

Three Privacy Breaches (and What We Can Learn From Them)

Presentation to the Law Society of Nunavut

June 26, 2024

John L. MacLean CIC.C, Senior Legal Counsel

Government of Nunavut

Disclaimer



The information in this presentation is intended for educational use and it is not legal advice.



The opinions and analysis in this presentation are the presenter's alone, and they do not necessarily represent the opinions or position of the Government of Nunavut or the Attorney General for Nunavut.


Outline

What is a Privacy Breach?

The Tell-Tale Blog

The Privacy Breach Cup

Privacy Breaches: there's an App for that



What is a Privacy Breach?

Overview



Relevant Legislation

Territorial

- ▶ *Access to Information and Protection of Privacy Act, C.S.Nu., c. A-20 (“ATIPP”)*
 - ▶ Applies to all territorial public bodies

Federal

- ▶ Privacy Act, R.S.C. 1985, c. P-21
 - ▶ Applies to federal institutions
- ▶ *Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5*
 - ▶ Applies to private sector organizations using personal information for commercial activities

A Privacy Breach is:

- ▶ Any unauthorized:
 - ▶ Collection
 - ▶ Use
 - ▶ Disclosure
 - ▶ Access
- ▶ Involving personal information that is in the custody or control of:
 - ▶ A public body (*ATIPP Act*)
 - ▶ An institution (*Federal Privacy Act*)
 - ▶ An organization (*PIPEDA*)

Data Breach vs. Privacy Breach

Data Breach


- ▶ Any unauthorized collection, use, disclosure or access to an organization's information
- ▶ Typically involves commercially sensitive information

Privacy Breach

- ▶ Always involves identifiable personal information
- ▶ All privacy breaches are data breaches, but not all data breaches are privacy breaches

Today's Examples


- ▶ We'll be looking at three privacy breaches
- ▶ All are true stories and matters of public record:
 - ▶ One is from Nunavut
 - ▶ One is from the United States
 - ▶ One involves a major national food service company
- ▶ Each is an example of a common privacy breach



The Tell- Tale Blog

The Breach

A Mental Health Nurse working in a Nunavut community writes a blog about “Life North of 60”



The blog doesn't name names, but reveals information about:

Conflicts with her roommates, who were also colleagues; and

Her clients, who could be easily identified

The Response

The Mental Health Nurse lost her job

The Department of Health:

- Issued a take-down notice for the blog;
- Notified the Information and Privacy Commissioner;
- Notified the affected individuals; and
- Increased the frequency of privacy training

Lessons Learned



Regular privacy training for all staff can help reduce breaches



Privacy training can never be considered “one and done”



Privacy breaches can have professional consequences

The Privacy Breach Cup

And the law of unintended consequences



The Breach

Nurses complain about the timed lockouts on their computer terminals

The nurses had to re-enter their password every time the computer locked out

As a solution, the Hospital's IT team installs a sensor at every computer terminal

Nurses discovered how to by-pass the sensor with an XL to-go coffee cup, so the computers never lock out

Now, everybody in the waiting room can see patient information on the computer screens.

Lessons Learned



Nurses were disciplined



Coffee cup was recycled



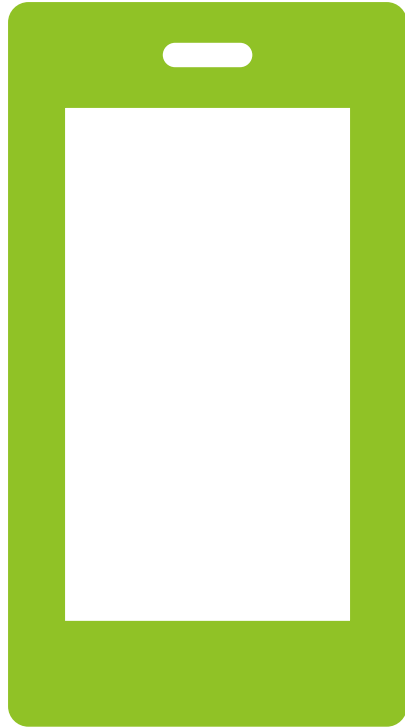
Hospital increased its privacy training



The IT department went back to the drawing board

Lessons Learned

- ▶ This case is a textbook example of:
 - ▶ Users finding workarounds for the employer's privacy and security programs
 - ▶ Employers instituting programs that may be unsuitable for their environment
 - ▶ IT solutions solving one problem while creating another, larger problem
- ▶ Involve employees when designing programs and solutions, and
- ▶ Don't deploy solutions until you're sure that they are fit for purpose.



There's an App for That

Coffee with a side of privacy breach

The Breach

- ▶ Tim Hortons used a new version of its App to track and collect location data from its users, including when the App was turned off
- ▶ Users consented to the data collection, but only when the App was in use
- ▶ Tim Hortons intended to use the data for the purposes of targeted marketing, but it never used the data



The Response

- ▶ Joint investigation by the Privacy Commissioners of Canada, Quebec, Alberta and BC determined:
 - ▶ Tim Hortons did not have a legitimate need to collect vast amounts of location data
 - ▶ Tim Hortons did not obtain valid consent (violating Principle 4.3 of PIPEDA)
 - ▶ The contract between Tim Hortons and its App Developer contained vague and permissive language on what information could be collected and how it could be used
- ▶ Tim Hortons deleted the data and agreed to implement and maintain a privacy management program

Lessons Learned

- ▶ Proportionality: is the loss of privacy proportional to the benefits to the commercial activity?
- ▶ Precise contract drafting can reduce the risk of a privacy breach
- ▶ Organizations should ensure that their clients understand how their information is being collected and used

The Cost of Privacy Breaches



Financial: The cost of mitigating a privacy breach can be as much as 15 times higher than the cost of implementing a privacy and security program

Global average cost of a privacy breach in 2023: \$4.45 Million US or \$165/record



Reputational: privacy breaches erode public confidence in your organization;



Employment: individuals who breach privacy legislation are subject to disciplinary action, up to and including termination

Summary

- ▶ Like nature, privacy breaches will always find a way
- ▶ Preventing privacy breaches will always engage:
 - ▶ Physical Safeguards (i.e., locks on doors, access controls)
 - ▶ Administrative Safeguards (i.e., policies, procedures, training)
 - ▶ Technical Safeguards (i.e., encryption, data masking)
- ▶ As in all contracts, precision matters
 - ▶ Engage subject matter experts
- ▶ Protect your clients' personal information
 - ▶ Know your obligations as a custodian

Sources

- ▶ The Tell-Tale Blog:
 - ▶ Review Report 16-106 (Re), 2016 NUIPC 10 (CanLII)
- ▶ The Privacy Breach Cup:
 - ▶ Jim Blythe, Ross Koppel, and Sean W. Smith, “Circumvention of Security: Good Users Do Bad Things” (IEEE Security & Privacy, vol. 11, Sept/Oct 2013, pp. 80-83)
- ▶ There’s an App for That:
 - ▶ Joint Investigation into Location Tracking by the Tim Hortons App, PIPEDA Findings #2022-001, 2022 CanLII 50894 (CanLII)
- ▶ Costs of Privacy Breaches:
 - ▶ IBM Security Cost of a Data Breach Report, 2023

Questions?

- ▶ Now's the time to ask, or contact me by phone or email:
 - ▶ John L. MacLean CIC.C
 - ▶ jmaclean@gov.nu.ca
 - ▶ (867) 975-6323