Privacy Impact Assessment

Note 1: these questions are to be read in conjunction with Ryerson's ***Privacy Impact Assessment Methodology***.

Note 2: The PIA was initiated in the spring of 2011, during the early stages of defining project requirements, and was instrumental in shaping the RFP requirements, selecting the vendor, and operationalizing implementation. Though Ryerson implemented core Google Apps for Education services in October 2012 (email, calendar, drive), we have continued to evaluate other Google tools. This PIA captures the ongoing evaluation efforts to October 25, 2013.

I. Step One – Background Information

1. General:

    a. Project Title: Email and Collaboration

    b. Institution: Ryerson University

    c. Business Owner Contact Name: Brian Lesser

    d. Business Owner Contact Job Title: Director, Computing and Communication Services

    e. Business Owner Contact Business Email: blesser@ryerson.ca

    f. Business Owner Contact Business Telephone Number: ext. 6835

2. Describe your Project:

    a. *What is the project's purpose? What are its objectives or goals? Describe in detail.*
        - Implement a new email and calendaring system for everyone at Ryerson
        - Provide a common collaboration platform including document sharing for all faculty, staff, and students

    b. *How does the system work? Describe in detail.*
        - Google Apps for Education provides a comprehensive email, calendaring and collaboration platform. Ryerson user's accounts are provisioned and configured in Google by Ryerson's Resource Management System, RMS, that provides identity and resource management services.

- The services provided by Google Apps for Education include (from: www.google.com/apps/intl/en/terms/user_features.html):
    - ○ Gmail (email)
    - ○ Google Drive (includes file storage as well as the ability to edit Google Documents, Spreadsheets, Presentations and Forms in a Web browser.)
    - ○ Calendar
    - ○ Google Talk (Note: Google Talk and Google Voice have been disabled, due to privacy concerns.)
    - ○ Google Groups for Business
    - ○ Google Sites (available by request.)

- Ryerson users are able to access their email, calendar, documents, spreadsheets, and other files using a browser, using an email client, Google Drive client, or with a mobile device.
- Google Apps on Mobile devices (such as the Gmail client and Google Drive client) are governed by Google's Consumer Terms of Service.
- Ryerson faculty members and students class schedule will be inserted into their Google calendar
- User behaviour may result in users also using services provided in Google Consumer Services (e.g. services such as Scholar and Search are covered by the Consumer agreement; or users may choose to forward their accounts to other email clients, including a commercial gmail account), which is not covered by the Google Apps for Education contract with Ryerson University.
- Sharing of documents in Google Drive may be required to complete academic and administrative work consistent with Ryerson's policies and procedures.

c. *What area of the university does it serve or support?*
    - All areas of the university including faculty, staff, students, alumni, visiting scholars, contractors, and others.

d. *Who are the university area contacts for this project (if different from above)?*

e. *What is the current status of the project?*
    - The project was implemented in October 2012. At that time, approximately 111,000 accounts were created. Of those approximately 47,000 users opted in to use Gmail. The remainder had Calendar and Drive access. Approximately 28,000 users did not opt to use Gmail so were provided an RMail account (as of October 1, 2013.)
    - When Gmail was introduced, 58% of active Ryerson Rmail users chose to switch. During the summer of 2013, 82% of new users chose to use Gmail.
    - The assessment for this project predated implementation and was used to identify vendor requirements.

f. *Does the project or system collect, use, retain and/or share personal information? Describe each type of personal information the system will collect. You may wish to provide a list and description*.

- Three types of personal information are used by the system:
    - Authentication and Identification information
        - Information used by the system to facilitate authentication and identification of the end user. This includes: Ryerson email address, the user's full name, and a Google Token.
    - User-created content
        - This refers to information in the user's profile, emails, in Google Drive or in calendar entries. This information is created by the user. Information may be personal or related to administrative work, teaching, and learning. It may include data about others and may be collected directly from others using tools such as Google Forms and document sharing.
    - System-captured content
        - This refers to data collected by Google from users during the operation of the system. It may include browser and operating system information, geolocation information and data recording the users' interaction with Google.

