Privacy in the Cloud

Innovative Solutions to Address Canadian Privacy Issues with Cloud-Based Learning Technologies

ALWAYS LEARNING

PEARSON

TABLE OF CONTENTS

Executive Summary

Cloud-based educational technology solutions offer powerful learning and other benefits to students, instructors, and administrators. Because cloud-based solutions may originate or be hosted anywhere in the world, their use poses challenges for educational jurisdictions in Canada where privacy laws and policies dictate strict information security protocols.

Educational organizations have responded in a number of ways to the challenge of protecting students' private information. From limiting access to Canadian technologies, requiring students to "opt-in," or not complying with regulations, none of these options offer a complete and lasting solution to the challenge.

A consensus is emerging among privacy experts that technology solutions themselves must, by design, protect private information and keep it secure from accidental disclosure. Privacy by design places the onus for protecting private information on technology developers and decision-makers rather than on students and instructors. Pearson's privacy solution is embracing that responsibility. This paper considers the challenge of protecting private information in a cloud-based world and describes the privacy server solution Pearson has developed.

The Challenge

Growth and benefits of SaaS (Software as a Service) learning technologies in education

Educational institutions are expanding their use of online learning technology. This evolution delivers clear benefits for students, instructors, parents, and administrators. Digitally-accessed curriculum resources engage students in dynamic learning experiences and may be used in class or for outside assignments. Digital grade books automate many time-consuming tasks of course administration, freeing instructors to spend more time interacting with students. Online assessment tools provide individualized skills inventories and self-study plans that personalize the learning experience for each student. And online learning resources offer anytime, anywhere, access to education. Technology in the education context means increased personalization of learning, flexibility, efficiency, access, accountability, and affordability.

Increasingly, today's educational technology solutions are web-based. The Internet has become the dominant delivery system for applications and services. Given the increasing ease of accessing the Internet from anywhere at any time, from fixed and mobile computers and devices, web-based education tools and resources will continue to grow in use.

The ubiquity of the Internet has enabled the delivery of a growing number of technology solutions from "the cloud." The cloud, in this context, refers to web-based technology solutions that are hosted and managed by the solution providers as a service (hence the term Software as a Service), rather than being deployed locally by individual institutions. Today, the best provider of an educational technology service could be located anywhere in the world. Software providers' data centres might be serving Canadian students and teachers from data centres in Canada, the United States, the European Union, or beyond. Canadian educational institutions want to access the best possible solutions regardless of their origin.

There are many benefits to this cloud-based approach. There is an economic benefit: it is cheaper to maintain a few centralized data centres that serve millions of users than it is to deploy hundreds of installations that serve smaller groups of users. The cloud-based approach reduces start-up costs for individual institutions because they don't have to invest in the necessary hardware and software to implement an educational technology program. Another significant benefit is scale and performance: one robust data centre, with best-in-class security measures, hardware and software redundancy, and disaster recovery measures can outperform dozens of smaller centres. Given the clear economic and performance advantages, more and more of today's education technology solutions are cloud-based.

Maintaining the security of the information stored within technology solutions is a priority. Protecting sensitive personal information is paramount. Just as medical information is considered private and must be safeguarded, education data contains sensitive elements that require effective security protocols. Because electronic information may be transported across global telecommunication networks, and because protecting electronic data can be extremely complex, the privacy and security concerns around electronic information are especially acute.

Protecting electronic data has become a topic of public policy. Some Canadian provinces have enacted laws to address how private electronic information collected by public Canadian institutions should be handled. These laws require that private data not cross provincial or Canadian borders, or be accessed by citizens or authorities of other countries. Pearson's solution protects personal data from being subjected to privacy laws in other jurisdictions–including the United States–that do not protect personal privacy as stringently as Canadian legal standards.

One aspect of these laws is that **private data** should not cross provincial or Canadian borders, or be accessed by citizens or **authorities of other countries**.

Global Access Balanced with Local Control: The Challenge

Pearson is addressing the challenge of achieving access to best-of-breed educational technology resources while ensuring the security of personal information. Introducing location dependencies into data management creates a fundamental conflict with the overall trend toward cloud-based educational technology solutions in Canadian educational institutions. How can we realize the learning and economic benefits, and freedom of choice associated with educational technology solutions while scrupulously protecting private data?

Pearson, whose cloud-based technology solutions are hosted in Canada, the United States, and around the world, endeavours to deliver technology solutions in a way that complies with local provincial privacy laws, while giving Canadian educational institutions the opportunity to choose the finest educational technology solutions for their student populations.

Who Manages Privacy within an Institution or Province?

