

GOOGLE APPS FOR EDUCATION

OCAD U STUDENT EMAIL SERVICE PRIVACY & RISK ASSESSMENT

July 27, 2011

On May 9th, 2011 OCAD University's Information & Communication Technology Governance (ICTG) Steering Committee approved a recommendation from Student Affairs and IT Services to adopt Google Apps for Education as a new service to replace the Horde student email and calendaring system that was implemented for September, 2004. Approval for implementation of Google Apps for Education by the ICTG Steering Committee was conditional on finalization of a Privacy Impact Assessment and Risk Assessment sponsored by the VP, Academic and VP, Finance & Administration.

CLOUD BASED SERVICES

One of the key strategic considerations the University needs to make is how most effectively to engage with and benefit from the cloud; compute resources, available from third parties, outside the OCAD U network. All sectors are looking to the cloud to create efficiencies, reduce overhead, improve services and align with the accelerated rate of change being driven by web enabled technologies.

OCAD University should move away from duplicating and attempting to compete with the capacity, functionality, scalability and stability provided by many cloud based services. If OCAD U plans to migrate commodity services such as email and calendaring to the cloud the University needs to consider the following:

- Does the cloud present a more secure, feature-rich and cost effective option in every case?
- How much institutional authority can extend to the cloud and how much is needed?
- What institutional accountability is involved in integrating the cloud with student and faculty services and support for teaching, learning, studio and research?
- Who will monitor the activities and records that users leave in the cloud and what security is in place to protect users and the University?

OCAD U needs to certify cloud based services, that it requires students to use, based on good security, open standards, robust ID management, encryption, data management protections, auditing requirements, reporting capabilities and business continuity.

GOOGLE APPS FOR EDUCATION

Google Apps for Education is a free, cloud based service providing email, calendaring and storage, at no cost, to students, faculty and staff at educational institutions, based on negotiated contracts and Google's terms and conditions of use for the service. The service is provided to educational communities free of the text advertising and data mining associated with the Google Apps service available to the general public. OCAD University has negotiated a five year contract for the service beginning in August, 2011.

A number of other Canadian universities and colleges have adopted or are adopting the Google Apps for Education Service including University of Alberta, Humber College, Wilfred Laurier, Nipissing University and University of Windsor.

PRIVACY IMPACT ASSESSMENT

A Privacy Impact Assessment (PIA) examines transaction level data flows and how they align with policies, legal requirements, user and stakeholder expectations and requirements.

RISK ASSESSMENT

A security Risk Assessment is intended to satisfy the requirement that data protection is equal to or greater than those systems already in place and that account generation and administration for the service is fully secure and administrative controls allow OCAD U to apply relevant institutional policies to the service(s).

PRIVACY IMPACT & RISK ASSESSMENT WORKING GROUP

Student Affairs and IT Services jointly recommended the establishment of a Privacy Impact & Risk Assessment Working Group to lead and facilitate review of Google Apps for Education in the context of guidelines available through The Office of the Information & Privacy Commissioner of Ontario and the best practices of relevant Canadian Universities who have already conducted PIA's and Risk Assessments in relation to the Google service. The Privacy & Risk Assessment Working Group included the following representation:

- Alastair MacLeod, Director, IT Services
- Deanne Fisher, AVP, Students
- Elisabeth Paradis, Registrar
- Geeta Sharma, Director, Risk Management
- Lynn Austin, Archivist/Records Officer
- Jonathan Graham, Manager, Enterprise Architecture & Development
- Kyle Nhan, Assistant Risk Management

PROCESS USED

OCAD University used a similar methodology as the University of Alberta, who recently rolled out Google Apps for Education services for all faculty, students and staff replacing their multiple legacy email and calendaring systems. The University of Alberta successfully negotiated a comprehensive contract for adoption of the Google Apps for Education service that was considered to meet the requirements of the University, the Province of Alberta's FIOPP (Freedom of Information and Protection of Privacy) Act. OCAD University was provided access to many of the key documents and templates used by the University of Alberta and modified some of those templates to facilitate the Privacy Impact and Risk Assessment.