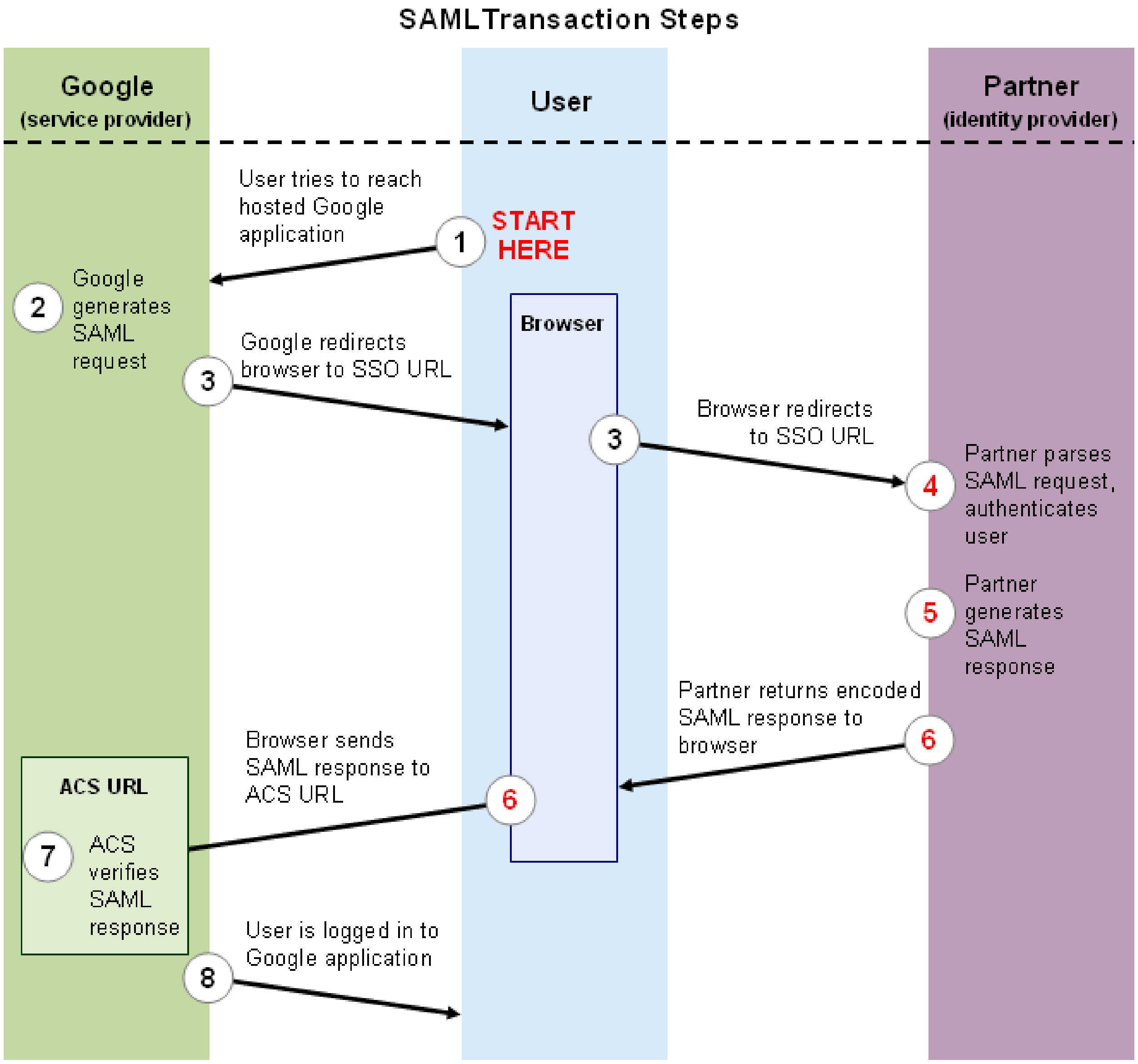
g. *Describe in detail how data moves through the system considering the entire data lifecycle (collection, use, storage/retention, sharing/disclosure, destruction). You may also wish to include a data flow diagram.*

- Identity information about people at Ryerson is collected and managed in Ryerson's Resource Management System (RMS) in order to provision and deprovision user accounts and other online resources and services.
- RMS receives student information from Student Administration System (SAS.)
- RMS receives employee (faculty and staff) information from the Ryerson HR system
- RMS provisions users in Google's Google Apps for Education service using Google's APIs
- Students and faculty can choose to opt in to using Gmail. RMS records their choice and provisions access to Gmail. If they do not opt to use Gmail RMS provisions an Email account in RMail - Ryerson's locally hosted email system. (All mail is delivered to Ryerson first before being sent on to accounts in Gmail or RMail.)
- All faculty, staff, and students are provided with an account in Google Apps for Education that provides access to Google Calendar and Google Drive.
- Staff are not normally able to opt out of using Gmail.
- Web access to Google Apps requires single sign on via SAML and Ryerson's Central Authentication Service (CAS). Single sign on is

implemented using SAML 2. The user's Ryerson password is never sent to Google. CAS provides an optional two-factor authentication system using a mobile device app or a dedicated hardware token generator.

- For devices (phones, tablets) and desktop clients that cannot authenticate against CAS (Outlook, Thunderbird), Ryerson provides users with a 'Google token' for authentication via their client. RMS creates the token and propagates it to Google. Users must enter it into their client software to authenticate.
- The diagram below illustrates the authentication flow. Google is the service provider and Ryerson serves as the identity provider, which is defined as an entity that "creates, maintains, and manages identity information for principals and provides principal authentication to other service providers within a federation."[1] After successful authentication, transactions occur between the user and the service provider. As with any third party provider, we do not have full transparency into their environment. This is why the diagram is an abstraction of what happens between us and them, but not what happens within their systems.

[1] As defined by the Organization for the Advancement of Structured Information Standards (OASIS) SAML specification.


SAMLTransaction Steps
Google
(service provider)
User
Partner
(identity provider)
User tries to reach hosted Google application
1
START HERE
2
Google generates SAML request
Browser
3
Google redirects browser to SSO URL
3
Browser redirects to SSO URL
4
Partner parses SAML request, authenticates user
5
Partner generates SAML response
Partner returns encoded SAML response to browser
6
ACS URL
Browser sends SAML response to ACS URL
6
7
ACS verifies SAML response
User is logged in to Google application
8

II. Step Two: Identification of Risk – Embedding Privacy into Design:

Privacy as the Default – Data Minimization:

(a**) Collection and Use / Processing**: *Demonstrate that the system is collecting and using the minimal amount of personal information required to achieve the project's stated purpose. Provide justification for each type of personal information why it is required and necessary to achieve the stated purpose. Consider whether it is possible to eliminate any of the listed types of personal information.*

- Authentication and Identification data - Is required by Google. Only the minimum is provided. Ryerson's implementation of single sign on insures that Google does not have passwords that are used to access other online services at Ryerson. Authentication is implemented in a federated identity model. Ryerson assumes the role of identity provider, therefore user identification, registration and authentication remains with Ryerson. Ryerson provides authentication tokens (via SAML or a Google Token). Tokens are provided strictly as a confirmation that the user is valid; Ryerson's login credentials are never shared with Google.

