we were not given evidence that Google offered greater protections than Microsoft apart from Google encryption of Gmail. It submitted that the added risk presented by US storage is not answered by saying that because we have these other risks you do not have to worry about US storage.

The union also argued that it was not accurate to state that Clement only got his information from the commentary of others. He had looked at many of the Snowden slides and documents but not all of them. It submitted that the Snowden documents were important because they showed that what was going on in practice was far different than what was on paper with respect to US regulation and protection for privacy. It submitted that the Snowden revelations were very important to the concerns expressed by Dr Clement and others with respect to privacy risks.

It submitted that the evidence of Ms St Pierre was important to counter any suggestion that there was a comprehensive review or consideration of risks by the employer. It pointed to her evidence of the employer giving them the Google contract and then later, after they got expert advice on that contract, telling the association that it was the wrong contract, and then telling them it was not negotiable in any event. Further it submitted that evidence of Ms St Pierre about the email system used by LUFA was a red herring because its email with members was not a matter of academic freedom.

The association also submitted that Dr Clement's opinion was not qualified or limited due to his failure to address other risks of the old and new systems, noting that he was not asked to address other concerns. It noted that he did not qualify his opinion that there was an increased risk to privacy when email is located outside of Canada. Further it argued that Dr Clement's evidence on the relative dangers for privacy presented by Upstream and PRISM did not represent a backing away from his written report on the dangers of email storage in the US, despite his admission that Upstream is worse than PRISM in some respects but not in others. It noted that while Clement recognized that boomerang transmission of email through the US was a serious problem for Canadian based email, he also noted that if you have a system with US based servers you are ensuring that emails have to go through the US in transit. If it has Canadian based servers it may go through the US but it also may not. Further the union noted that although Dr Clement recognized some enhanced privacy value from the encryption of email, at the end of the day he remained of the opinion that there was greater risk presented by storage of data in the US.

The union also contended that the employer argument that Professors Clements and Austin were ignoring the problem of the Canadian security agencies acting illegally to access emails did not undermine the union argument. It submitted that even if Canadian surveillance agencies might act illegally to present a risk to privacy, that is not a reason to add to the risk by sending the data to the US for storage so that it becomes subject to two risks rather than one. Instead the employer should try to remove as much risk to privacy as possible. In short, any risk presented by Canadian government access to data does not get any better by taking the data to the US.

The union also asked me not to accept the employer argument that this case is just based on the risk of breach and there is not evidence of any actual breach. It submits that the union does not have to wait for an actual breach to say that the right to privacy has been breached by the employer's failure to take reasonable and available steps to minimize risks to privacy.

The association argued that the *Lakehead University* award should not be viewed as applicable to this case because the association in that case was making a different argument about the nature of the employer's obligation to protect privacy, an obligation that was impossible to meet according to the arbitrator in that case. However, it noted that Arbitrator Carrier did recognize an employer duty not to subvert or undermine the privacy of faculty in that case. It submits that the employer decision to use an email provider that stores data in the US is undermining the privacy of faculty members in this case. It distinguished the *Ontario Ministry of Natural Resources* and *Twentieth Century*

Fox cases on the basis that they dealt with statutory protections that included a reasonableness requirement.

The association submitted that article 3.10.6 does not have a reasonableness standard. It submits that the privacy right under article 3.10.6 includes a duty to take all appropriate measures to maximize privacy protection. It submitted that this obligation is similar to the 'necessity' requirement found in the Nova Scotia privacy legislation that was at stake in the *Dalhousie University* decision. It submitted this was higher standard than reasonableness. Further it submits that is not unreasonable to require a system that hosts email on a Canadian server because they already exist.

With respect to the employer's arguments based on art 3.20.1 concerning management being given a right to determine the level and manner of computer and technical services, the union submits that this refers to the type of telephone or computer or email service, but does not refer to the level of security of the service provided. Further it argues that the principle of interpretation of giving priority to the specific provision over the general does not apply here because you don't have two provisions dealing with the same right or subject matter. Further it notes that you cannot give preference to one provision or right if that would result in a complete overriding or undermining of the other provision or right. Rather if there is a potential conflict of rights then one is to attempt to interpret the provisions in a manner that does not result in rights under one provision violating rights under the other provision. Thus any interpretation of the employer's rights under article 3.20.1 must be done in a manner that recognizes and respects the privacy rights of the faculty under article 3.10.6.

