Privacy

Information Session

Suzanne van den Hoogen, MLIS
April, 2020

SAINT MARY'S UNIVERSITY SINCE 1802
One University. One World. Yours.

Outline

PART 1: FOIPOP

- Introduction of Policy
- Review of FOIPOP Act, personal information, access and privacy rights
- Collection, Use & Disclosure

PART II: Privacy: Best Practices

- Privacy Breach
- Best Practices
  - Passwords
  - Email, FAX, Phone, Copying
  - Office Practices
  - Taking Work Home

Questions/Discussion

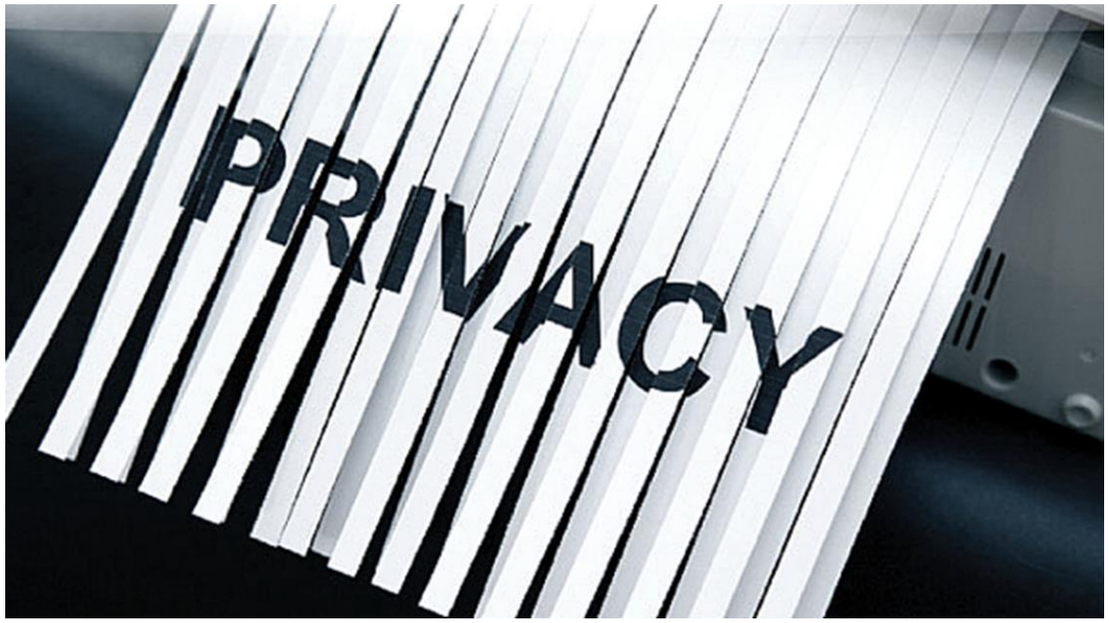


Image Source: http://www.davidellis.ca/wp-content/uploads/2013/07/Privacy-is-stupid.jpg

Canada Student Loans Privacy Breach Class Action – Notice of Settlement Approval

From Employment and Social Development Canada

News

How data breaches cause harm even if no financial info is stolen

Jason Contant

Tweet Share Share Print this page

Share

A recent data breach at an Ontario college highlights the importance of educating clients on cybersecurity, even if no financial information was exposed.

"Even having your name, address and date of birth stolen can still cause problems," Don Duncan, security engineer for Vancouver-based NuData Security, said Tuesday. "Cybercriminals can use this information to create a complete profile of students. Add a bit of social engineering, and they can start cracking all types of accounts and even open up new accounts in the students' names."

Duncan said protecting data from breaches is becoming increasingly challenging, but innovations in technology and following best practices can help organizations detect and mitigate damage after a breach.

Organizations should implement

CBC | MENU

news Top Stories Local The National Opinion World Canada Pc

Edmonton

Laptop stolen with health information of 620,000 Albertans

Health officials recently

CBC News · Posted: Jan 22, 201

Delaware college dean sends list of failing students to all students

November 8, 2010

This week, the dean of students at Delaware-based Wesley College mistakenly forwarded to the school's 2,400 students an e-mail containing the names of 18 students at risk of flunking out. Orig sent to academic advisers, the e-mail described one student as hine shaft in Chile." When college rs recalled the e-mail, but not befo ened it. The institution has apolog nail. The breach potentially violate US Family Educational Rights an rnal | *The Chronicle of Higher Edu*

Politics

CBC warns past, current staff personal data may be at risk after break-in, theft of computer

Corporation has budgeted $300,000 to cover outreach, insurance costs

CBC News · Posted: May 16, 2018 4:20 PM ET | Last Updated: May 16, 2018

Province just sort of stumbles across massive data breach

Personal information for thousands of Nova Scotians compromised thanks to paper-thin security standards.