RESEARCH & INVESTIGATION

The OCAD University Privacy & Risk Assessment Working Group networked extensively with other Universities and related organizations leading adoption, review and discussion of strategies for implementation of cloud based email and calendaring solutions including:

- University of Alberta
- University of Toronto
- Ryerson University
- Wilfred Laurier
- CUCCIO (Canadian University Council of Chief Information Officers)
- ACSO (Association of Computing Services Directors) of Ontario

Members of the OCAD University Privacy & Risk Assessment Working Group also attended the following conferences and symposiums where extensive review of cloud based email and calendaring services was discussed:

- Ryerson University's symposium on Email & Collaboration Tools
- CANHEIT (The Canadian Higher Education IT Conference)
- OUCC (Ontario Universities Computing Conference)

The OCAD University Privacy & Risk Assessment Working Group conducted comprehensive reviews of the following legislation, policies and documents:

- Ontario FIPPA (Freedom of Information & Privacy Protection Act) legislation
- Ontario Privacy Commissioner "Privacy By Design" and "Privacy in the Clouds" reports
- "Privacy and Cloud Computing" report by David Fraser of McInnes Cooper, legal expert on Canadian privacy legislation
- OCAD University Privacy & Risk Assessment Working Group
- Google Apps Technical Support Services Guidelines
- Google Apps Acceptable Use Policy
- Google Enterprise Products Security Standards

GUIDING PRINCIPLES FOR ASSESSMENT

The following guiding principles were used for conducting assessment of the Google Apps for Education service and contract:

- All email is considered confidential
- Email is generally not considered a secure communication medium
- All information created or maintained through the service remains under the custody and control of the University
- Information is protected against unauthorized collection, use and disclosure
- Provider meets the requirements of FIPPA/PIPEDA where applicable.

- FIPPA and PHIPA data must be encrypted as per the Privacy Commissioner for Ontario.
- Account permissions/Authentication protected while in transit
- OCAD U is required to be able to monitor activity for the service
- Health related (PHIPA) - Student medical information should not be communicated via email
- Consideration as to other sensitive topics inappropriate for email (disabilities, censure, standing, financial matters, etc.)
- Assessment of Google as an appropriate service provider
- A threat/risk analysis to determine security standards

GUIDELINES FOR CONTRACT NEGOTIATIONS

Agreements for contracting for information held by third party service providers are advised to address the following:

- Limit service provider to only using your data for your purposes and for no other purposes.
- Include provision that data is held "in trust" for customer.
- No disclosures of information without consent.
- Obligation to resist - to the extent lawful - orders to disclose information without consent.
- Liquidated damages for any disclosure without consent.
- Obligation to cooperate with you in any regulator's investigations.
- Will not deal with any regulators related to your information without your participation.
- Implement safeguards to protect information - set minimums but shift as much responsibility to the service provider.
- Do not accept any limitations of liability related to privacy and security - full indemnity.
- No retention of your information.

FINDINGS

Privacy Impact Assessment

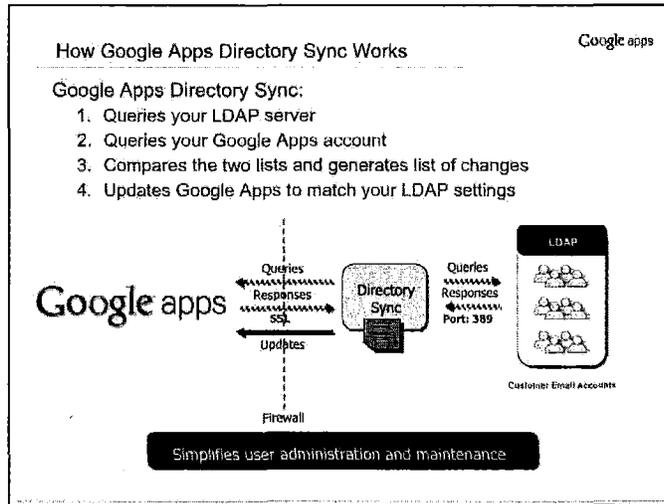
The Privacy Impact Assessment process collected information regarding institutional privacy management, structure and organization as well as privacy considerations specific to the Google Apps for Education project. Institutional privacy management varied depending on specific departments operating as custodians for personal information. The Office of the Registrar, the primary custodian of student personal information, reported adherence to comprehensive privacy controls, management, processes and policies. Since the Office of the Registrar uses the student email system as its primary means of communication with students regarding their status at the University their adherence to privacy controls, management processes and policies is considered essential