Decision

After careful consideration of the evidence, the relevant provisions of the collective agreement, and the submissions of the parties, I have decided that the grievance must be dismissed. In short, I have concluded that the association has failed to prove a violation of the rights of faculty members under articles 3.10 (academic freedom) and 3.10.6 (privacy) by providing the faculty with an email system through Google's Gmail. My reasons are as follows.

First, I cannot accept the association contention that the recognition in article 3.10.6 "that Members have a right to privacy, consistent with the traditions of academic Freedom and the provisions of this article" imposes an obligation on the employer to take all available measures to enhance the privacy of the employer provided email. Such a claim is simply not consistent with the other relevant provisions of the collective agreement (in particular 3.20.1) or the arbitral and tribunal jurisprudence on the privacy obligations of employers under collective agreements and privacy legislation.

Nor can I accept the employer's primary argument, that the right to privacy under art. 3.10.6 does not apply to these circumstances given the management right under article 3.20.1. That provision gives the employer the right to "determine by consideration of the financial resources of the University, the manner in which and the level at which facilities and services are provided to Members." The same article goes on to oblige the employer to provide and maintain "reasonable levels of … computing … [and] technical services …". While that provision does give the employer an express management right

and discretion with respect to the provision of computing and technical services such as email, and the right to take into account financial resources in exercising that discretion, it does not give it an unfettered discretion to do as it likes without regard to the internal restraints within the article ("reasonable levels" must be maintained) or the other provisions of the collective agreement.

However, I agree with the employer submission that the recognition of a right to privacy for faculty members in art. 3.10.6 cannot be read as obligating the employer to take all available measures to maximize the privacy of the email system. When the right to privacy is interpreted in the context of the licence or grant of discretion given to the employer with respect to the manner and level of facilities and services and an obligation to maintain reasonable levels of computing and technical services (in art.3.20.1), it must be read as imposing an obligation on the employer to act reasonably and take reasonable security measures with respect to the provision of email services to faculty members and its impact on their privacy interests.

I note as well that such an interpretation is the one most consistent with the arbitral and privacy commissioner jurisprudence on employer obligations with respect to the protection of the privacy of employees under collective agreements or provincial privacy legislation. In that respect the employer submitted several arbitral and privacy commissioner precedents that dealt with challenges to employer decisions to retain a US based provider of data storage or email under a collective agreement or privacy legislation (See for eg. *Ontario Ministry of Natural Resources* (2012), *supra*; *Dalhousie University*, *supra*; *Twentieth Century Fox Film Corporation, su*pra; and *Lakehead*

University, supra). Those decisions appeared to all accept that transfers of personal data to the US in the provisions of storage or email services by third parties are not prohibited and the issue became whether the personal information remained protected by 'reasonable security measures'.

The association argument that article 3.10.6 obliges the employer to take any available measure to maximize the privacy protection of members' email is simply not practicable or consistent with the terms of the express grant of discretion given to the employer under article 3.20.1 with respect to computing and technical services such as email. It also ignores the express recognition of the employer right to consider its financial resources in determining the level and manner of providing such services. On this point I note as well that even in a case like *Lakehead University*, where the collective agreement appeared to expressly recognize a "right to privacy [for faculty members] in their personal and professional communications and files, whether on paper or electronic form", Arbitrator Carrier found that such language could not be read as an undertaking or guarantee to protect faculty from any form of intrusion or access either by the university or a third party to their professional or personal communications. He found such an interpretation to be too broad and impractical and not technologically achievable given the nature of email. He found that for the privacy protection clause to be given such a broad meaning with respect to email privacy it would have to refer explicitly to a duty to protect the email privacy of faculty from all manner of surveillance, intrusion or interception. In arriving at that finding he took note of the fact that email is not generally

regarded as a very secure medium for communicating sensitive or confidential information, a fact that was acknowledged by both parties in this arbitration.