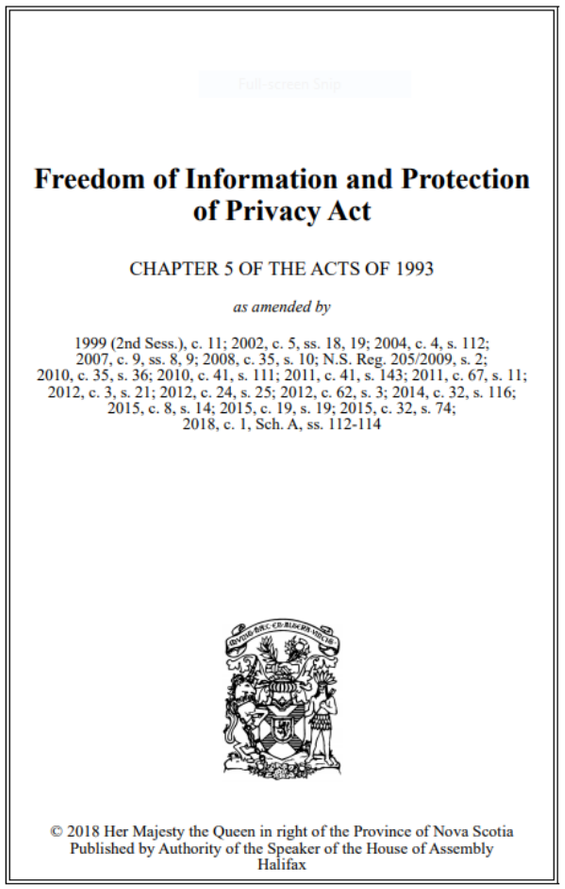
Posted By **Jacob Boon** on Wed, Apr 11, 2018 at 9:36 PM

click to enlarge

The province has been opaque about its transparency website's dangerous transparency.
VIA ISTOCK

FOIPOP

Freedom of Information and Protection of Privacy



Freedom of Information and Protection of Privacy Act

CHAPTER 5 OF THE ACTS OF 1993

as amended by

1999 (2nd Sess.), c. 11; 2002, c. 5, ss. 18, 19; 2004, c. 4, s. 112; 2007, c. 9, ss. 8, 9; 2008, c. 35, s. 10; N.S. Reg. 205/2009, s. 2; 2010, c. 35, s. 36; 2010, c. 41, s. 111; 2011, c. 41, s. 143; 2011, c. 67, s. 11; 2012, c. 3, s. 21; 2012, c. 24, s. 25; 2012, c. 62, s. 3; 2014, c. 32, s. 116; 2015, c. 8, s. 14; 2015, c. 19, s. 19; 2015, c. 32, s. 74; 2018, c. 1, Sch. A, ss. 112-114

- Nova Scotia was the first province in Canada to enact a *Freedom of Information Act* in 1977.
- The *Act* was replaced in 1993 by the considerably improved *Freedom of Information and Protection of Privacy Act* (in force 1994).
- In 1999, the *provincial Act* was also extended to cover local public bodies including hospitals, **universities**, **colleges** and **school boards** (in force since 2000).

A Summary of FOIPOP

Duty to Assist: A Balanced Approach

"Pursuant to the Acts, all public bodies, municipalities and local public bodies are obliged to adopt a policy of **accountability, openness** and **transparency** and to provide a **right of access** to information with limited exceptions. They are also obliged to ensure the **protection** of individuals' personal privacy."

- *NS Office of the Information and Privacy Commissioner*

https://oipc.novascotia.ca/about-the-review-office

When Do Access Rules Apply?

- ALL records in custody, or under the control of Saint Mary's University are subject to the Act, and are "foi-able"
- Records are defined in the Act to include anything on which information is recorded, and include emails, texts, PINs, photographs, etc.
- If an employee does work on a personal device, or uses personal email, that record must be produced in response to an access to information request.

When Do Privacy Rules Apply?