- User-created content - Users have the ability to create their own content and collect content from others. Ryerson policies on information security, privacy protection and access to information, and student computing guidelines, applies to these activities and to the content users place in this system according to their user role (staff, faculty, student). The risk is that users may not understand and comply with these policies, nor do we have the ready ability to audit for compliance.

- System-captured content - this is information that Google collects from users and logs during the operation of the service. Google's privacy policy (www.google.com/intl/en/policies/privacy/) outlines the type of information collected and how Google limits the use of this information for the provision of Google Apps for Education services.

(b) **Storage / Retention**: *Demonstrate that the system stores the minimal amount of personal information to achieve the stated project purpose. For example, if the system records and stores data about a conversation between users, does it need to retain all of the conversation or only the initial question and or final resolution?*

- Authentication and identification data: Google stores the email address and name
- User-created content - All user-created content is stored by Google until the user deletes it.
- System-captured content: System captured content is retained by Google.

(c) **Sharing/ Disclosure**: *Demonstrate that in any case where personal information is being shared (with other users, with the university and a third party or agency or external institution, or between university departments) that the system does so in a way that minimizes privacy risks.*

i. *Consider whether the data can be provided in aggregate form.*
ii. *Can the data be de-identified with unique individuals?*
iii. *If personal information is being shared, do you have the individuals' permission? Explain how you will obtain individuals' permission.*
iv. *Are there other circumstances, envisaged within the normal operations of this project, which justify the disclosure of personal*

information?

- ○ In all cases, personal information is only shared when the user takes an action that causes the information to be shared. In particular:
- ○ Authentication and Identification data: Authentication Data is not shared. Identification (user name) data may be shared when a user sends an email.
- ○ User-created Content: Data may be shared by the user. Ryerson requires that it have the ability to set up Google Apps for Education services for Ryerson users where privacy is the default setting; in other words, the default setting is for private or no sharing and then a user can choose with whom else they wish to share selected information.
- ○ Ryerson system administrators observe the rights of all users for privacy and freedom of information, in accordance with Ryerson policies and relevant legislation. Administrators will not instigate an investigation that requires examining the contents of mail logs, data files, or programs stored in user disk areas, unless they are investigating a case of system abuse. At such times they will notify the user, and, if relevant the student's instructor (or the Computing Coordinator of the student's program), of the actions taken, the reasons and findings.
- ○ Lawful access to data may be provided by Ryerson or Google at the request of law enforcement officials to assist in the investigation of criminal activity. Both Google and Ryerson have processes in place to carefully review, validate and respond to lawful access requests. This access may not be disclosed to the end user.

(d) Data destruction:

i. *What is the data retention period for personal information in the system?*

- Data retention is managed by the end user. They determine when data is erased.

ii. *Are there exceptions?*

- When a user's account is deleted, the deletion of the data is managed by the Ryerson system administrator

iii. *Is all data stored for the same retention period?*

- System-captured content may be retained indefinitely by Google.

iv. *Do you keep any parts of the data longer?*

- No.

v. *What is the process for data destruction – is it automatic?*

- Google uses a process known as sharding for data storage. Data is not stored contiguously, the system maintains 'pointers' which reference where the particular pieces of data are stored.

When an item is erased, the pointers to that particular item are erased removing access to that item. The storage locations containing the actual data are then available to be over written. The actual overwriting may take several days. Effectively at the time that the user deletes an item, it is then unavailable, since without the pointer it is not possible to recreate the document.

vi. *What assurances do you provide that the system will destroy data as described?*

- Audit information provided by Google should provide assurances that these processes work as described and designed.

vii. *What happens to the data if Ryerson decides to no longer use the system, or the contract ends, or the party providing the service and/or storing the data ceases to operate?*

- Ryerson will be provided with the ability to export data (emails, calendar entries, documents) and import into the system that replaces Google.

<u>**End-to-end Data Lifecycle Protection – Safeguarding Personal Information:**</u>

○ *Is the system data stored on Ryerson systems (internal) or on external systems?*

i. *If internal, is the system supported by CCS? Describe what security measures are in place to protect the data.*

ii. *If external, describe the security methods and standards used to protect the data.*

- All data is stored on servers external to Ryerson. Security standards are described as part of the contract with Google (Attachment A).
- In addition, the Google Apps Security Whitepaper describes Google's security (docs.google.com/file/d/0B5Y-fwYJF2hLOTVmMzQ1MjAtMDFmNS00YjFhLWI3MmUtZjI5MDQ5Mzc3NmMz/edit?pli=1&hl=en)

iii. *Is the security system audited? Describe.*

- Google is subject to regular SSAE 16 and ISAE 3402 Type II audits. These audits cover Logical security, Privacy, Data Center physical security, Incident Management and availability, Change management and Organization and Administration. These audits are available to Ryerson on a written request.