In a broader context, organizationally, based on review by the OCAD University Archivist/Records Officer and institutional FIPPA coordinator, OCAD University was reported to still be in process for implementation and updates to policies and controls that ensure full compliance with FIPPA legislation.

Whereas in most areas OCAD University's understanding of FIPPA compliance and management of personal information was being effectively addressed, some further review and formalization of process and departmental adoption of those practices is still in progress. All University IT Services staff that will administrate access to administrative consoles for the Google Apps for Education service have signed institutional confidentiality agreements as a condition of their employment.

Specific to the Google Apps for Education Sync project the Privacy Assessment identified the need to formally document the following:

- Personal information and data elements to be collected as part of the project
 - The following information is stored:
 - Surname and Given Names
 - Student number
 - Student User ID (aa01xx)
 - Password in hashed SHA-1 format
 - Diagrams indicating flow of personal information
 - Google Directory Sync Overview
 - Google Directory Sync is a software application that runs on OCAD U Servers
 - Queries our main LDAP repository on the ACS domain (ACSDC)
 - Google Apps communicates via SSL encryption to Directory Sync the list of users that need to be created and passwords synchronized through our institutional firewall
 - All traffic from Directory Sync travels from the 317 Data Centre through the Orion Research Network to Google directly, and not over the Commercial Internet¹



¹ <http://www.orion.on.ca/newsletter/jun10/buzz.html> "ORION peers directly with Google, allowing ORION institutions to access Google resources over the network, bypassing commercial Internet. ORION also provides connectivity and hosts CANARIE gear at ORION's facilities at Toronto Front Street (TFS) in Toronto."

- Identification of employees who will have access to personal information
 - Any Help Desk Support Assistant or Technician have access to Active Directory, and the Personal Information listed above, however the password is hashed and not human readable unless unhashed.

Whereas this documentation is now regarded as essential to moving forward with this project it was noted that equivalent documentation was not developed for the current Horde student email service.

Amendments to OCAD University “Privacy and Personal Information Collection” notice will be undertaken to reflect any relevant information regarding collection of personal information related to the Google Apps for Education service.

Many of the Privacy Controls and Security are addressed through Google, as the service provider, and are assessed in more detail below. Contractual requirements ensuring OCAD University ownership and jurisdiction over institutional data (including student email content) are articulated in the contract with Google and are described in the “Provision of Service and Agreements” section of this document. However formalization of OCAD University IT Services processes and privacy controls for management of personal data requires updated documentation. Updates to existing IT Services policies and guidelines relevant to the handling of student personal information will be based on consultation with the Office of the Registrar, review of existing policies and Google Enterprise Products Security Standards and Google Apps for Education Acceptable Use Policy.

Threat and Risk Assessment

Two primary criteria were assessed for risk factor impact and mitigation:

- Risks to the Inappropriate Collection, Use, Disclosure and integrity of Personal information
- Risks to the Generation, Use, Transmission, Availability and Authorized Destruction of Records of the University

Within each of these criteria two classifications of data were assessed:

- Infrastructure Data: This is data which is required for the setup and maintenance of accounts. Google will have access to this information even if the student does not use their Gmail account, which in that case the information will be limited to the student’s full name, their student number and, potentially, their encrypted password.
- Email Data: This represents the information from the contents of email sent or received by users of the Google Apps for Education system.

