Privacy Law Update

David Goodis, Assistant Commissioner, Information & Privacy Commissioner of Ontario)

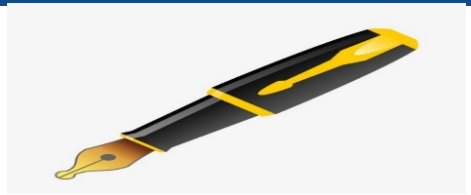
Claire Feltrin, Associate – Privacy, Technology & Data Management, Torkin Manes LLP)

Ontario Connections
May 31, 2018

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Torkin Manes
Barristers & Solicitors

Video surveillance
R v Jarvis (SCC 2018)



- high school teacher used camera pen to surreptitiously video female students
    - videos included faces, but focused on students' chests and cleavage
- charged with voyeurism [*Criminal Code* s. 162(1)(c)]
- trial court says students have reasonable expectation of privacy, but not satisfied beyond reasonable doubt that videos done for sexual purpose

Video surveillance
R v Jarvis (SCC 2018)

- Ontario Court of Appeal:
  - videos taken for sexual purpose – trial judge had found conduct "morally repugnant"
  - but students not in circumstances giving rise to reasonable expectation of privacy while engaging in normal school activities and interactions in "public" areas
- SCC appeal [heard April 2018, on reserve]
  - REP in school context hotly debated, court seems divided
  - many intervenors (ON IPC, CCLA, CLA)

Video surveillance
Municipal video cameras

- BC cities plan to implement video surveillance in public spaces
  - BC IPC working with them to determine if lawful
  - key question: less invasive options attempted?
  - "If we surrender our public spaces to surveillance – where we all have the right to be – we may never get them back" [BC Commissioner McArthur]
- similar debate in ON
  - Hamilton proposed bylaw change to allow private property cameras to aim towards street
  - Is this being done on behalf of police?

Extra-territorial reach of Canadian privacy law

Three key cases:

- *Douez v Facebook* (SCC 2017)
- *AT v Globe 24h* (FC 2017)
- *Google v Equustek* (SCC 2017)

Douez v Facebook (SCC 2017)

- Latest SCC guidance re: class actions and privacy breaches
- SCC found plaintiff established strong reasons to decline to enforce FB's forum selection clause (action under BC *Privacy Act* permitted to proceed in BC)
- Important implications for:
  - consumers and corporations seeking to rely on forum selection clauses in the event of privacy disputes
  - Provincial legislatures

AT v Globe 24h (FC 2017)

- Globe24h.com = websites hosted and operated in Romania which republishes public documents, including Canadian court and tribunal decisions containing PI
  - Also appeared on third party search engines (i.e. Google)
- Globe24h profited by charging fees to remove this information from its site
- Issues:
  - a) does PIPEDA apply to activities carried out abroad;
  - b) what remedies can Canadian courts order in the circumstances
- Globe24h ordered to remove Canadian decisions containing personal information from website and search engine caches

Google v Equustek (SCC 2017)

- June 2017: SCC released highly anticipated decision arising out of IP litigation between Equustek (E) (a tech company) and a third party called DataLink (D) (a distributor) involving unlawful use/sale of E's IP over the internet
- SCC upheld injunction restraining Google (a non-party to the litigation and non-resident corporation) from publishing offending websites in its search results worldwide
- Grounds for upholding injunction
    - Re extraterritorial application: The problem is occurring online and globally. The Internet has no borders – its natural habitat is global
    - No violation of international comity (injunction does not require Google to violate foreign laws)
- December 2017: US District Court (California) grants a counter-injunction, holding that the SCC's injunction = unlawful and unenforceable in the US
- April 16, 2018: Google application to set aside or vary the Canadian injunction dismissed by BCSC

Privacy v public interest in disclosure

Ontario Medical Assn v ON IPC 2017 ONSC 4090, appeal pending

- judicial review of IPC order directing Ministry of Health to disclose to a reporter
  - names, annual billing amounts, medical specialty of top 100 billing doctors
- IPC rules not PI; even if so, public interest override requires disclosure
- court agrees with IPC that names, OHIP billing amounts not personal information [professional or business info]

Privacy v public interest in disclosure

Barker v ON IPC 2017 ONSC 7564, appeal pending

- judicial review of IPC order upholding Algoma Public Health (APH) decision to disclose KPMG forensic investigation report into allegations of serious misconduct by senior staff
- APH used rarely invoked public interest override [*MFIPPA* s. 16]
- applicant is APH's former CEO/Medical Officer of Health

Privacy v public interest in disclosure

Barker v Ontario (IPC) 2017 ONSC 7564, appeal pending

- court quashes IPC order, finds Commissioner did not identify each piece of PI that is exempt under personal privacy exemption [*MFIPPA* s. 14]
- public interest override requires decision maker to consider specific information exempted, weigh against relevant public interest
- IPC granted leave to appeal to Court of Appeal
    - arguing in part that court's interpretation imposes unreasonable, impractical burden on gov't, IPC, unsupported by s. 16 language

Canada and the EU's GDPR

What is the GDPR?