iv. *Is the data stored in Ontario, elsewhere in Canada, or in a foreign jurisdiction? Describe.*

- Google stores data in multiple jurisdictions, none of which is in Canada. Primary Data Centers are in the United States and the European Union.

v. *Is the data stored in a cloud-based system? If so, is the data segregated from other customer data?*

- The data is stored in a cloud-based system . Google logically isolates data on a per end user basis at the application layer and also logically isolates data on a per customer account basis . In addition, data is not stored contiguously, but is sharded, so that the actual entire item does not exist except at the time the user views it.

vi. *In the event of a security breach involving Ryerson data, what steps would you take? Describe.*

1- We notify Ryerson's Information and Privacy Coordinator as well as Ryerson's Information Systems Security Officer.
2- We initiate an incident response activity
3- We collect data about the incident such as users involved, dates and times
4- We disable the network access of the affected devices
5- We take a memory dump of the device/s involved
6- We clone the hard drive/s for further forensic investigation
7- We ask the user to re-install the devices impacted from scratch
8- We work with the users involved in validating assumptions and confirming results
9- After completing the forensic work, we issue an incident report about the entire process
10- Depending on the nature of the breach we work with the users, developers and administrators to harden the security to prevent the reoccurrence of a similar breach
11- After a fix is found, we run penetration tests to validate the security of the systems involved.

vii. *If a specific data security standard is being applied, describe the standard.*

- Google does not reference a particular security standard, however, security standards used are described in an addendum to the contract. In addition see: static.googleusercontent.com/external_content/untrusted_dlcp/
www.google.com/en/us/a/help/intl/en-GB/admins/pdf/ds_gsa_ap

ps_whitepaper_0207.pdf, a Google Security Whitepaper for Google Apps

viii. *How is the data transmitted between the individual/user and Ryerson and the external system provider or storage provider? Be specific.*

- Data transferred between the individual user and Ryerson or the individual user and Google is transmitted using the HTTPS protocol. Data transmitted between Ryerson systems and Google also uses the HTTPS protocol

ix. *What assurances are there for data integrity? Be specific.*

- Google manages data integrity at the application level. We do not have insight into their development process to understand the effectiveness of their data integrity safeguards
- The user's email address is unique and serves as the identifier that is used to link to all data, email, calendar and documents.

x. *In the event that the data storage site is compromised through unforeseen disaster, is the data backed-up elsewhere?*

- Google replicates data between data centers, so that if a data center is no longer able to function, other data centers will be able to take over. Google backs up customer data separately from their sharded storage system.

<u>Respect for User Privacy – The Self-Service Principle:</u>

○ *Describe how the system enables users to participate and control (to the extent that is legitimate and appropriate) how their personal information and data is displayed, used, shared, and destroyed.*

- Email: Users are not able to change their email address or personal information.
- Drive: Users can control how individual documents that they create are shared. By default, documents are not shared.
- Calendar: Users are able to control how their calendar information is viewed by other Ryerson faculty, staff or students. By default, Student calendars are private, faculty and staff calendars display free/busy information only.
- Google does not serve advertisements to users of the Google Apps for Education tools. This practice is in contrast to Google's commercial accounts where users are served advertisements based on an algorithm which matches advertisements to the contents of users' emails or searches. Ryerson students, faculty and staff would not receive advertisements; however, alumni would.
- Google Contacts: Employee names and email addresses are

automatically placed in Google Contacts where they can be seen by anyone with a Ryerson account. Non employees, including students contact information is not placed in Google Contacts.

- ○ *Is user participation optional in this system?*
  1. *If yes, then describe how the system responds when a user closes their account? Is all their data destroyed? How long does this process take? Are there circumstances when the system retains their data after the user has closed the account?*
     - The use of Google email for email is optional for alumni, faculty and students, but not for most staff members. If a faculty member or student opts out of Google email after using it then their email is transferred from Google to Rmail

  2. *If the user requests to end their participation with this system, describe the process for closing an account. What happens to all of the kinds of personal information stored on the system? Please describe the process for each type of personal information collected, particularly if there are differences.*
     - When an account is closed, the data associated with that account is deleted. It may take up to 5 days for the data to be permanently deleted.

- ○ *Describe what options, if any, the system provides to the user to give them control over what is shared, how they are displayed on the system, and how their personal information is used?*
  1. *If there are options, is the privacy-friendly option the default?*
     - For Student users, their calendar information is, by default set to be private, meaning that no one can see their calendar
     - For Faculty and Staff users, the default is that other employees can see their busy/free status but cannot see the details of the meeting
     - Users can change their calendar settings.
     - For Google Drive, new documents are not shared with other users by default. Users may elect to share their documents.