In all cases assessments were based on:

- Risk Factor
- Probability
- Severity

- Assessment details
- Mitigation (if necessary)

Probability and Severity were assessed as being “less than”, “equal to” or “greater” than risk associated with the current service; the OCAD U Horde student email system.

In 11 cases out of 13 the probability of risk associated with the Google Apps for Education solution was considered to be “less than” or “equal to” the probability of risk associated with the current Horde student email system.

In all 13 cases the severity of the impact associated with the occurrence of the risk was “equal to” the impact associated with the Horde student email system.

The two cases where the probability of risk associated with Google Apps for Education was considered to be “greater” than the current Horde student email system were:

- Possible information breach by services provider compromising the integrity and authenticity of University Information
- Changes in service provider’s business model compromising integrity or availability of University information

These two risks were recommended to be mitigated through contract language requiring notification before changes to Google business processes (see “Provision of Service & Agreements”) and enforcement of mandatory student email password change and stronger password rules, which would make any decryption of student email passwords infeasible, in relation to any attempted breach.

PROVISION OF SERVICE & AGREEMENTS

Service Administration

Google provides an online administrative console for service administration providing designated OCAD U Google Apps administrators full control of reporting functions and the services provided to end users.

Data ownership, access and disclosure

In the Google Apps for Education Agreement customer data is defined as all OCAD U data, including email, provided, generated, transmitted or displayed via the Google Apps for Education services by OCAD U or the end users (students) of the service. Customer data is considered to be OCAD U’s confidential information. Confidential Information cannot be disclosed, except to relevant OCAD U or Google affiliates, employees and agents who have agreed in writing to keep it confidential and who need the confidential information to exercise rights and fulfill their obligations under the terms and conditions of the agreement. Google and OCAD U are both responsible for any actions of their respective affiliates, employees and agents.

Privacy Legislation

The contract defines Google as “merely a data-processor” and that its responsibilities do not extend to the internal management or administration of the services for OCAD U end users. The contract acknowledges that customer data may include personally identifiable information, that is subject to privacy legislation and that, in its capacity as a service provider, acting on behalf of OCAD University, Google will comply with relevant privacy legislation.

Third Party Disclosure

It is possible, that at some time during the term of the agreement, a third party may request records or information relating to the service or end user data. In all cases OCAD U would be solely responsible for responding to these requests.

If a request, by a third party, for OCAD U confidential information, as defined by the terms of the agreement, was made directly to Google, Google will, to the extent allowed by law and by the terms of the third party request: (a) promptly notify OCAD U of its receipt of a third party request; (b) comply with OCAD U’s reasonable requests regarding its efforts to oppose a third party request; and (c) provide OCAD U with the information or tools required for OCAD U to respond to the third party request.

Each party may disclose the other party’s confidential Information when required by law or valid legal order, such as a search warrant, court order or subpoena, but only after it, if legally permissible: (a) uses commercially reasonable efforts to notify the other party; and (b) gives the other party the chance to challenge the disclosure.

Liability

Under the terms of the agreement, liability for Google and OCAD U is limited, except in relation to breaches of confidentiality obligations or violation of intellectual property rights by either party.

Security Systems

Google provides detailed specifications for security levels in their Google Enterprise Security Standards and states in the agreement that all facilities used to store and process OCAD U data will adhere to reasonable security standards no less protective than the security standards at facilities where Google stores and processes its own information of a similar type. An assessment of the Google Enterprise Security Standards was incorporated in the OCAD U Risk Assessment referenced in this document.

Encryption and Authentication

Google Apps for Education by default encrypts all aspects of a session, including account permissions and authentication while in transit, using Secure Socket Layer (SSL) encryption. This meets requirements stipulated by relevant privacy legislation.

Google Apps for Education ensures passwords are encrypted using SHA1, a Secure Hash Algorithm, that provides encryption of data. Passwords will be stored at Google in encrypted form. OCAD U will also be enforcing strong password rules making decryption infeasible.