Thus the provisions of article 3.10.6, when read in the context of the language of 3.20.1, can only be read as imposing an obligation on the employer to not act unreasonably or fail to take reasonable security measures in deciding on the manner and level of email services to provide to faculty members. I agree with the employer submission that in applying the standard of reasonableness or reasonable security measures, one must assess compliance based on a consideration of all the circumstances. Relevant circumstances considered by adjudicators in other privacy cases have included factors such as the sensitivity of the personal information, the foreseeability of a privacy breach and resulting harm, the relevance of generally accepted or common practices in a particular sector or kind of activity, the medium and format of the records containing personal information, the prospect of criminal activity and the cost of additional security measures (*Twentieth Century Fox Film Corporation, supra*). I would add to this list, the extent to which employer changes to the provision of services can be said to improve or worsen the protection for privacy interests of its employees.

Starting with the last mentioned factor, Dr Clement acknowledged that he was not familiar with the former on-premises email system of the employer or the security problems with that system. Nor was he asked to compare the former system and the current Gmail system with respect to privacy and other issues. Thus the association was unable to establish whether threats to the privacy or security of personal information of faculty members were actually worsened or increased by the move to Gmail for faculty

members. Instead, all attention in the association's evidence and argument was directed at an alleged increased threat with respect to surveillance by US state security agencies under the new system. I will say more about that increased threat later. My point here is that the union did not prove that the overall threat or risk to the privacy interest of faculty members was actually worsened by the move from the former email system at Laurentian to Gmail.

With regard to the other circumstances to be considered in assessing whether or not the employer provided a reasonable level of services or failed to take reasonable measures to protect privacy interests, in terms of the medium and the nature of the records at issue, both parties in this case and the arbitrators in other university cases have recognized the inherently insecure nature of email as a medium for sensitive communications. On that point there was evidence in both *Lakehead, supra*, and *Dalhousie, supra*, that senior IT officials at those institutions had cautioned users in the university community that email messages were no more private than a postcard (*Lakehead*, at para 13 and *Dalhousie*, at page 35). In addition, users were advised by IT officials in both cases that where privacy was imperative, other methods of communication and storage should be utilized (*Dalhousie University* at page 33, *Lakehead University* at para 13). On this point I am generally in agreement with the following comments by Arbitrator Outhouse at the conclusion of his award in *Dalhousie University*:

> Finally, it must be observed that email communications are far from being completely secure, even when hosted in Canada. They are subject to various forms of interception, hacking, sharing, etc. The comparison of emails to

> postcards, although perhaps somewhat of an exaggeration, is not inapt. Certainly, any person who entrusts personal information to email, particularly their work email, cannot do so with a high expectation of privacy. (at page 91)

Similar views on low expectations for privacy and security in communication by email were expressed by Arbitrator Carrier in *Lakehead University, supra* (at paragraph 20).

I note that Dr Clement agreed with the suggestion that Canadian researchers on a locally stored email system ought to take precautions when communicating with foreign sources who might attract surveillance to protect those communications from CSEC. He agreed there were other less convenient devices for communication they could use to ensure their privacy on such matters. While the notoriously low reputation for email as a method of private communication from any provider does not give the employer *carte blanche* with respect to selection of a provider, it does provide context for assessing the reasonableness of measures taken in the selection of a provider.

With respect to the circumstance of generally accepted or common practices in a particular sector or kind of activity, I agree with the employer submission that the fact that seven other Canadian universities, in addition to Laurentian, had adopted Gmail for their faculty email is relevant to assessing the reasonableness of the employer's decision to move in that direction. On this point, the employer's consideration of the PIA's done by three of the other universities that adopted Gmail before it made that move (Ryerson, Alberta and Memorial) is another important circumstance that forms part of the context for assessing the reasonableness of its decision. I will return to those PIA's below when

addressing the union's argument concerning the employer's failure to follow best practices. In terms of the employer relying on a move to Gmail being consistent with accepted practice in the university sector, I would add its consideration of the *Dalhousie University* arbitration award, *supra*, given that at the time of Dalhousie's adoption of Microsoft 365 for its faculty email in 2012-13, that email system relied on servers around the world (including in the US) for its cloud based email system. The challenge against the move to Microsoft under the Nova Scotia privacy legislation was based on the fact it would result in the storage of personal information outside of Canada. Thus when the employer was considering its options for email in the 2015 to 2017 period, the Dalhousie precedent has to be seen as being part of what was becoming a common practice of Canadian universities, moving to US based email providers with storage of information on servers in the US and other countries.