- ○ *Can the user access all their personal information in the system? Describe.*
  - Yes, the user can access their personal information. Some data, such as the name, can be changed, but others, such as email address cannot

- **Visibility and Transparency, Accountability:**

- *If the data-storage is external to Ryerson, please provide a copy of the storage provider's or third-party vendor's privacy policy, IT security policy, and records policy. Note, sometimes these types of policies may be combined. Are these policies publicly available? If so, please describe where they can be found.*
    - The Security and Privacy policies are part of the Google contract. In addition, Google publishes Privacy policies at: www.google.ca/policies/privacy

- *Describe how you will inform the user how their personal information interacts with the system. Please address the entire data-lifecycle; for example, do you tell them where the data is stored?*
    - CCS has created a web site, www.ryerson.ca/google for providing information about Google Apps at Ryerson. It includes information on default privacy settings and how to share information.
    - CCS has been providing introductory training on the use of the Google Apps for Education products. As part of this training, information is provided about the system and how to protect private information, such as calendar appointments
    - It is anticipated that a form of this PIA will be published and made available to the Ryerson community
    - The consultation done (please see http://email.blog.ryerson.ca) with the Ryerson community before the Google implementation also highlighted and informed users on various security and privacy implications of a cloud-based email and collaboration platform.

- *Is there a contract for the service or system?*
    - Ryerson has negotiated a contract with Google for Google Apps for Education

ii. *If you are associated with Ryerson, please review the Execution of Documents and Contracts policy, which includes a risk assessment checklist and information about appropriate signatories to contracts*.

iii. *If you are external to Ryerson, please note that Ryerson is subject to Ontario's Freedom of Information and Protection of Privacy Act ("FIPPA"), which contains requirements about protecting personal information, providing notice about the collection, use, and disclosure of personal information, and also provides a framework for enabling access to information. You may want to seek your own legal advice on what this means for your organization and the data stored on the system or associated with this project.*

III. Step Three – Evaluation of Risk and Identification of Solutions to Reduce Risk

The following is to be filled out by the Privacy, Information Security, and Records Management Office

Identified Risks and Corresponding Recommendations:
Ryerson decided in January, 2012 to use Google Apps for Education suite of services (“Google”), based on a recommendation from the Advisory Committee on Academic Computing to the Provost and Vice President Administration and Finance. The recommendation followed a one-year community consultation and procurement process.

Our decision presented a number of challenges to compliance with FIPPA. Ryerson had decided to outsource the processing and storing of Ryerson data to a third-party that existed in a multi-jurisdictional environment, in which there are differing privacy and security requirements as well as lawful-access regimes. The Ryerson data may contain personal information, for which Ryerson is responsible for protecting and securing. Ryerson cannot outsource its privacy-protection requirements; it remains accountable for the privacy and security of Ryerson data.

We proceeded to document the compliance challenges or “risks”, as well as Ryerson’s response to each risk. The identification of risks below is separated into sections based on: 1) those risks we identified prior to Ryerson’s implementation of Google or “pre-implementation”; 2) those risks we identified after implementation or “post-implementation”; and, 3) those risks that continue to be present or “residual risks”.

We identified two broad categories of personal information captured by Google: 1) information required to authenticate a Ryerson user, and 2) information a Ryerson user inputs into a Google App such as Gmail, Google Drive or Google calendar.

Pre-Implementation Identified Risks and Corresponding Recommendations:

1. **Institutional Accountability for Personal Information Stored in the Cloud:** We recognized that Ryerson Google Apps for Education users will be able to create, process, store, and share data using Google Apps for Education tools. We expect that some of this data could contain personally-identifiable information; for example, student records, employee records, financial

transactions, health-related records, and institutional planning research. As well, we recognized that faculty and researchers at Ryerson may use these Google Apps for Education tools to collect, store, disclose and communicate about their research and that some of this research could contain personal information belonging to the research data subjects. Ryerson researchers (faculty, post-docs, researchers, and students) needed a communication and information storage solution that would enable them to communicate and collaborate with other researchers both in and outside of Ryerson, and to store sensitive data, in a secure manner that would enable compliance with Research Ethics Board's requirements and Tri-Council policies and procedures.

a. **Risks:** Ryerson needed to document a process that would determine if the Google Apps for Education tools support Ryerson's privacy protection and security requirements. Ryerson is accountable for providing students, faculty and staff with tools that will enable them to operate in ways that support Ryerson's mission and its academic plan but also complies with privacy legislation and university policies.
b. **Recommendations and Outcomes:**
    i. Ryerson undertook a privacy impact assessment in the early stages of the project to identify risks and make these part of the documented requirements for the project. We used the international standard of Privacy by Design ("PbD"), to develop an assessment methodology* for the purpose of enabling Ryerson to make an informed decision about the risks.
    ii. Ryerson negotiated a legal agreement with Google to outline each party's duties or obligations, rights, and discretionary authority. The agreement facilitates Ryerson's compliance with FIPPA.
    iii. Ryerson developed communication, consultation and outreach mechanisms to enable Ryerson employees to make informed decisions about the appropriate use of Google Apps for Education cloud-based tools for university business, teaching and research.
    iv. Ryerson's Computing and Communication Services ("CCS") undertook to analyze, test, and where necessary modify, the Google Apps settings to make privacy the default setting, in order to exercise due diligence and to facilitate compliance with FIPPA. CCS decided to enable only those Google Apps for Education tools where users' privacy could be made a default setting. Please see Appendix A for the complete list of setting CCS used configure Google Apps with privacy as the default.
    v. Google will provide Ryerson with logs of user authentication activities upon Ryerson's request. Ryerson uses this information to audit for compliance with Ryerson policies and CCS procedures, including that appropropriate information security safeguards are in place and effective.

