Privacy Legal Update: Recent and Upcoming Privacy Law Developments

David Goodis, Information and Privacy Commissioner of Ontario

Fida Hindi, Fasken Martineau DuMoulin LLP

Ontario Connections: Access, Privacy, Security and Records Management Conference May 21, 2015

Overview

- Personal Information Definition (ONCA)
- Collection of Personal Information (Div Ct)
- Police Searches and the *Charter* (SCC)
- *PIPEDA* Compliance
- Police Record Checks
- Employee Monitoring
- Common Law Tort and *PHIPA* (ONCA)
- Common Law Tort (ONSC)
- Privacy Breach and *PHIPA*

Personal Information

***Royal Bank of Canada v. Trang*, 2014 ONCA 883**

- RBC has judgment against the defendants and the defendants own property which they have mortgaged to Scotiabank
- RBC wants the sheriff to sell the property so it can collect the judgment
- The sheriff requires a mortgage discharge statement from Scotiabank
- RBC attempted to obtain the mortgage discharge statement by examining the defendants as judgement debtors but they did not appear for the examinations
- RBC asked Scotiabank to produce a mortgage discharge statement
- Soctiabank said that *PIPEDA* precluded it from disclosing the mortgage discharge statement

Personal Information

- RBC brought a motion for an order that Scotiabank produce a mortgage discharge statement
- Motion and appeal dismissed
- Mortgage discharge statement is personal information
- Financial details of a mortgage when it is registered are on the public record in the Ontario Land Registry System. However, current mortgage balances are not publicly available
- "[I]t can hardly be denied that a current mortgage balance is, under PIPEDA, personal information of a mortgagor – it is "information about an identifiable individual." Nor can it be said that the Trangs have waived any privacy interest in their current mortgage balances simply because the details of their mortgage at the time of registration are on the public record."

Personal Information

- Financial information is sensitive information – RBC cannot rely on implied consent and express consent is required
- disclosure of a discharge statement to a judgment creditor is not within the reasonable expectations of a mortgagor
- RBC could have obtained the mortgage discharge statement by:

1. a term in its loan agreement with the Trangs; or
2. a motion under r. 60.18(6)(a) of the Rules of Civil Procedure.

- RBC cannot rely on s. 7(3)(c) of *PIPEDA* by bringing this motion.
- Dissent by Justices Hoy and Sharpe

Collection of Personal Information

LCBO v. Vin De Garde Wine Club, 2015 ONSC 2537

- LCBO has private ordering system, allows wine clubs to register with LCBO, buy wine on behalf of club members
- when registering, club must provide members' names
- LCBO begins practice of requiring name of each member and details of wine they are ordering, before filling club's order
- IPC investigates, finds collection of PI does not meet test of "necessary to the proper administration of a lawfully authorized activity" [*FIPPA*, s. 38(2)]

Collection of Personal Information

- IPC makes “cease collection” order against LCBO under *FIPPA* s. 59(b) [Order PO-3356-R]
- Divisional Court upholds IPC on judicial review
- agrees that necessary in s. 38(2) means more than merely helpful, and if purpose can be achieved another way, institution must choose the other route [see *Cash Converters*, 2007 ONCA 502]
- IPC reasonable in finding that evidence of necessity insufficient, including lack of evidence of fraud
- LCBO has applied for leave to appeal to ON CA

Police Searches and the *Charter*

***R. v. Fearon*, 2014 SCC 77**

- Two men robbed a store
- Police located the suspects and completed a pat-down search during the arrest
- Police found a cell phone and searched it
- A draft text message read “We did it were the jewlery at ni**a burrrrrrrrrrr”, and some photos, including one of a handgun
- The police subsequently searched a vehicle with a warrant and recovered the handgun used in the robbery and depicted in the photo
- The police applied for and were granted a warrant to search the contents of the phone a few months after

Police Searches and the *Charter*

- Common law power to search incident to a lawful arrest permits search of cell phones and similar devices
- Some modification to existing common law framework necessary because the search of a cell phone has the potential to be a much more significant invasion of privacy
- Four conditions must be met in order for the search of a cell phone or similar device incidental to arrest to comply with s. 8:

1. arrest must be lawful
2. search must be truly incidental to the arrest (must be done promptly upon arrest) to serve law enforcement purposes
3. nature and the extent of the search must be tailored to its purpose
4. police must take detailed notes of what they have examined on the device and how they examined it

Police Searches and the *Charter*

***R. v. Spencer*, 2014 SCC 43**

- police identify IP address of computer used to access child pornography
- police ask for, ISP discloses, subscriber information associated with IP address (name, address, phone number)
- disclosure made under *PIPEDA* s. 7(3)(c.1)(ii) [disclosure without consent for law enforcement purpose]; no warrant
- person located, charged, convicted of possession
- did accused have reasonable expectation of privacy in subscriber information?