It is important to examine the human context in which educational technologies are selected and deployed. For example, in Ontario, with the approval of the Council of Directors of Education, the Privacy and Information Management (PIM) Taskforce (www.pimedu.org) supports the development of an information management culture to respect privacy in the province. One goal: to find the balance between operational efficiency, providing educational services, and protecting privacy. All school districts have designated a Senior Administrative PIM Champion responsible for overseeing local school district implementation. Each district has also identified a cross-organizational local implementation team and developed an approach to the role based on local privacy and information management culture and needs.

The role of the PIM Champion is to

- Champion privacy and information management issues within their school district
- Understand MFIPPA and the Education Act
- Represent the district in partnership discussions relevant to privacy and information management
- Bring to bear insights into privacy and information management on the development and delivery of the district's services and policies
- Create a cross-organizational team to advocate privacy concerns and ensure that the district's privacy policies are embedded in daily practice

What exactly is personally identifiable information?

ALTHOUGH VARIATIONS IN THE DEFINITIONS of personal information exist among privacy laws, personal information generally includes any information unique to an individual, such as their home address, opinions, educational records, age, gender, income, medical records, and financial data.

Some personal information is deemed to be in the custody of a public body, like educational records in the custody of a school or medical records in the custody of a hospital.

Anonymous data, i.e., data not identified or linked to an individual by name, is not personally identifying information. Personal information does not usually include employee contact information.

Canadian privacy laws

FEDERAL LAWS

Canada has two federal privacy laws: the Privacy Act and the Personal Information Protection and Electronic Documents Act (PIPEDA).

The Privacy Act imposes obligations on federal government departments and agencies to respect privacy rights by limiting the collection, use, and disclosure of personal information. Individuals are also protected by the Personal Information Protection and Electronic Documents Act that sets out rules for how private sector organizations may collect, use, or disclose personal information in the course of commercial activities. The law gives individuals the right to access and request correction of the personal information these organizations may have collected about them. It obliges organizations to protect and limit access to personal information and provide a ready means for individuals to review, alter, or remove their personal information.

Oversight of both federal Acts rests with the Privacy Commissioner of Canada who is authorized to receive and investigate complaints.

PROVINCIAL LAWS

Each Canadian province has laws to protect and govern the gathering, storage, and use of personal information. Of particular relevance to educational institutions are British Columbia's privacy laws, as well as those of Nova Scotia, because these two provinces have enacted some of the strictest guidelines in the country. This legislation is in part a response to the USA Patriot Act.

British Columbia's two principal laws are the: Freedom of Information and Protection of Privacy Act (FIPPA) and Personal Information Protection Act (PIPA). FIPPA allows access to information held by public bodies (such as ministries, universities, and hospitals) and determines how public bodies may collect, use and disclose personal information. PIPA sets out how private organizations (including businesses, charities, associations, and labour organizations) may collect, use, and disclose personal information.

Under FIPPA, personal information that is in the custody of a public institution, e.g., schools, colleges, and universities, must reside on a server in Canada, unless consent is obtained from the individuals for it to reside elsewhere.

The relevant legislation in Nova Scotia is the Freedom of Information and Protection of Privacy Act, which applies to provincial and local public bodies, including community colleges, schools, and universities, and the Personal Information International Disclosure Act, which prohibits access to or storage of personal information outside Canada if the personal information is in the custody or under the control of a public body, without explicit consent of the individuals or under particular circumstances, such as meeting requirements of the public body's operation.

USA PATRIOT ACT

The USA Patriot Act, an Act of the United States Congress signed into law in 2001, reduces restrictions on law enforcement agencies' ability to search telephone and email communications, medical, financial, and other records; eases restrictions on foreign intelligence-gathering within the United States; expands the regulation of financial transactions, particularly those of foreign individuals and entities; and broadens the discretion of law enforcement and immigration authorities in detaining and deporting immigrants suspected of terrorism-related acts. The Act, particularly its provisions for enhanced surveillance of electronic records of foreigners, raised concerns among some Canadians about the privacy of personal information that might be hosted on U.S. servers. Some jurisdictions in Canada have responded by forbidding the storage of its citizens' personal information on U.S. servers in certain circumstances.

Privacy interests of students

Student marks and grades, or comments about students, are personal information particularly relevant to students of public institutions. This data is deemed to be in the custody or under the control of a public body and is therefore subject to the restrictions on hosting stipulated in the relevant provincial legislation.

Other personal information, such as name and address, is subject to privacy protection but is not subject to the restrictions on hosting that apply to personal information belonging to a public institution.