2. **Jurisdiction and Lawful Access:** During consultation with Ryerson students, faculty and staff, we frequently heard concerns related to risks of governments, particularly foreign governments, accessing Ryerson data via lawful-access treaties, such as the U.S.A. Patriot Act, or warrantless searches without users' or Ryerson's knowledge. There were concerns that moving to a cloud-based service represented a greater risk of the data being subject to these types of government searches.
    a. **Risk:** Lawful-access treaties are agreements between the Canadian government and other foreign governments which provide foreign governments with access Ryerson users' data, often without notice. Warrantless searches provide entities (such as law enforcement or government bodies) with the authority to search Ryerson records without first obtaining a court-reviewed warrant. In both cases, because no notice is provided, Ryerson and Ryerson users are left without the ability to challenge the purpose, validity or authority of the access requests.
    b. **Recommendations**:
        i. After Ryerson decided to "Go Google", but prior to implementation, we recommended Ryerson investigate Google's security safeguards and standards to determine if Google's data security standards and practices met or exceeded what Ryerson could offer through data storage on Ryerson's own servers and through Ryerson's in-house mail service ("Ryerson mail" or "R-mail").
        ii. We recommended that we continue to monitor this risk represented by lawful-access treaties and warrantless searches. Our understanding of this risk and the associated threat landscape may change as additional information becomes available; for example, the public perception of this risk was heightened following former National Security Agency ("NSA") subcontractor Edward Snowden's disclosures of top-secret documents revealing multiple governments', including Canada's, surveillance activities of their respective citizens and how these governments shared information with other governments.
        iii. We sought legal and subject matter expert advice on the impact of lawful-access treaties and warrantless searches or access. We determined that the risk remained unchanged regardless of whether the data was stored at Ryerson, or externally in the cloud but within the same jurisdiction, or externally in the cloud in a foreign jurisdiction. We acknowledged that storage risks were not the same for all foreign jurisdictions. We recommended that we seek to limit data storage to those foreign jurisdictions that demonstrated similar legal or regulatory frameworks for data protection.
        iv. We also recommended that Ryerson undertake to educate users about the nature of this risk as a key aspect of ensuring users make informed decisions based on their role at Ryerson and the

sensitivity of the data they created, stored, and or processed.

c. **Outcomes**:
   i. Opt In to Google Apps for Edu: In alignment with the PbD principle of “respect for user privacy”, Ryerson enabled students and faculty to choose the email provider (Rmail or Gmail) so that users had control over where their email accounts would be stored. By default, staff were migrated to the Google Apps for Education platform, but allowances were made for individual staff cases to stay with the in-house systems where the staff held more than one role (staff and faculty or staff and student, or in the case of a department that worked with sensitive data and the department decided to stay with the current in-house system.
   ii. Monitoring Risk: Ryerson continues to monitor risks, associated with lawful access treaties and warrantless searches.
   iii. Legal Agreement: As part of the negotiations with Google about the agreement for services, we ensured Ryerson had the ability to review Google security audits. Ryerson was not able to specify or limit the locations of where our data would be stored.
   iv. Education and Outreach: Education and Outreach: Users were educated about how email systems work, such as routing pathways and networks (for example an email sent from Toronto to a recipient in Toronto may cross into a foreign jurisdiction in transit to the recipient); risks about which they have little to no control, such as the email recipient’s data storage practices (retention, disclosure); and risks about which they can exercise control, such as the content of the message, message recipients, and the user’s own data management practices. These risks are present regardless of whether Rmail or Gmail are used.
   v. Security Assessment: Our assessment prior to implementation was based on information we researched about Google’s data-security practices and what we could ascertain based on in-house testing of the services. We were satisfied that Google was able to provide data-security that, at the minimum, met or exceeded what we were able to provide internally at Ryerson.

3. **Authentication:** Google requires certain information for the purposes of provisioning a Ryerson user with a Google Apps for Education account and to authenticate the identity of a given Ryerson user.
   i. Risk: Google requires the collection of personal information as well as passwords in order to verify users’ identity and provide access to users’ accounts. We received feedback from the Ryerson community that they were concerned about Google having this information about them.
   ii. **Recommendation:** We recommended that Ryerson minimize the

amount of information we are required to share with Google for the purposes of user authentication.

iii. **Outcome:** CCS planned to provide access to Google Apps for Education through the already existing Ryerson Central Authentication System ("CAS") (see PIA Step 3, part 1, section 2.g), an internal service available only to Ryerson students, faculty and staff. Users are authenticated through CAS, and Ryerson therefore only need to confirm authentication with Google. Accordingly, Google only required user's proper name and their user-name, not their password, to connect them with the Google Apps for Education services as provisioned by Ryerson. The exception was for desktop clients and mobile access where a user name and password are required. To facilitate mobile access Ryerson generate a Google Token to use instead of a user's Ryerson password.

4. **Email:** Prior to implementation, Ryerson provided choice to faculty and students about whether they wanted to migrate to Gmail or remain with Rmail.
   a. **Risk:** Aside from previously discussed risks associated with lawful-access treaties and data security, there are also privacy risks associated with user behaviour; in other words, how users utilize the email tool directly correlates with changes in privacy risks. For example, users control the content of their email messages, what attachments, if any, are included and whether the attachments have additional security protection (password, encryption), what links are embedded, and the list of email recipients. They also likely control the security settings of the devices upon which they are sending email.
   b. **Recommendations:**
      i. Education and Outreach is a key to enable users to make informed decisions about the most appropriate tool to use to create, use, process, disclose, and store personal information. Remind users of their responsibilities when they become aware of a suspected or actual privacy incident.
      ii. System Design: CCS tested the Gmail tool as offered within Google Apps for Education to see if we could alter the settings to build in additional privacy protections.
   c. **Outcomes**:
      i. Education and Outreach: We committed to developing a new outreach program designed to help faculty and staff make informed decisions about the wide-array of tools available to them. We plan to develop an online companion to this outreach program. CCS developed online resources to help users navigate the tools and use them appropriately. CCS also offered training sessions to users.
      ii. System Design: CCS altered the default settings to "private" for the

Gmail tool.