- EU General Data Protection Regulation (GDPR) came into force on May 25, 2018, replacing the existing EU Data Protection Directive
- Key elements:
    - Enhanced Consent
    - Data Erasure/Right to be Forgotten
    - Data Portability
    - Right to Object to Automated Decisions
    - Privacy by Design
    - Mandatory Breach Notification

GDPR and Canadian Adequacy Status

- Under the existing EU Data Protection Directive, *PIPEDA* has "adequacy status"
  - An adequacy decision of the EC permits transfers of information about EU data subjects to organizations in Canada without additional safeguards or the need for Canadian organizations to show compliance with EU data protection Law
- Substantially similar provincial laws also benefit

GDPR and Canadian Adequacy Status

- Is Canada in danger of losing it adequacy status?
    - Adequacy decisions to be reviewed every 4 years
- Recent ECJ cases also serve to emphasize access to personal information by government authorities
    - European Commission monitoring developments in Canadian privacy law
- Foreign organizations must comply with GDPR if processing data about EU data subjects for:
    - The offering of goods or services; or
    - The purpose of monitoring the data subjects' behaviour within the EU
- Significant financial penalties for non-compliance

Law enforcement and hydro data

R v Orlandis-Habsburgo 2017 ONCA 649

- accused operated commercial-sized marijuana grow-op in basement
- Horizon noted pattern of electricity use in home consistent with grow-op, provided info to police
- Horizon and police had developed informal information-sharing arrangement whenever Horizon noticed suspicious energy consumption pattern

Law enforcement and hydro data

R v Orlandis-Habsburgo 2017 ONCA 649

- did police receipt of information breach *Charter* s. 8?
- Court of Appeal finds reasonable expectation of privacy in energy consumption data
- *PIPEDA/MFIPPA* provisions allowing organizations to disclose PI to law enforcement [s. 7(3)(d)(i)/32(g)] do not permit ongoing PI sharing arrangement with police
    - case by case discretion required for each disclosure
- court did not exclude evidence [*Charter* s. 24(2)]; police's understanding reasonable given state of the law at time of search [pre *Spencer* (SCC 2014)]

Use of PI for Political Purposes

- Ongoing investigations (OPC, OIPC BC, UK ICO, etc) into possible privacy contraventions involving alleged manipulation of UK and US election campaigns
- Potential implications for political parties/campaigns and data and social media companies (e.g. Cambridge Analytica [CA], AggregateIQ [AIQ], and Facebook [FB])

Use of PI for Political Purposes

Background:

- 2014: Aleksandr Kogan (data scientist at Cambridge) created FB app which surveyed thousands of FB users for “academic purposes”
- Varying reports indicate CA purchased the app or the data
- FB’s design enabled collection of PI not only of surveyed users, but also of their FB “friends”; resulted in compilation of millions of FB users’ psychological profiles
- Various political campaigns alleged to have retained CA and AIQ to use the data to micro-target voters

Use of PI for Political Purposes

- March 2018: Christopher Wylie (former CA employee) blows whistle re: ties between CA, AIQ, and UK political campaigns
- April 2018: FB CEO testifies before the US Congress and publicly apologizes for the data breach
  - FB has been sued in the US by users and shareholders and recently announced changes to its partner category service (involving use of third party data to target advertising)
- May 2018: CA commenced insolvency proceedings in the US and UK due to impact of negative media coverage (no clients and legal fees)

Mandatory breach notification to IPC

ON *Personal Health Information Protection Act*

- pre-existing
    - health information custodian must notify affected individuals at first reasonable opportunity if PHI stolen, lost, used or disclosed without authority
- new [October 2017]
    - custodian must notify IPC if circumstances surrounding theft, loss, unauthorized use/disclosure meet prescribed requirements [significant breach]
    - custodian also must provide IPC with annual statistical report of breaches

Mandatory breach notification to IPC
ON *PHIPA*

IPC guidance provides more detail about when a breach must be reported

SEPTEMBER 2017

Reporting a Privacy Breach to the Commissioner

GUIDELINES FOR THE HEALTH SECTOR

To strengthen the privacy protection of personal health information, the Ontario government has amended the *Personal Health Information Protection Act* (the act). Under section 12(3) of the act and its related regulation, custodians must notify the Information and Privacy Commissioner of Ontario (the Commissioner) about certain privacy breaches. This law takes effect **October 1, 2017**.