Current Methods of Addressing the Privacy Challenge

A number of strategies have been employed to give students access to educational technologies while protecting private information. A survey of these strategies reveals that all present disadvantages: some are too costly, some will not scale, some restrict choice of technologies, and some simply don't offer necessary security of private information.

Local Hosting: Cost-Prohibitive

Educators often ask why Pearson and other providers don't simply establish locally hosted instances of their applications in Canada. Pearson has thoroughly investigated the costs involved and found that hosting our complex and built-to-scale learning applications locally would significantly increase the prices we would have to charge to cover the cost of the additional data centres.

With quality digital resources produced on every continent, and given the importance of selecting the best resources for teaching and learning at the best price, it is not always possible to have all applications operating from servers in Canada. While it might seem logical to simply move all applications to Canadian hosting sites or school jurisdictions, this option is cost-prohibitive and unsustainable.

Canadian Applications

With Canada's growing knowledge-based society, are there Canadian-only digital solutions ready and waiting for Canadian K–12 educators? The answer: yes and no. Yes, digital resources are being developed by Canadian-based educational resource companies like Pearson, by start-up companies, and by technology companies. Many of these resources are exceptional tools for teaching and learning. But that does not preclude educators, parents, and students from wanting and needing exceptional digital resources from other countries, including the United States.

Non-Compliance

Canadian educational jurisdictions naturally wish to access best-of-breed technological resources at affordable prices. In many cases, the best solutions are not made in Canada. Yet decision makers are obligated to adhere to privacy regulations and protect students' personal data. These competing requirements have forced Canadian educational jurisdictions to choose between protecting private information and accessing preferred educational technologies. Sometimes, the decision is not to comply with all of the privacy regulations. An analogy might shed additional light. If a K–12 school district is in need of busing services it logically turns

> "We at Pearson believe that we offer some of the best, **most competitive** online **resources in the world** and we want to guarantee that Canadian students and teachers are able to **access these solutions** no matter where the resources are physically hosted."
>
> *—Kendrick McLish, Pearson Vice President, Integration Strategies*

to local bus providers. The district might discover that some of these businesses are subsidiaries of American-owned bus companies. Still, if local Canadian-owned bus providers lack the capacity needed, the district might choose the subsidiaries of American-owned companies to meet the transportation demand. In doing so, school officials choose not to comply with the privacy law because students' personal data such as their name and home address could potentially cross the border to servers for the American-based busing company. School jurisdictions take their responsibility to protect students' personal data very seriously, so school officials would inform parents of the choice not to comply.

Similar situations arise when selecting digital resources for learning. For example, a classroom teacher may decide to ask students to compose an autobiographical project using a service like Google Docs. Students could conceivably include personal information as they create these autobiographical projects but the teacher may not be aware of where that personal data is being stored. And yet, to forswear all digital learning resources to avoid the possibility of non-compliance would deprive students of relevant and valuable educational experiences. Thus, educators are faced with difficult choices.

Opting-In: A Partial Solution Limited to the Higher Education Context

In higher education most students are of the age of majority and students can agree to allow their personal data to leave Canada. With a K–12 student population, it is at best cumbersome to establish protocols for parents "signing off" on their children's personal data being potentially stored on servers in American data centres. For those parents who refuse to sign off, there is often no suitable alternative to the rejected technology solution.

Toward a New Standard on Privacy

It is critical that Canadian students be able to access the world when it comes to exceptional tools for learning. This requires imaginative and judicious approaches to safeguarding students' personal data. In Pearson's opinion, the protection of students' personal data should be standard practice. It should not be the responsibility of the teacher or the student to investigate where the server is located or to turn a blind eye when using digital resources. Students and teachers should not be found at fault for transferring students' personal data outside Canadian borders. Rather, the protection capability should be built in to the digital resource itself, removing the responsibility from end users and rendering privacy breaches nearly impossible.

Views of Canadian organizations on cross-border storage

Gartner Research's recent publication on the Canadian perspective of privacy by Ouellet, Casper, and Young (November 2010) provides results of a recent survey of organizations. While this survey is not restricted to educational organizations and includes organizations in both the public and private sectors, it is likely that school districts hold similar views.

Key findings of the survey include that privacy is a priority for 100 percent of respondents; awareness of and compliance with privacy regulations is high; a majority of organizations have a dedicated individual for privacy, though a much smaller number have a separate budget for privacy.

According to the report, "fifty-seven percent of Canadian organizations indicate that they store and treat personal data nearly exclusively in Canada, so cross-border issues can be avoided."

A key recommendation of the report is for organizations to "look beyond the obvious technology choices for privacy (such as encryption and website scanning), and consider privacy management tools, data masking, data loss prevention, and metadata redaction to protect personal information."