5. **Contacts:** Prior to implementation, Ryerson committed to following the current practice of not making student email addresses publicly available or searchable, or added by default to institutional email contact lists.
    a. **Risk**: We needed to ascertain if Google Apps for Education could be modified to fit our current practices regarding student contact lists. We treat student email addresses as confidential and personal information as it reflects their current educational history. This is an element of personal information as defined by FIPPA section 2 and therefore requires protection in accordance with Part III of the Act.
    b. **Recommendations and Outcomes**: CCS tested how contact lists are built and shared within Google Apps for Edu. CCS altered the default settings to make only faculty and staff email addresses part of the default contact lists for Ryerson users.

6. **Calendar:** Prior to implementation, Ryerson intended all students, faculty and staff, regardless of which email or storage solution they chose, would be provided with access to Google Calendar.
    a. **Risk:** Google Apps for Education facilitates the publication of users' calendar details, which may not always be intended or appropriate under the circumstances. WIthin the calendar, users could post personal information about themselves or about the individual(s) with whom the user planned to meet, disclosure of which could expose users to risks of harm (reputational, health or safety, etc.), or expose other types of information that Ryerson would otherwise endeavour to protect as described in our Information Protection and Access Policy and supported by FIPPA.
    b. **Recommendation:** We recommended that prior to implementation CCS explore configuring the default settings for this tool to protect users' privacy.
    c. **Outcome:** CCS designed the default settings for all users to private, which meant only the account holder or "user" could see the details. By default, faculty and staff calendars could be found by other employees, and these calendars showed only busy or available periods, not details. By default, student calendars are not available to faculty, staff or other students. All users have the ability to invite specific people to view a meeting or to see additional details in their calendar. A user is reminded that he/she has invited people to see events before the event is posted in a user's calendar.Following implementation, CCS took the additional step following implementation to review if and how users had modified the default settings for the calendar. All those users who had changed their settings to share their entire calendar publicly were notified and reminded

how to control the settings.

7. **Google Drive:** Prior to implementation, Ryerson planned to provide access to Google Drive to students, faculty and staff as a means to supplement or replace storage available through Ryerson's Windows-based Central File and Print Services (CFAPS.) This tool included the provision of Google Docs, Sheets and Slides, which are comparable with MS Office Word, Excel and Powerpoint software.
    i. **Risk:** The default setting for the Google Drive tool was to share records publicly. Due to the nature of administrative and academic work, Ryerson needed a collaboration and storage tool that was secure and enabled records to be protected from unauthorized disclosures.
    ii. **Recommendation**: Prior to implementation, we recommended that CCS reconfigure the default “share” setting to “private”. This meant that by default any records created or saved in Google Drive would only be available to the user. Users would have to authorize additional email address account holders in order to share this data or to collaborate on a record.
    iii. **Outcome:** CCS was able to set the default setting to “private”. Following implementation, we realized additional outreach to faculty and staff was required to facilitate the safe use of Google Drive. The ISSO and Privacy Officer began offering to all faculty and staff a privacy and security awareness program on a monthly basis in March, 2013; in addition they have met with every academic department in TRSM and continue to work on strategies to make this outreach effective.

b. **Other Google Apps for Education services**: There are additional services available within the Google Apps for Education bundle of services besides Gmail, Drive and Calendar; specifically Google Talk and Google Groups for Business. These services enable additional means of collaboration. Google Talk is an instant messaging service that provides both text and voice communication. Users of this service can see when other users are active online within the Google Apps for Education services. Google Groups for Business supports discussion groups; users participate in threaded conversations and can review archived postings.
    i. **Risk:** Ryerson is committed to protecting the privacy of its students, which includes disclosing that they are a current student to unauthorized individuals without the students’ permission. Ryerson does not publish a list of current student names or email addresses. Ryerson is concerned it may not be able to support this committment by enabling these services. Furthermore Ryerson is concerned about possible safety risks associated with making it known when users are on- and off-line.

ii. **Recommendation:** We recommend that Ryerson analyze each additional Google Apps for Education application to determine if its privacy settings can be altered to meet our internal requirements for privacy as the default setting. We recommend that the analysis be documented and shared with the Privacy Officer and Information Systems Security Officer before the application is turned on. We recommend this approach be followed as Google adds new services to the Google Apps for Education platform.

iii. **Outcome**: CCS evaluated Google Talk prior to implementation. At that time Ryerson could not configure Google Talk with privacy as the default setting or to allow users to control when other users could see their online or offline status. For these reasons, CCS did not enable Google Talk. CCS also committed on a go-forward basis to apply the same approach to other Google Apps for Education services at such a time when Google makes them available.