The sensitivity of the personal information at issue has also been recognized as a factor in assessing the reasonableness of an employer decision to opt for a US based provider of data storage. Dr Clement accepted that faculty members can, and in some cases should avoid using email for communication of their most sensitive information. In fact, he recognized that this may well be an advisable course of action for Canadian researchers dealing with sensitive information on a local email system, with Canadian storage for communications, when communicating with foreign senders or recipients. Thus the sensitivity of the information at issue is very much in the control of the user, in this case the faculty member who may well have privacy concerns when dealing with sensitive information.

With regard to the factor of the foreseeability of a privacy breach and resulting harm, for any attempt to compare the new Gmail system to the former Laurentian system, or an alternate system with servers based only in Canada, the picture appears to be very unclear, and quite unpredictable in terms of which system is more prone to state surveillance of email. Dr Clement agreed, during cross-examination, that he had taken the position in 2014 that CSEC surveillance of online communications in Canada was 'secretive, extensive and out of control'. He acknowledged in his testimony that he still agreed with that opinion. He also agreed that legislative regulation and oversight of state surveillance agencies like the NSA and CSEC was greater, at least in the formal sense, than in Canada. In addition, it was evident in the testimony of Dr Clement, and the evidence of Dr Michael Geist accepted in *Lakehead University, supra*, that there were several methods by which U.S. agencies could get access to email information transmitted in a Canadian based system, both with and without the cooperation of Canadian agencies.

To make the matter more complex, the following factors must be considered with respect to the likelihood of email sent on a Canadian based email system being subject to some form of electronic surveillance by a US state agency. According to a paper written by Dr Clement in 2016 (Addressing Mass State Surveillance Through Transparency …), approximately 28% of Canadian internet communications sent from one person located in Canada to or from another Canadian person will follow a boomerang traffic pattern with routing through the US at some point. This routing is due to the location of Internet transmission lines and Internet exchanges, and routing choices made by Internet

providers, and is not dependent on whether an email provider's servers are located in Canada or the U.S. Further, Dr Clement found, in that same paper, that 81% of communications between Canadian persons and persons in third countries were also routed through the US. This meant that a significant proportion of Canadian email communications were being routed through the US and made subject to US state agency surveillance through programs like Upstream that allowed such communications to be searched and intercepted while in transit, with no need to have access to a US based server where such data might be stored. Thus using an email provider with storage servers in Canada does not guarantee protection from U.S. state agency surveillance of email communications for a significant portion, if not the majority of emails (when both boomerang traffic routing and emails between Canadians and persons outside of Canada are both considered). Given these factors, and the evidence on the extensive CSEC surveillance and sharing of personal information gleaned from Canadian communications, it was difficult to make a conclusive finding on whether the foreseeability of a privacy breach and resulting harm was greater with an email provider based solely in Canada or one that also had US data storage.

The association's argument for a detrimental impact on privacy protection from the move to Gmail focused narrowly one on factor, that a system that allowed data storage in the US meant a loss of Charter protection for privacy rights in terms of access for US state surveillance agencies under US law while the data was in the US. But Dr Clement recognized that those same US agencies are also not subject to the Charter or Canadian law when they access the same personal information of Canadians while in

transit, either as part of boomerang traffic routing for email between two Canadian persons, or routing through the US for over 80% of emails sent between Canadians and persons outside of Canada. Thus those Charter protections are lost with respect to possible surveillance by foreign surveillance agencies for a significant portion of email communications whether the system is based solely inside Canada or not. Thus ensuring an email provider only has Canadian servers for data storage may only make a difference, in terms of reducing a risk of interference with an email user' privacy without Charter protection, for a relatively small amount of their email traffic, depending on who they primarily communicate with concerning sensitive information and the routing choices of their Internet provider. In any event, users worried about surveillance of sensitive information certainly could not rest easy with regard to worries about US state agency surveillance solely on the basis of the geographic location of their email servers. I note that this appeared to be a central point of the arguments made in the 2016 paper by Dr Clement on the need for greater transparency as to the risks to privacy inherent in electronic communications over the Internet (exh. 30, tab 1).