Privacy rules apply to all COLLECTION, USE & DISCLOSURE of personal information

What is Personal Information?

3.1 (i) "Personal Information" means recorded information about an identifiable individual, including:

(i) the individual's name, address or telephone number,

(ii) the individual's race, national or ethnic origin, colour, or religious or political beliefs,

(iii) the individual's age, sex, sexual orientation, marital status or family status,

(iv) an **identifying number**, symbol or other particular assigned to the individual,

(v) the individual's fingerprints, blood type or inheritable characteristics,

(vi) information about the individual's health-care history, including a physical or mental disability,

(vii) information about the individual's **educational**, financial, criminal or employment history,

(viii) anyone else's opinions about the individual, and

(ix) the individual's personal views or opinions, except if they are about someone else;

Personal

Information about an identifiable individual that is recorded in **ANY FORM**

NS FOIPOP Act: https://nslegislature.ca/sites/default/files/legc/statutes/freedom%20of%20information%20and%20protection%20of%20privacy.pdf

Information and Privacy Rights

There are two major rights under *the Act*:

1. **Access:** the right of **access** to records in the custody or under the control of a public body, including your own personal information; and
2. **Privacy:** the right of protection for the **privacy** of your personal information in the custody or under the control of a public body.

As employees of a public body we share in these responsibilities and duties.

What is a **record** under the Act?

- A **record** is documented or fixed information. This information may be correspondence, a video, emails, databases or any other source of recorded or stored information.

- The Act applies to ALL **records** in the custody or under the control of the public body.

Note: You have the right to request **access** to your personal information, to **view** this information, to **ensure its accuracy**, and to **request correction** of errors.

FOIPOP: Balancing access and the protection of privacy

What are the basic access to information rules?

- Anyone can apply
- $5 fee for general information
- $0 to request your own personal information
- 30 days to respond

FOIPOP: Balancing access and the protection of privacy

What are the basic access to information rules?

- Full disclosure unless exemption applies
- 15 limited and specific exemptions
- Duty to sever
- FOIPOP Officer/coordinator processes the request

Access rules for staff

- Keep good records – always file centrally
- Follow records retention schedules whenever possible
- Respond promptly and thoroughly to any search request
- Keep personal information secure
- Know the privacy rules that apply to your work

Office of the Registrar

- ✓ Maintains/protects official student academic records
- ✓ Controls access to student information
- ✓ Authorises the release of official information

Image Source: http://www.dataprix.com/files/uploads/103image/lock.jpg

Three Points...

1

In the process of getting students from admission to graduation the University must collect personal information from students.

- there is a duty to ensure that information is used only for the intended purpose for which the information was collected
- there is a duty to ensure that information is held in confidence and that students' privacy is respected

Three Points…

2

The Office of the Registrar oversees students' academic records at Saint Mary's University.

- access is controlled
- official information may only be released under certain conditions

Three Points…

3

A clear distinction must be made between public and private information.

- expectations about privacy are changing due to changes in legislation, and decisions rendered by the courts
- only a very few pieces of information may be released without the student's permission

Disclosures Authorized by FOIPOP

Information considered to be public record:

- period of registration
- programme of studies
- credentials awarded
- dates of graduation

NOTE: Students have the right to request that this information NOT be made publicly available.

Basic Privacy Rules

- **No** collection unless authorized
- **No** use unless authorized
- **No** disclosure unless authorized
- Keep personal information secure

Advice

Be respectful of students' privacy, and follow University policies

When in doubt, ask the Registrar, or contact the FOIPOP Officer

Part II

Privacy: Best Practices

SAINT MARY'S UNIVERSITY SINCE 1802

One University. One World. Yours.

Privacy Quiz

Privacy Quiz

THE 5-MINUTE PRIVACY CHECKUP

As an employee of a public body, you should be aware of your responsibilities to keep personal and sensitive information secure. Current privacy standards require that public bodies protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

This 5-minute privacy checkup asks a series of questions relating to the security of personal information and sensitive business information both hard copy and electronic. A "no" answer to any of these questions is a warning sign that the information may not be secure.