Privacy by Design

Developed by Ontario Information and Privacy Commissioner Dr. Ann Cavoukian, Privacy by Design advances the view that privacy cannot be assured solely by compliance with legislation and regulatory frameworks, but that privacy assurance must become an organization's default mode of operation.

Dr. Cavoukian is recognized as one of the leading privacy experts in the world. Noted for her seminal work on Privacy Enhancing Technologies (PETs) in 1995, her concept of Privacy by Design seeks to proactively embed privacy into the design specifications of information technology and business practices, thereby achieving the strongest protection possible. In October 2010, regulators from around the world gathered at the annual assembly of International Data Protection and Privacy Commissioners in Jerusalem, Israel, and unanimously passed a landmark resolution recognizing Privacy by Design as an essential component of fundamental privacy protection. This was followed by the United States Federal Trade Commission's inclusion of Privacy by Design as one of its three recommended practices for protecting online privacy—a major validation of its significance.

Innovative New Way to Safeguard Private Information Developed by Pearson

The new approach developed by Pearson honours our commitment to Canadian privacy laws by storing private data within Canada while allowing Canadian students to access our cloud-based applications hosted outside of Canada. Pearson is installing a specialized server and database in Canada. This server (see Fig. 1), which we are calling our privacy server, will act as intermediary between our Canadian students and our cloud-based applications hosted outside Canada.

During the registration process (see Fig. 2), Canadian students will not connect directly with our cloud-based applications. Instead, the registration process will occur between the student and the privacy server. Any private information requested from the students during this process will be captured and stored locally on the privacy server based in Canada.

At the end of the registration process, the privacy server will enroll the students in the appropriate application. During this phase, the privacy server will encode and lock the private information by transforming individual pieces of information into tokens. Only the tokens

FIGURE 1
PRIVACY SERVER OVERVIEW

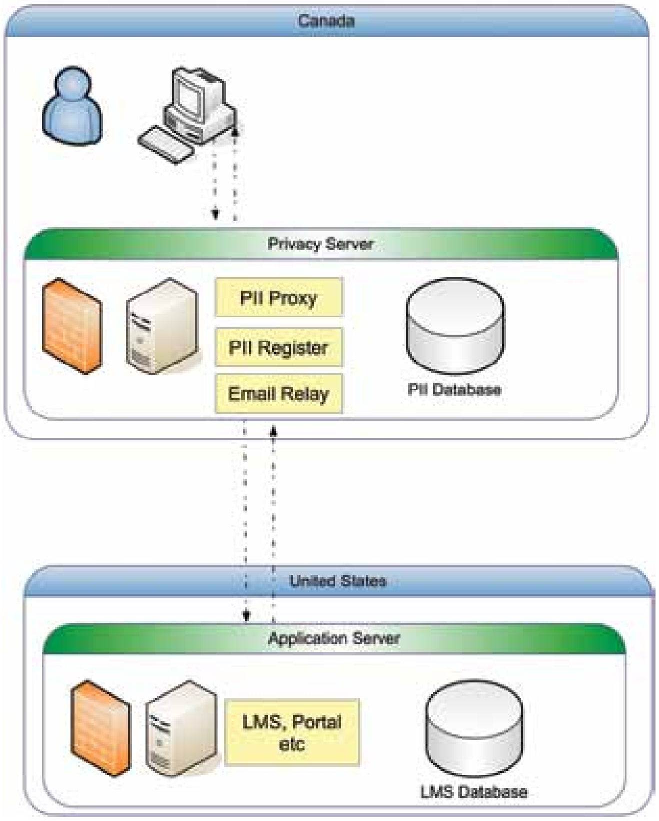
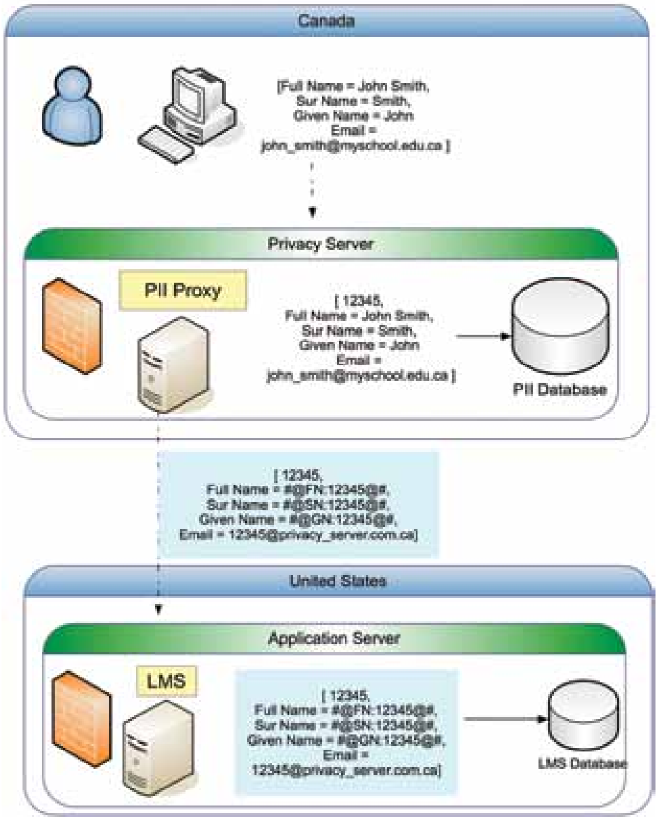