Data Retention and Termination

In the event that the service is terminated or the agreement is not renewed, under the terms of the agreement, Google will provide OCAD U access to, and the ability to export, the OCAD U data. After a commercially reasonable period of time, Google will delete OCAD U data by removing pointers to it on Google's active and replication servers and overwriting it over time; and upon request each party will promptly use commercially reasonable efforts to return or destroy all other confidential information, as defined under the terms of the agreement. Terms of the agreement that reference confidential information, intellectual property rights and liability will survive termination of the agreement.

Jurisdiction

The agreement states the terms of the agreement will be governed by New York state law. Agreement as to legal jurisdiction was based on the University of Alberta's legal assessment that New York State privacy laws are considered to be similar to Canadian privacy legislation.

Data Location

For Canadian Universities considering adoption of Google Apps for Education it is recognized that the data is not stored in Canada and that the data is hosted on Google servers in the United States or in any other country in which Google or its agents maintain facilities. As a U.S. company Google is governed by laws and regulations maintained by the U.S. Department of Commerce, including trade and economic sanctions, which restrict storage of data in specific countries considered hostile to U.S. interests.

The Province of Ontario does not restrict public sector institutions from hosting data outside of Canada and the Information and Privacy Commissioner, Ontario does not actively discourage use of cloud based services hosted outside Canada. However some institutions have expressed concern regarding U.S. Patriot Act law enforcement surveillance and investigative powers. Whereas under FIPPA the University has an obligation to comply with FIPPA legislation, in terms of the control and ownership of personal information for which they provide a service, a Canadian law enforcement agency can disclose personal information to a foreign country. According to David T.S. Fraser, a Canadian privacy lawyer, practicing privacy law with the Atlantic Canadian firm of McInnes Cooper:

- The Canadian Anti-terrorism Act of 2001 amended the Criminal Code, CSIS Act and National Defense Act.
- The CISC Act allows for interception or access to email through a wiretap order or search warrant and allows for specially designated judges from the Canadian Federal Court to grant secret warrants.
- Canadian ministers can authorize interception of private communications for the purpose of foreign intelligence.
- Mutual legal assistance treaties allow Canadian authorities to get warrants for US authorities and vice versa.

- Canadian authorities can get information in the US without a warrant and American authorities can get information in Canada without a warrant
- Most of the provisions of the USA Patriot Act are mirrored in Canadian law
- Canada has a “secret court” that allows *ex parte* applications for warrants, including sneak and peek warrants
- Canada has warrantless wiretap powers for international communications, similar to the US
- There is a huge degree of cooperation between Canadian and US authorities, both formal and informal

Based on this information differentiation related to jurisdiction and access to data between the Google cloud based service and OCAD University’s current student email service does not confirm potential government access to data as being any more or less likely.

Google, in the interest of transparency does report on government requests for information and in 2011 reported that the Canadian government demanded user data 38 times between July and December of 2010. The U.S. government made similar requests 4,601 times, a relative percentage of the population of Canada compared to the United States.

The Google Transparency report is available at:

<http://www.google.com/transparencyreport/governmentrequests/CA/>

CONCLUSION

Upon comprehensive review the OCAD University Privacy & Risk Assessment Working Group has determined the cloud based Google Apps for Education presents no appreciable additional risks to protection of personal information. In two instances, where additional risk was identified, mitigating measures, to be enacted by OCAD University, were determined to address concerns.

As stated email is not a secure form of communication so ongoing best practices and guidelines to educate the OCAD University community should be enacted through policy updates and faculty and staff training and resources. Relevant privacy legislation may not be able to be effectively applied to all student email communication since not all student email communication is directly under the control of the University. However custodianship of the service and the administration and provision of that service will still fully reside with the University, once the Google Apps for Education service is implemented. Therefore jurisdiction of the service is considered to be equivalent to the current, locally hosted Horde student email service in use by OCAD University since 2004. Security and system stability will actually be improved through implementation of the Google Apps for Education service due to much greater resources Google has to support the service. Most importantly, after completing due diligence

confirming compliance with privacy requirements and risk minimization, quality of service for student end users will be substantially improved.