8. **Post-Implementation Identified Risks and Corresponding Recommendations:**

a. **Information Security Assessment**: Simply put, information security enables privacy protection. We require strong information security practices to be in place, both by Google as the data processor and data storage facility, and by Ryerson. In practical terms, we understand that accountability for information security is shared between

i. **Risk**: By moving to an externally-hosted solution for email, calendaring and collaboration tools, Ryerson is expecting Google to provide strong and sufficient security for the data it is processing and storing. Ryerson remains accountable for the protection of personal information, even if it has outsourced the data processing and data storage to a third party.

ii. **Recommendation:** We recommend that Ryerson assess Google's information security practices and that, as per our agreement with Google, we request Google's security audit on a regular basis.

iii. **Outcome:** The Information Systems Security Officer is collaborating with CCS on an information security threat and risk assessment. Ryerson has requested and received the audit. It has been reviewed by the Director, CCS and the Information Systems Security Officer. To date, Ryerson is satisfied that the Google is able to provide sufficient informaiton security; however, we note that at this time Ryerson has not completed the assessment. Should Ryerson find serious security concerns which impact our ability to protect personal information, we will reopen the PIA to address that matter at that time.

b. **Google Consumer Services:** Google Apps for Education users will have access to Google services that fall outside of the Google Apps for Education agreement, otherwise known as Google Consumer Services, via their Ryerson Google accounts. For example, Google Search and Google Scholar applications are accessible to Ryerson users logged in to their Ryerson Google Apps for Education suite of applications. Users can move seamlessly between the two suites of services (Consumer and Edu).

   i. **Risk:** Ryerson committed to students faculty and staff that it would assess the privacy and security implications of tools before it made them accessible under the Google Apps for Education suite of services. As delineated above, we have not made accessible tools that do not meet our privacy and security expectations. With Google Search and Scholar we cannot control the default settings for these tools nor does our agreement with Google apply to these services. We cannot assess the security for these applications. We also cannot control or prevent our users from linking to these services while logged in to their Ryerson Google accounts.

   ii. **Recommendations:**

      1. We recommend Ryerson obtain clarity from Google on what services fall under which agreement and whether our users have agreed to Google's terms of service for Consumer Services.
      2. We recommend Ryerson consults with Google to determine if there is a way that we or Google can flag for users when they are moving from one set of services to another.
      3. We recommend that CCS, in partnership with the Information and Privacy Officer and the Information Systems Security Officer, develop guidance to inform users how to utilize the services in a privacy-friendly manner, to understand the implications of their choices if they select non-default settings, and to understand the implications of using Consumer services via their Ryerson account.

   iii. **Outcome:** in progress.

* Ryerson's PIA Methodology is provided as an Appendix the PIA Step 3.

By undertaking the privacy impact assessment and in accepting these recommendations, the project owner is embedding the seven principles of ***Privacy by Design***, an internationally-recognized standard for privacy protection, into this project.

Ryerson Data/Project Decision Maker Name:

Signature:

Date:

References

Google Security Information

Google's Approach to IT Security (A white paper.)
https://cloud.google.com/files/Google-CommonSecurity-WhitePaper-v1.4.pdf

Google Apps' Security and Privacy Overview:
https://support.google.com/a/answer/60762?hl=en

Google Apps' Security:
http://www.google.com/enterprise/apps/business/benefits.html?section=security

Google Data Centre Locations:
http://www.google.com/about/datacenters/inside/locations/index.html

Lawful Access References:

- David Drummond, Google's Chief Legal Officer statement regarding Prism accusations: https://plus.google.com/+google/posts/TMh6gUVrwMq
- Larry Page, CEO fo Google's statement on Prism: http://googleblog.blogspot.ca/2013/06/what.html
- "In order to compel us to produce content in Gmail we require an ECPA search warrant," said Chris Gaither, Google spokesperson. http://arstechnica.com/tech-policy/2013/01/google-stands-up-for-gmail-users-requires-cops-to-get-a-warrant/
- Google's Transparency Report re Legal Process https://www.google.com/transparencyreport/userdatarequests/legalprocess/#what_does_google_do

Google's agreement with the FTC:
http://www.ftc.gov/os/caselist/1023136/110330googlebuzzagreeorder.pdf

Other References:

- David Fraser's presentation here: https://ryecast.ryerson.ca/25/watch/1050.aspx (Use the slider to go to the 01:43:00 mark.) His slides are here: http://blog.privacylawyer.ca/2011/02/ryerson-university-looks-to-cloud.html Information about David Fraser is here: http://www.privacylawyer.ca/contact.html

- Commissioner Cavoukian Says the Patriot Act Is “Nothing” by Dan Michaluk, Hicks Morley: http://www.slaw.ca/2011/02/26/commissioner-cavoukian-says-the-patriot-act-is-nothing/
- Office of the Information and Privacy Commissioner of Ontario: http://www.ipc.on.ca/english/Home-Page/
- Assistant Privacy Commissioner of Canada on the U.S.A. Patriot Act: http://www.michaelgeist.ca/content/view/3308/125/
- Recent Canadian court cases on government surveillence of your data: Kirk Makin, “How far should we let the law follow digital footprings?”, Globe and Mail, Nov. 18, 2011, http://bit.ly/tEpmnN
- U.S. rethinking warrantless searches? Julia Angwin, “Judge Declares Law Governing Warrantless Cellphone Tracking Unconstitutional”, Wall Street Journal, Nov. 16, 2011, http://on.wsj.com/rYWDKV

Additional Update