FIGURE 2
PRIVACY SERVER REGISTER



will be passed from the server in Canada to the cloud-based applications outside Canada. No actual private student information will leave the server in Canada.

The other major function of the privacy server is to serve as an intermediary proxy (see Fig. 3) between students and the cloud-based applications. Canadian students will never make requests to, or receive responses directly from the applications. Instead, all this web traffic will pass through the privacy server. This configuration mirrors the system currently used by many schools whereby proxy servers filter web traffic. In the case of the privacy server, Pearson filters private information.

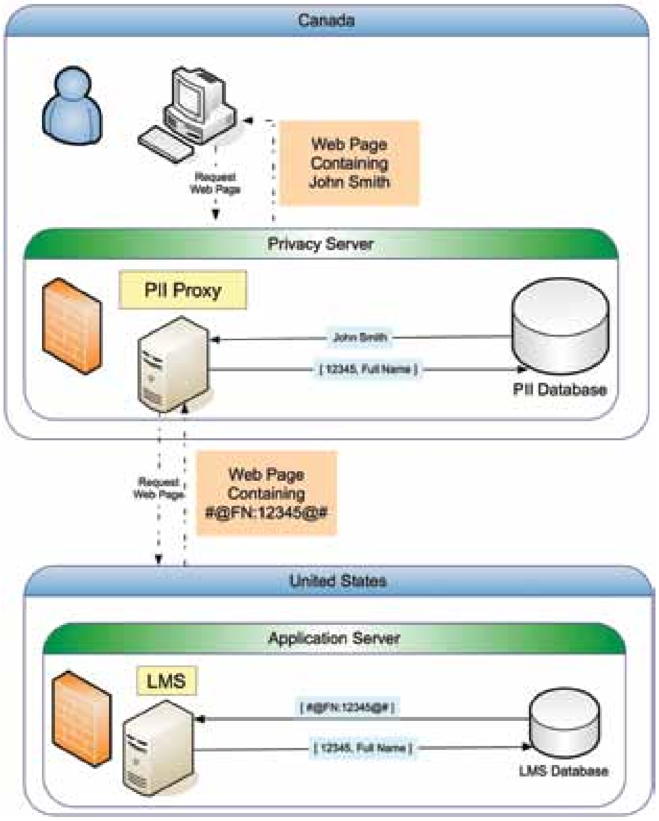
Web requests will pass from the students, through the privacy server, and be delivered to the cloud-based application. Web responses will flow in the reverse direction. On some web pages, the applications may request private information like the student's name. Such a request will generate a lookup of the student's name. Since the student's name and other private information is locked within the privacy server inside Canada, the application will receive and display the token representing the student's name.

When web pages containing tokens pass back through the privacy server, they will be examined by the proxy before they are returned to the student. Any tokens that are found in the web pages will be removed and the actual private information will be inserted in their place. When all tokens have been replaced, the page will be returned to the student. Thus the student will see the private information on a web page generated outside of Canada even though no private information actually left Canada. The process, as experienced by the end user, is seamless and instantaneous.

Conclusions

After careful consideration of the challenges surrounding the protection of private information in a cloud-based environment, Pearson believes that privacy protections should be designed into the technologies themselves. This privacy-by-design approach enables education officials to select best-of-breed learning solutions for their students and teachers with the assurance that private information will be kept securely private. The privacy server described in this paper keeps Canadian students' information locked and encrypted within Canada while still allowing students to access learning resources originating in the United States or elsewhere.

FIGURE 3
PRIVACY SERVER PROXY



Pearson Canada

For more information, please contact us:
26 Prince Andrew Place
Don Mills, Ontario M3C 2T8
416-447-5101
1-800-263-9965
416-443-0948 (fax)
www.pearsoncanada.ca

Download the PDF of this document at:
http://www.pearsoncanada.ca/whitepapers