Lakehead
UNIVERSITY Office of Risk Management and Access to Information

Tel.: (807) 343-8518; 343-8267
Fax: (807) 346-7735
Email: mshaw1@lakeheadu.ca

MEMORANDUM

TO: Inquirers about Lakehead University's Adoption of Google's Gmail System

FROM: Millo Shaw, Director of Risk Management and Access to Information

DATE: August 1, 2007

RE: Arguments in Defence of Switching to Gmail

The practical advantages of adopting Gmail are well known. The system has fewer problems and "down time" than the one we were using – for the simple reason that Google can afford the significant resources necessary to keep their system operating efficiently: for example, they have back-up servers in place in case their main servers crash; we did not; and they have staff dedicated solely to ensuring that their system remains operational 24 hours a day, 7 days a week, which we did not. Gmail gives all users over 2 gigabytes [as of Sept. 2012 **25 gigabytes**!] of storage, which is more than 13 times greater than the maximum of 150 megabytes to which we were restricted before. It also gives access to more services (e.g. the Calendar that has enabled us to give up our old and expensive appointment setting software, and "instant messaging technology" – the new wave in electronic communication). Google's system is, in general, more user-friendly.

Concerns have been raised, however, about the Google service's security – particularly with respect to protection of privacy. When discussing the security of email systems, one has to keep in mind that "security" is, in this context, an entirely relative term – for the simple reason that email is, almost by definition, a fundamentally insecure means of communication – unless extraordinary and restrictive – and obstructive - measures are put in place. On the one hand it would be at least theoretically possible to set up a special system that would be completely closed-circuited – but, for the provision of electronic communication beyond a single location, such a system would be difficult to establish and expensive, for it would have to ensure not only that access to the system would be completely secure, but also that no one would be able to send, copy, or forward an email message to anyone outside the system, and it would have to have completely dedicated transmission lines and servers. On the other hand, senders can acquire software that encrypts their messages – but this requires every receiver to have some means of securely acquiring each sender's encryption key (and each sender would have a different key!). While such a set up is certainly conceivable on an individual basis, trying to extend it to an institution's entire email service would be both very complicated and very expensive. Both of these alternatives to regular email service would be obstructive and, indeed, frustrate the main attractions of email transmission over the internet: facilitation and speed of communication. Indeed, it is highly questionable whether such trammeled systems could even be accurately called "email" as the term is generally understood. Standard email transmission, however, is susceptible to intrusion. It can be penetrated both by hackers and service providers at any number of points - as a careful reading of the terms and conditions of <u>any private service provider's email contract will confirm</u> - whether the email server is based in Canada or the US. To use the standard analogy, one should consider regular email communication as no more confidential than sending a postcard by mail. For this reason there is significant case law supporting the proposition that privacy cannot be guaranteed for email communications (see, e.g., ***Re Camosun College and Canadian Union of Public Employees Local 2081***, [1999] B.C.C.A.A.A. No. 490, paragraphs 20-29 and ***Re Naylor Publications Co. (Canada) and Media Union of Manitoba*** (2003), 73 C.L.A.S. 116 at page 26).

With this reality in mind, before committing Lakehead University to switching over to Google's Gmail service, the Director of the Technology Services Centre (TSC), in consultation with myself, both of us reporting to the Vice-President (Administration and Finance), considered the privacy implications - and concluded that our use of Gmail would not be likely to breach privacy more than did our - or anyone else's - current email service. On the contrary, the evidence was that Gmail would give us overall <u>***much better***</u> privacy security than we ourselves - or anyone else - provided or could provide. Following are our responses to specific concerns about Gmail's security:

(1) <u>**Technical Vulnerabilities**</u>: Software bugs are a fact of life. Virtually every major software system (e.g. Microsoft, Sun, *et al*.) has them, and since every computerized electronic communications system relies on software, most email systems have vulnerabilities created by these bugs. We were responsible for making sure that our former system stayed patched from problems to which its creators alerted us - but, frankly, had to rely on nothing more than a wing and a prayer that the vulnerabilities we didn't know about wouldn't be exploited. TSC simply did not (and does not) have the hefty resources necessary to guard against all such risks. This is a major problem for ALL technological service providers who do not author their own email systems.

By contrast, Google DOES have sufficient resources to search out and protect against possible software vulnerabilities.

- The Gmail servers have firewall protection that our old system couldn't match – and they employ additional intruder prevention technology that we did not and do not possess.

- Google monitors their system for attacks 24 hours a day, 7 days a week; we did not and could not afford to.
- Google can control physical access to their servers; our security cannot match their standard.
- Google can afford to apply top-of-the-line antivirus and antispam solutions to their system; we could not and cannot.
- The one software vulnerability that they did discover - the first of its kind – was very circumscribed. It was reported Dec 30th, 2006 and affected only the Google Video offering, not the Google "Apps for Education" through which we get Gmail (Google "Apps for Education" has a separate infrastructure). Google has confirmed that such a problem did not and could not touch the Gmail system; moreover, this particular exposure was resolved within one day - making it very unlikely that any exploitation could have taken place. In view of the security resources available to Google, such a sterling record is not surprising.