Police Searches and the *Charter*

- person's identity linked to their internet activities indicates privacy interest beyond that inherent in name/address/phone number [not just phone book!]
- people have strong interest in anonymity online -- may be foundation of privacy interest that engages constitutional protection against unreasonable search and seizure [*Charter* s. 8]
- *PIPEDA* section not a factor weighing against REP, since its proper interpretation depends on existence of REP
- contractual provisions with ISP support REP

Police Searches and the *Charter*

- since REP in this case, police request for information = search under *Charter* s. 8

- search not lawful: neither *PIPEDA* nor *Criminal Code* [s. 487.014(1)] create authorization

- but evidence not excluded, since doing so would bring administration of justice into disrepute

- Canadians now have RE that ISPs will not disclose subscriber info to law enforcement unless required by law [*e.g.*, court order]

PIPEDA Compliance

PIPEDA Report of Findings #2015-001

- Commissioner initiated complaint to consider privacy issues surrounding Bell's use of customers' network usage and account information to enable the serving of targeted ads (Relevant Advertising Program)
- Commissioner found express consent is required due to:

1. Sensitive information collected; and
2. Reasonable expectation of customers

- Commissioner found customers unable to withdraw consent
- Opt-out consent not the default for all behaviourally targeted advertising
- Following release of report, Bell decided to withdraw the program

Police Record Checks

Crossing the Line Investigation Report: ON IPC

- Toronto woman denied entry to US at Pearson Airport due to mental health concern
- 2012 suicide attempt on CPIC due to 911 call
- US border officials have direct, instant CPIC access
- IPC finds police uploading information about suicide attempt/threat is improper disclosure [*FIPPA*, s. 42]
- disclosure permissible only where valid public safety concern [e.g., threat of harm to other individuals, history of violence]

Police Record Checks

- most police services comply with IPC's recommendations
- but Toronto Police Service refuse
- IPC brings application for judicial review, asks Divisional Court to order compliance [hearing expected in fall 2015]
- note province considering legislation on police record checks, in context of employment, volunteer positions

Employee Monitoring

BC IPC Investigation Report F15-01

- January 2015, Mayer Atwell of the District of Saanich made public comments that the District installed software on his office computer that was collecting his PI without his knowledge and consent

- Saanich Council and the District made various comments, including an assertion that employees do not have a reasonable expectation of privacy at work

- Commissioner initiated an investigation to determine if District's use of monitoring software was compliant with *FIPPA*

Employee Monitoring

- Commissioner's findings:

1. District did collect the PI of employees and citizens through its use of monitoring software. District collected all PI that a user entered into their workstation
2. District did not have the authority under *FIPPA* to collect the PI recorded by the monitoring software
3. District did not notify employees of the collection of their PI as required by *FIPPA*
4. Could not be determined whether District used or disclosed PI collected by the monitoring software in compliance with *FIPPA* because the District had not activated the functionality to monitor user access through logs that show user activity

Privacy Tort and *PHIPA*

***Hopkins v. Kay*, 2015 ONCA 112**

- *PHIPA* provides avenue to seek damages where IPC makes an order [s. 65]
- class action proceeding brought in Superior Court against Peterborough Hospital based on common law tort [*Jones v. Tsige*]
- hospital argues *PHIPA* is sole avenue
- IPC intervenes, argues in favour of CL right, since IPC will exercise discretion not to conduct review/issue order for wide variety of reasons

Privacy Tort and *PHIPA*

- Ontario Court of Appeal rules that limiting right to cases where IPC issues *PHIPA* order too restrictive
- case allowed to proceed despite absence of *PHIPA* order
- hospital seeks leave to appeal to Supreme Court of Canada

Common Law Tort

McIntosh v. Legal Aid Ontario, 2014 ONSC 6136

- Plaintiff learned during a fight with her ex-boyfriend that his new girlfriend, who worked at Legal Aid Ontario, had accessed her file in order to gather information about the plaintiff
- Defendant phoned the plaintiff and revealed that she had obtained confidential information from the plaintiff's LAO case file, including that the plaintiff was involved with a children's aid file
- Defendant threatened to call the Children's Aid Society in an effort to have the plaintiff's children taken away from her

Common Law Tort

- Plaintiff plead that she experienced “substantial anxiety, emotion [sic] upset, depression, significant stress, embarrassment, weight loss, insomnia, isolation, and an inability to concentrate at work”
- Defendant accessed the file for an improper purpose
- No evidence provided to show that anxiety or depression was caused by the intrusion
- No evidence provided to show defendant contacted the Children’s Aid Society and disclosed the plaintiff’s personal information
- No evidence plaintiff was employed at time of incident
- General damages in the amount of $7,500

Privacy Breach: *PHIPA*

PHIPA Order HO-013: Rouge Valley Health System

- two clerical staff accessed "new baby" information, to market/ sell RESPs

- IPC reviews breaches, finds:
  - deficiencies in audit functionality meant hospital could not comply with its own policies, and *PHIPA*
  - certain of hospital's privacy policies, training insufficient
  - non-compliance with *PHIPA* s. 12(1) duty to have reasonable measures to protect PHI

- *PHIPA* interpretation issue: agent definition in s. 2(1) includes employees who act for or on behalf of a HIC in the usual course of their duties [even if they act beyond authority delegated by HIC]

Privacy Breach: *PHIPA*

- IPC requires hospital to [among other things]:
  - change system to ensure ability to fully audit agent access to PHI
  - revise audit, confidentiality policies
  - develop/implement privacy training, privacy breach management policies
- hospital has appealed order to Divisional Court

- **David Goodis**
- david.goodis@ipc.on.ca
- 416-326-8723

- **Fida Hindi**
- fhindi@fasken.com
- 416-865-4389