As a custodian, you must report breaches to the Commissioner in seven categories described in the regulation and summarized below. The categories are not mutually exclusive; more than one can apply to a single privacy breach. If at least one of the situations applies, you must report it. The following is a summary—for the complete wording of the regulation, see the appendix at the end of this document.

It is important to remember that even if you do not need to notify the Commissioner, you have a separate duty to notify individuals whose privacy has been breached under section 12(2) of the act.

SITUATIONS WHERE YOU MUST NOTIFY THE COMMISSIONER OF A PRIVACY BREACH

1. Use or disclosure without authority

This category covers situations where the person committing the breach knew or ought to have known that their actions are not permitted either by the act or the responsible custodian. An example would be where a

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Mandatory breach notification to individuals/OPC
PIPEDA

- *PIPEDA* organizations [November 2018] must notify individuals and report to federal Commissioner any breach of security safeguards where reasonable to believe breach creates **real risk of significant harm** to the individual
- Organizations also must notify other organizations/government institutions of breach where notifying organization believes other organization/institution may be able to reduce risk of harm or mitigate that harm, or if any of the prescribed conditions are satisfied

Mandatory breach notification to individuals/OPC
PIPEDA

"significant harm" defined to include:

1. bodily harm
2. humiliation
3. damage to reputation or relationships
4. loss of employment, business or professional opportunities
5. financial loss
6. identity theft
7. negative effects on the credit record
8. damage to or loss of property

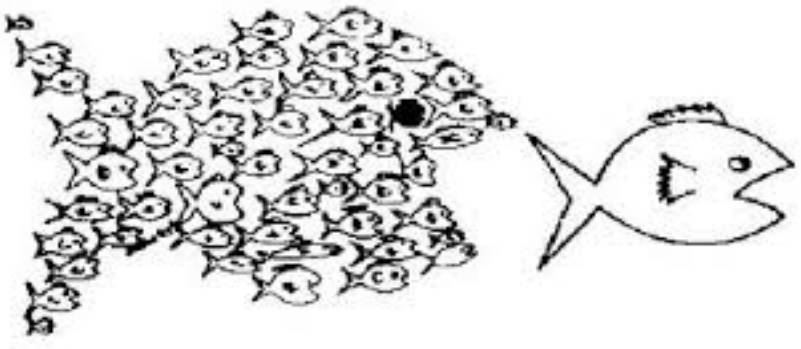
Mandatory breach notification to individuals/OPC
PIPEDA

Factors relevant to determining whether breach creates a real risk of significant harm include:

1. sensitivity of the personal information
2. probability that information has been/will be misused
3. any other prescribed factor

Privacy Class Action Update

- *Daniells v McClellan,* 2017 ONSC 3466 – Ontario health breach class action – hospital – employee snooping
- *Condon v Canada*, 2015 FCA 159 (Ministry of HR & Skills Development) – loss of PI – class action – settlement approval – lost device



Daniells v. McLellan, 2017 ONSC 3466

Background:

- Employee snooping at North Bay Regional Health Centre
- Hospital employee improperly accessed 5000 patients' PHI between 2004 and 2011, including representative plaintiff (Daniells)

Basis for Certification:

- Hospital consented to order certifying action but argued should be **subclasses** of plaintiffs based on patients' reactions to the news that PHI had been accessed & whether patients contacted hospital after learning of breach
- Court: no basis in fact to support assumption that a patient's failure to contact hospital = a reliable indicator of degree to which employee's actions affected that patient
- Also: punitive damages may be appropriate where "systematic failure" by institution in failing to prevent a data breach

Condon v. Canada, 2015 FCA 159

Background:

- Loss of external hard drive containing details of approx. 583,000 Canadian student loan recipients by Ministry of Human Resources and Skills Development (Nov 2012)
- Class action certified by FC and upheld on appeal in 2015

Motion for Settlement Approval:

- Parties agreed to settle for $17.5 million (capped at $60/class member)
- Feb 22 2018: Motion for settlement approval heard (decision on reserve); Likely to be instructive for privacy class action proceedings in future

Questions?

David Goodis
David.goodis@ipc.on.ca

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Claire Feltrin
cfeltrin@torkinmanes.com

Torkin Manes
Barristers & Solicitors