Technically, then, we have much better security with Google than we could ever even have hoped to provide for ourselves. We did have numerous improvements in the works to enhance the security of our former system, but even after their full implementation we would not have been able to match the level of security provided to us by Google. Moreover, it is highly unlikely that any university anywhere can genuinely claim that their email system security is better than Google's ***or, frankly, comes even close to it***. We are confident that, by adopting the Google service, we have provided our Users with one of the best and most secure email systems available, and far superior to what we were offering and could offer before - period.

(2) **Access by External Individuals and Entities**: Concern has been expressed about access available in the Google system to non-users and the U.S. Government – in the latter case because the *USA PATRIOT Act* (actually an acronym for the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001") allows the American Government to peruse records stored on U.S. servers. Keeping in mind that anyone who truly wishes an ironclad guarantee of security in the communication of their personal and confidential information should NOT be using **any email system** (including Lakehead's old system), we do not view this concern as having sufficient weight to justify declining or abandoning Gmail.

First, **every email system** permits system administrators to access email communications under certain restricted circumstances – as a perusal of the terms and conditions of service of any private email operator will confirm. Lakehead's adoption of Gmail, however, has actually made this a more difficult process for our system administrators.

- Not only does Google have a strict access code in this regard, but Lakehead's technical staff must now seek Google's approval before accessing emails sent or received by University users – a bar to access that did not confront them in the administration of our old system.
- And Lakehead server administrators can no longer, as they were able to before, monitor all incoming and outgoing email communications; such monitoring can now occur only with Google's restrictive permission.

Second, access by the U.S. Government to Gmail users' personal information stored on Google's American servers, while a possibility, is nevertheless restricted, and must be considered in the context of email communication and the internet in general:

- Google, to our knowledge alone among US service providers, has not granted the US Government, when they've requested it for security reasons, informal access to their files and servers - but has insisted that such requests be backed up by formal judicial orders. Now a warrant issued under the *PATRIOT Act* cannot be disregarded or even reported by the recipient, but we have Google's assurance that, to the extent permitted under American law, they will actively resist such warrants if and when they are issued. And it should be noted that, even under the *PATRIOT Act*, the American government must convince a Court – albeit the highly secretive Foreign Intelligence Surveillance Act (FISA) Court – to issue a warrant before it can gain access to such electronic correspondence.
- It is true that, if Lakehead had its own servers from which to send and receive email transmissions, or if it relied on the servers of a company that was wholly Canadian and not in any way directly or indirectly controlled by an American entity, the American government would not be able, without resorting to clandestine means (and it is probable that the American government has highly sophisticated and extensive clandestine access capability), to access information residing in those servers. **Such an arrangement could NOT, however, guarantee exclusion of American government access to email messages either originating, or that could be sent, OUTSIDE the University's system – in other words, potentially ALL email messages in the University's email system – for the simple reason that neither the University nor any other entity could or can secure the sources or ultimate transmission of such messages which may have been or may be, at some point, routed through servers/equipment owned or ultimately controlled by U.S. companies – where the messages would be potentially accessible to the American Government through the *USA PATRIOT Act*.** As far as the American courts are concerned – at least to the extent that they have expressed views in this area (as in Hunter Douglas Inc. v. Comfortex Corp [1999 WL 14007 (S.D.N.Y. 1999)]) – it would appear that "the test to determine whether a corporation has custody and control over documents located with an overseas affiliate is not limited to whether the corporation has a legal right to those

documents, but rather focuses on whether the corporation has "access to the documents" and the "ability to obtain the documents" (David Keeshan, “Patriot Act Controversy Heats Up,” in *The Riley Report* (http://www.rileyis.com/report/july04.htm) for July, 2004).” That being the case, personal information passing through equipment even in Canada that belongs even to a Canadian company is potentially accessible to the American authorities if that company is ultimately controlled by an American firm or even just affiliated with that firm. The practical conclusion to be drawn from this state of affairs is inescapable: **anyone who wants to guarantee that their email communications remain beyond the reach of the American government must refuse to send or respond to email not only in the United States, but even in Canada or anywhere else in the world** – that is, unless they are willing to use one of the highly restrictive and cumbersome security procedures (involving a completely closed circuit or encryption) described earlier in this memorandum.

- It is also worth noting that the Canadian government, under the “Anti-terrorism Act” which received Royal Assent in December, 2001, has no less secret access, by warrants secretly obtained, to Canadians’ electronic communications than has the American government to communications controlled by Americans. Moreover, while Canadians may have less objection to their own than the American government snooping through their private electronic correspondence without their knowledge or consent, there can be no basis for confidence that their personal information will not end up in the hands of American authorities – for which the Maher Arar case provides an object lesson.

Conclusion:

In conclusion, in an imperfect world and in the light of the inherent and so far ineradicable security weaknesses in email as a medium of communication, we believe that we've chosen the best practical option available to us. We have made one concession: we do not insist that only Gmail be used for email communication to the University, and we do not compel students, faculty, and staff to adopt it - they actually have to sign into it, and formally agree to its terms of service and use before being granted access – although we do use it as an official means of communicating with the members of the Lakehead University community.