Finally, although I am in agreement with the association's argument that the employer failed to adhere to best practices in terms of performing a comprehensive TRA and PIA with respect to the decision to move to Gmail for faculty email in 2017, I am unable to find that his failure constitutes a violation of the collective agreement. During the hearing the association abandoned its initial claim in the grievance that the employer had violated article 2.30 with regard to the process to be followed for the alteration of existing practices for working conditions not covered by the collective agreement. In the

absence of a claim based on an allegation of breach of a process oriented provision of the collective agreement, I am unable to see the relevance of the award in *LUFA and Laurentian University (Selection of President) Gr)*, *supra*, to the issues in this case. Rather I accept the employer's argument that the employer can be found to have not followed best practices or procedures and yet arrive at a decision that does not violate the collective agreement by arriving at a 'not unreasonable' decision with respect to the provision of email services. Thus the real issue is not whether the employer followed proper or appropriate procedures to arrive at their decision with respect to the move to Gmail, but whether the move to Gmail itself can be found to amount to a failure to maintain reasonable levels of computing or technical services with respect to email, or be found to be a failure to take reasonable security measures providing for email services for faculty members. While the association may have established a failure to follow best practices or the most appropriate process to come to the best solution, it failed to prove the decisions actually taken by the employer amounted to a violation of the collective agreement.

Further, while the employer failed to do its own comprehensive TRA or PIA, it appears to have relied on the reports of other universities that did follow the best practices advocated by Dr Clement, and made enquiries with respect to the same threat to privacy represented by a move to Gmail that was being raised by the association during discussions over a 3.5 year period from 2013 to 2017. It was accepted in evidence that the employer considered the documents contained in exhibit 33 before arriving at its decision to move faculty email to Gmail. Those documents included the report entitled

"Seeing Through the Cloud ….", coauthored by Dr Clement, the PIAs done by Ryerson, Alberta and Memorial, and the arbitration award in *Dalhousie University, supra*. That evidence, together with the evidence of the association concerning its communication of the CAUT advice on the risks raised by moving to Gmail, indicates that the employer cannot be said to have been unaware of the risks to privacy raised by Gmail that were of prime concern to the association. While this somewhat "second hand" method of informing itself and making assessment of the risks raised by a move to Gmail could not be seen as the equivalent of having a current and custom fit TRA and PIA for Laurentian, it suggests that the decision arrived at cannot be described as negligent, ill-informed or per se unreasonable simply because of a failure to follow best practices.

I am of course in agreement with the association submissions on the central importance of academic freedom for faculty members to the mission of universities and their role in ensuring the proper functioning of democratic societies and systems of government (as per *McKinney, supra*). However, I am not able to find that the association has proven that the employer's decision to opt for Gmail for faculty members has impaired their academic freedom. Ms St Pierre testified that the union did not grieve when the employer made Google Documents available to faculty because it was not mandatory, but grieved the move to Gmail because it was mandatory. However, while there may be a university policy requiring faculty to use Gmail for corresponding with students, there was no evidence that faculty were compelled to use Gmail for correspondence regarding their research, or for the purpose of criticizing its employer or various levels of government. During cross-examination Dr Clement agreed that he

would advise faculty to use some other means to communicate with respect to sensitive information that might attract state surveillance, even if they had an employer-provided local email system that used only Canadian servers. In short, there was no evidence that the employer compelled faculty members to use Gmail for the communication of sensitive information concerning their research. Dr Clement admitted that there were alternatives available for the communication of sensitive information, even if it might be somewhat less convenient that the employer provided email system. There was no evidence given by a faculty member concerning interference with their academic freedom or privacy resulting from the employer move to Gmail. Given that context it is difficult to see how the employer's choice to go with Gmail as an employer provided email tool for faculty can be viewed as a threat to the academic freedom of faculty members at Laurentian.

For all the foregoing reasons, I am unable to find that the association has established any violation of the collective agreement by reason of the employer's decision to move faculty email to Gmail. The grievance is hereby dismissed.

Signed in Guelph this 4th day of May, 2020.

Arbitrator Brian Etherington