Physical Security		
	Y	N
Do you have files containing sensitive information stored in your office? • If yes, is the sensitive information stored in a locked filing cabinet? • Do you lock your office door whenever you leave the office?		
At the end of the day do you always: • Clear your desktop of all files containing sensitive information? • Store your laptop and all files in a locked filing cabinet? • Lock your office door? • Log off your computer? • Remove all documents containing sensitive information from faxes and printers?		
Email & Faxing		
Before emailing sensitive information do you: • Ensure that either the owner of the sensitive information has consented to transmission via email or that the information is encrypted? • Always attach a confidentiality notice?		
Before faxing any sensitive information do you: • Only send from a secure fax machine? • Prior to sending, call the receiver to confirm that the receiving fax machine is secure and to confirm the fax number? • Always use a cover sheet that includes both the sender's name and phone number and the intended recipient's name and phone number? • Always attach a confidentiality notice?		
Security of Electronic Files		
	Y	N
Do you always have to login to any system using a unique identifier and password?		
Is your password complex (numbers, symbols, letters etc) and at least six characters in length?		
Have you changed your password in the last 90 days?		
Do you store all electronic files containing sensitive information on a secure central server? (i.e. no sensitive information stored on local hard drive)		
Is your office computer screen positioned so that no unauthorized individuals can view sensitive information displayed?		
Have you set your screen saver so that you are automatically logged out after a 5 minute period of inactivity?		
Training & Knowledge		
In the last 12 months, have you completed training on privacy and security of sensitive information?		
Do you know whether or not you have authority to collect, use or disclose personal information?		
If you do have authority to collect, use or disclose personal information, do you know the limits and conditions of that authority?		
Mobile & Portable Devices		
	Y	N
Do you always store mobile or portable storage device such as laptops in a locked cabinet when not in use?		
Is all sensitive information contained on your portable storage devices limited to the absolute minimum necessary?		
Have you ensured that all sensitive information contained on any portable storage device you use is encrypted?		
Do you permanently delete sensitive information from your portable storage devices as soon as possible after use?		
Secure Disposal of Sensitive Information		
Do you dispose of hard copy records containing sensitive information by placing them in a secure shredding bin or by shredding them yourself?		
Privacy Habits		
Do you avoid discussing personal information in any area where the conversation can be overheard by unauthorized personnel?		
Do you disclose personal information to co-workers only where the information is necessary for the performance of the duties of your co-workers?		
If you must travel with personal information, do you always ensure that any personal information you have is stored in a locked cabinet or cupboard and never in your car?		

What is a Privacy Breach?

A privacy breach occurs when personal information is collected, retained, used or disclosed in ways that are not in accordance with the provisions of the Act.

It's the LAW: Mandatory Data Breach Reporting

NOTE: As of Nov 1, 2018, we are required by law to report privacy breaches involving personal information, even if they do not pose a real risk of significant harm to an individual. These records must be maintained for a period of 24 months after determining that a breach has occurred.

Examples of Privacy Breaches

Among the most common breaches of personal privacy is the unauthorized disclosure of personal information, such as:

- sending communications to the wrong recipient (email, FAX)
- improper records destruction procedures
- loss or theft of unsecured devices, such as laptop computers, smart phones, digital cameras, or portable storage devices (USB sticks)
- unauthorized access (snooping, looking up your co-worker's birthday)

Harder-to-Spot Privacy Breaches

- Your daughter sat in your office while you completed a few performance evaluations
- You left out those performance files overnight so you can get back to them first thing in the morning
- You post work-party photos on Facebook

Best Practices: Passwords

Image Source: http://www.techeconomy.it/wp-content/uploads/2014/01/password.png

- ✓ Select a secure password
- ✓ Never share or disclose your password
- ✓ Do not use the same password for multiple accounts
- ✓ Do not use a dictionary word
- ✓ Adopt long passphrases

Best Practices: Email & Internet

- Update your operating system regularly
- Be aware: spyware and viruses can be sent as email attachments.
- Double check that you have the correct email address BEFORE sending
- Make it easier for others to identify you by including your profile photo, or an icon/logo representing your department on your internal mail

Image Source: https://www.techtrends.co.zm/wp-content/uploads/2014/07/foto-oops-e1373900707160.jpg

Mobile Devices: Know the risks

Image Source: http://pngimg.com/uploads/smartphone/smartphone_PNG8514.png

Image Source:http://freesoftwaremagazine.com/articles/grub_intro/usb_flash_memory_key.jpg

- Do you really need to transport personal information? (i.e., taking work home)
- Password Protection & Encryption
- Physically protect and secure your device (i.e., don't leave your laptop in your car)
- Promptly report lost or stolen devices
- Be selective when downloading apps

