FTR Now

Cloud Computing, Second Life and the University

Date: September 17, 2008

This short university sector bulletin raises an important policy issue about setting rules that govern the choice faculty and staff have in using the internet to perform their jobs. We would like to raise and invite a policy discussion on the legal issues raised by “cloud computing” and the increasing business use of consumer-marketed internet applications such as Second Life.

TRADITIONAL COMPUTING

The still-dominant model by which most of a university’s administrative computing needs are met is based on the personal computer. Universities use software that resides on personal computers and processes data on personal computers. Universities also store electronic information on personal computers, or at least on computers that reside within a network of university-owned or university-controlled computers.

The security risks associated with this model of computing are well-understood and have been accounted for in computer use policies with fairly standard terms – terms about virus protection software, terms that prohibit installing software and terms that deal with password security, for example. The same policies also ensure that universities control the information on the computers they own. Most university computer use policies limit personal use, reserve a right of ownership over all stored information and specify that employees and other users should have no expectation of privacy.

WHAT IS CLOUD COMPUTING?

“Cloud computing” is the name for a new means of accessing computing power. The cloud is a metaphor for the internet, and in cloud computing, people access computing power through the internet. The software used to process data in cloud computing often resides on another organization’s computers and the information processed is also often stored externally.

We’re all familiar with internet-based applications like MS Hotmail and Facebook, but there are also internet-based applications that are marketed to consumers as business productivity tools, the most popular being the “Google Apps” suite. Google Apps includes chat and collaboration applications, a calendar application and spreadsheet and presentation applications, for example, all freely-available to consumers and with significant potential for improving business productivity.

WHAT’S THE RISK?

Given that freely-available internet applications with real potential to improve productivity are proliferating, university employees now have a great degree of choice in how they meet their work-related computing needs. Yet the exercise of such choice can cause a university to suffer a near complete loss of control over confidential university information, student and employee personal information and other work-related information in which it has an ownership interest.

Consider the example of an administrative staff member who uses an externally-hosted and freely-available internet-based “wiki” to encourage collaboration on her department’s work. She signs up for an account and invites colleagues to do the same. She and her colleagues agree to terms of service that grant them some control over the web pages they create, but the service provider also reserves a very broad right of use over content. Most significantly, the university itself is an apparent third-party to the contractual relationships entered into by its employees, and has no effective right of control.

The wiki works well, and after a year of use, it contains a significant amount of useful and sensitive content, all of which is

related to the department's business and some of which includes student personal information The wiki is password protected, but the security-related promises in its terms of service pale in relation to those the university requires in its own outsourcing contracts.

Here are the main risks and costs associated with this arrangement:

- The information is not necessarily secure from loss, theft and misuse. Regarding student personal information, the university may be in breach of the safeguarding duty imposed by the *Freedom of Information and Protection of Privacy Act*.[i]li>
- It is relatively easy for the participants, should they depart from employment, to take the information. The university may have a legal right to control it based on its right as employer, but the service provider will not likely recognize this right absent a court order.
- The university doesn't know that information is there. If there is a legal claim to which the information relates, it may be overlooked in the university's e-discovery process. The university could lose the benefit of the information if it is helpful evidence or, if it is not, may face production-related sanctions. In either case, it has now become more costly to search for, retrieve, process and produce electronically stored information in the course of the litigation.

Universities shouldn't blame the vendors of internet-based applications for what is really a problem of internal control. There are very controllable risks associated with the use of internet-based applications that are provided as part of an "enterprise" service package that is based on university-to-vendor legal agreements. Such "standard" outsourcing arrangements have been the subject of comment by Canadian privacy commissioners, who have suggested that outsourcing is fine provided notice of the outsourcing relationship is given and the service provider gives certain contractual assurances.[ii] A university will not receive the benefit of any such assurances when its employees *register themselves* to use internet-based applications for work-related purposes.

USE OF SECOND LIFE

Second Life is an internet-based application that is of particular interest to universities and their faculty. Hosting classes in Second Life's online virtual world has been tried and has been touted as having the potential for greatly improving distance education.[iii] Yet for all of Second Life's potential, it has a particular makeup that demands universities be particularly sure to retain control over its use.

In his article, "Second Thoughts About Second Life,"[iv] Michael Bugeja of Iowa State University raises the potential for liability associated with requiring students to register for Second Life in order to participate in a course. Mr. Bugeja's focus is on the risks inherent in participating in the Second Life virtual world, in which anonymous communication is made the norm by virtue of Second Life's design,[v] and which itself is prided by its proprietor Linden Lab as a "free-form canvass [where] you can do what you want, and be what you want."[vi] As Mr. Bugeja suggests, universities can require faculty members who invite students onto Second Life to ask students to acknowledge risk and waive liability (as they would for any field trip). There are, however, regulatory requirements which cannot be so waived.[vii]

The regulatory requirements most likely to be engaged by the use of Second Life are those relating to the duty to provide a harassment and discrimination free environment, especially the aspect of this duty that requires universities to investigate incidents of discrimination and harassment and restore an educational environment poisoned by discrimination and harassment.

If a student is harassed in Second Life's virtual world and suffers real world harm, is the mere fact that the student registered for Second Life enough to engage a university's duty? If the duty is engaged, either on the broad theory above or based on the specific context in which the harassment takes place, how does a university investigate when most information about the event will be electronically stored and controlled by Linden Lab? Unless it has entered into a legal relationship with Linden Lab itself,[viii] a university with a duty to investigate may be confronted with a common problem associated with uncontrolled use of internet-based applications – it may need access to information held by Linden Lab yet will have no legal right of

access to it absent a court order.[ix] Similarly, it will have no legal right to issue authoritative directions to Linden Lab if necessary to restore the educational environment.[x]

POLICY OPTIONS FOR UNIVERSITIES

The correct policy approach for resolving the issues we have raised is by no means clear, and as external legal counsel to universities, we respectfully defer to our clients on matters of university policy. We do, however, wish to make the following general suggestions:

- An absolute ban on the use of internet-based applications in university business is likely too strong of a response. Even an internet search, for example, relies on the use of an external organization's computers.
- A more favourable approach would involve establishing a general rule requiring that university business be conducted on the university's computer system, an approvals-based exception and a specific duty to ask for approval to use unapproved internet-based software applications. The criteria established for approval should draw a link to the university's information technology strategy and other policy-based imperatives (e.g. those relating to academic freedom), and might allow for reasonable use of internet-based applications that meet needs that are not currently provided for and which may not be met through a more standard outsourcing arrangement (i.e. one that relies on an legal agreement between the university and the service provider).
- Along with the general framework for approvals, universities may also put employees on notice that certain applications should not be used to conduct university business. For example, it may be prudent to completely prohibit the use of internet-based applications like Hotmail for work-related purposes.

We hope this document encourages discussion about a relevant and difficult issue. If you have any questions, please feel free to contact your regular Hicks Morley lawyer.

With thanks to Heather Colman, our Knowledge Management Specialist.

i R.R.O. 1990, Reg. 460, s. 4.
ii See e.g. PIPEDA Case Summary #313.
iii See e.g. Daniel Terdiman, "Campus Life Comes to Second Life" (2004) Wired.com and Education Programs – Second Life Grid.
iv Michael Bugeja, "Second Thoughts About Second Life" (2007) The Chronicle of Higher Education.
v For example, Linden Lab assigns Second Life users a last name: Second Life – FAQ.
vi Daniel Terdiman, "Phony kids, virtual sex" (2006) CNet News.
vii Wall and University of Waterloo (Re) (1995), 27 C.H.R.R. D/44 (Ont. Bd. Inq.) is a leading case on these duties.
viii Linden Lab does offer a secure "intranet" space for restricted membership to certain students and faculty. Linden Lab may offer universities special terms to give them greater control over information related to their virtual classrooms, but we are not aware of the terms on which Linden Lab contracts with educational institutions.
ix Article 6.1 of the Second Life Terms of Service specifies that Linden Lab will not give personal information to third parties except to "operate, improve and protect its service," but by the same article Linden Lab also reserves the right to disclose information to "private entities" as it believes is necessary or appropriate to resolve possible problems or inquires: Second Life – Terms of Service.
x Article 4.1 of the Second Life Terms of Service requires Second Life users to comply with a set of Community Standards and other rules of use established by Linden Lab. However, Article 5.1 of the Second Life Terms of Service specifies that Linden Lab has the right but not the obligation to resolve disputes between users: Second Life – Terms of Service.

The articles in this *Client Update* provide general information and should not be relied on as legal advice or opinion. This publication is copyrighted by Hicks Morley Hamilton Stewart Storie LLP and may not be photocopied or reproduced in any form, in whole or in part, without the express permission of Hicks Morley Hamilton Stewart Storie LLP. ©