Best Practices: Office

- Clean-Desk Policy
- Lock filing cabinets
- Shut down your computer at the end of every work day
- Proper disposal

Image Source: https://lignux.com/wp-content/uploads/2016/02/basura_confidencial.jpg

FOIPOP: Saint Mary's University

Website: https://smu.ca/about/foipop.html

FOIPOP

- Guidelines for Requests
  - Record-Keeping Tips
  - Confidential Records
  - Student Information
  - Use of Email
  - Administration of Rights
- FAQs
- Information
- Web Sites

Image Source: https://lignux.com/wp-content/uploads/2016/02/basura_confidencial.jpg

DON'T HAVE AN IDENTITY CRISIS

10 TIPS FOR PREVENTING IDENTITY THEFT

Secure your devices

Ensure your operating system, software, browsers, anti-virus and firewalls are **installed, updated and properly configured.**

Lock it down

If you use a computer, laptop or mobile device, both privacy and security depend on use of strong **passwords and encryption.**

Protect your mail

Ensure your **mailbox is secured**; pick-up sensitive documents in-person; follow up on bills or statements that don't arrive.

Consider what you carry

Remove cards or documents from your wallet that you don't use regularly, especially your Social Insurance Number (SIN) card or birth certificate.

Shop securely

If online, ensure the site is secure (**look for the 'lock' icon** or green highlighted URL). In person, use chip and PIN devices only.

Don't dump data

Shred personal documents that you no longer need and **delete** personal information before discarding or selling a digital device (although deleting doesn't always wipe data completely —additional steps may be required).

Take care with credit

Be cautious when providing credit card information, **review statements** and cut up unused or expired cards.

Spot the scam

Do not reply to email messages, click links or open attachments from companies or others asking for your personal information.

Be firm on the phone

Don't give personal information to anyone who phones unless you can **confirm they are from a legitimate company.**

Be cautious and curious

If asked for your personal information, ask how it will be used, why it is needed, and how it will be protected. **When in doubt, don't give it out.**

Office of the Privacy Commissioner of Canada

priv.gc.ca Follow us on Twitter - @PrivacyPrivee

Additional Resources

Freedom of Information and Protection of Privacy Act: https://nslegislature.ca/sites/default/files/legc/statutes/freedom%20of%20information%20and%20protection%20of%20privacy.pdf

Managing a Privacy Breach: https://beta.novascotia.ca/documents/manage-privacy-breach-protocol-and-forms

Nova Scotia FOIPOP: https://novascotia.ca/tran/hottopics/FOIPOP.asp

Office of the Privacy Commissioner of Canada: https://www.priv.gc.ca/en/

Online Privacy: Tips & Best Practices: https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/online-privacy/

Personal Information International Disclosure Protection Act (PIIDPA): https://nslegislature.ca/sites/default/files/legc/statutes/persinfo.htm

Personal Information Protection and Electronic Documents Act (PIPEDA): https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

Saint Mary's University FOIPOP: https://smu.ca/about/foipop.html

References

Slide 3: In the News

- https://www.thecoast.ca/RealityBites/archives/2018/04/11/province-just-sort-of-stumbles-across-massive-data-breach
- https://www.cbc.ca/news/canada/edmonton/laptop-stolen-with-health-information-of-620-000-albertans-1.2507161
- https://www.academica.ca/top-ten/delaware-college-dean-sends-list-failing-students-all-students
- https://www.canada.ca/en/employment-social-development/programs/canada-student-loans-grants/privacy-breach-notice.html#h2.1
- https://www.cbc.ca/news/politics/cbc-privacy-breach-insurance-1.4665909
- https://www.canadianunderwriter.ca/legal/data-breaches-cause-harm-even-no-financial-info-stolen-1004134615/

Slide 4: FOIPOP: Freedom of Information and Protection of Privacy

- https://nslegislature.ca/sites/default/files/legc/statutes/freedom%20of%20information%20and%20protection%20of%20privacy.pdf

Slide 32: Don't Have an Identity Crisis: 10 Tips for Preventing Identity Theft

- https://www.priv.gc.ca/en/privacy-topics/identity-and-privacy/identity-theft/idt_info_201303/

Acknowledgement:

Slide content and design adapted, with permission, from Cape Breton University FOIPOP Officer, Catherine Arseneau

- https://www.cbu.ca/wp-content/uploads/2018/09/Student-Records-Policy-MASTER-2018.ppt

Thank You

Discussion

Questions