大成 DENTONS

CPD Bootcamp 2019
Critical Developments and Issues in Data

大成 DENTONS

Critical Developments and Issues in Data

With:
Chloe Snider
Karl Schober
Luca Lucarini

Agenda

- Critical Developments
  - Canada’s Digital Charter and PIPEDA’s Modernization
  - Mandatory breach reporting – 1 year anniversary
  - Class action developments

- Critical Issues
  - Third-party service providers
  - Privilege

Critical developments
Canada’s Digital Charter

Canada's Digital Charter - 10 Principles

1. **Universal Access:** All Canadians will have equal opportunity to participate in the digital world (including tools such as access, connectivity, literacy and skills).
2. **Safety and Security:** Canadians will be able to rely on the integrity, authenticity and security of the services they use and should feel safe online.
3. **Control and Consent:** Canadians will have control over what data they are sharing, who is using their personal data and for what purposes.
4. **Transparency, Portability and Interoperability:** Canadians will have clear and manageable access to their personal data and should be free to share or transfer it without undue burden.
5. **Open and Modern Digital Government:** Canadians will be able to access modern digital services from the Government of Canada, which are secure and simple to use.

Canada's Digital Charter – 10 Principles

6. **A Level Playing Field**: The Government of Canada will ensure fair competition in the online marketplace while protecting Canadian consumers from market abuses.

7. **Data and Digital for Good**: The Government of Canada will ensure the ethical use of data to create value, promote openness and improve the lives of people.

8. **Strong Democracy:** The Government of Canada will defend freedom of expression and protect against online threats and disinformation.

9. **Free from Hate and Violent Extremism:** Canadians can expect that digital platforms will not foster or disseminate hate, violent extremism or criminal content.

10. **Strong Enforcement and Real Accountability**: There will be clear, meaningful penalties for violations of the laws and regulations that support these principles.

Canada's Digital Charter – next steps

- Proposed initial focus of the government's Digital Charter based actions is on modernizing PIPEDA
- Digital Charter will likely have broader industry-specific effect through anticipated changes in the *Competition Act*, *Canada's anti-spam legislation* (CASL), *Telecommunications Act*, *Broadcasting Act* and *Radiocommunication Act*.

Example: As part of the Digital Charter "action plan", the government also proposes to modernize CASL and to review enhanced e-protection measures, where appropriate, to make sure CASL is clear and effective.

Critical developments
PIPEDA Modernization

PIPEDA Modernization

- Gov't released *Strengthening Privacy for the Digital Age* Discussion Paper on May 21, 2019 - proposals to modernize PIPEDA
- Seeks to create a modern regulatory privacy framework that:
  - is responsive and **agile**;
  - has an enhanced, reasoned **enforcement model**;
  - is **interoperable** with other jurisdictions; and
  - **balances** support for data-driven innovation with respect for individuals' privacy by providing users with meaningful control.
- PIPEDA modernization plan is focused on four areas:
  1. Enhancing **individuals' control**
  2. Enabling **innovation**
  3. Enhancing **enforcement**
  4. **Clarifying** PIPEDA

1. Enhancing Individuals' Control

- Provide more meaningful control, transparency and consumer choice by:
  - requiring specific, **standardized, plain-language** information on use of PI, the 3rd parties it's shared with, and prohibiting bundling of consent into a contract;
  - incorporating **alternative grounds to consent** (similar to GDPR's legitimate interests basis for processing PI);
  - introducing the **right to data mobility**;
  - requiring enhanced transparency of business practices via **"demonstrable accountability",** including in the context of transborder data flow;
  - introducing **algorithmic transparency** requirements for automated decision-making;
  - adding a **definition of de-identified information** (and potentially pseudonymized data), plus an exception to consent for its use/disclosure for certain prescribed purposes and penalties for re-identification; and
  - introducing the **right to request deletion of PI** and mandating defined retention periods but **not including the right to be forgotten** (aka de-indexing) because the matter is before the Federal Court of Canada.

2. Enabling Innovation

- To balance data-driven innovation with the need to ensure businesses are transparent, accountable and appropriately use data, the government proposes:
  - using **data trusts** as a way to enable responsible innovation and data use; and
  - the creation of **codes of practice, accreditation/certification schemes and standards**, validated through recognition by the OPC.

3. Enhancing Enforcement

- Enhancing the OPC's enforcement and oversight abilities by providing it with **order making powers** in the form of cessation and record preserving orders
- Proposals to **extend the existing fine regime** to other areas of PIPEDA, and **substantially increasing** the range fines

4. Clarifying PIPEDA

- The proposed reforms also aim to clarify the application of PIPEDA (and thereby enhance accountability), including by **extending PIPEDA's applications to certain non-commercial data collection** activities.
- In an effort to address new business models, which do not fit in the traditional "controller-processor" framework, the government also plans to **update and clarify PIPEDA's applicability**, including in the context of transborder data flows.

Timing:

- Consultation period anticipated, but not yet announced
- Modernization necessary, in part to ensure Canada maintains its "adequacy" standing with the EU, which is up for review as early as 2020.

Critical developments
Competition Call Out

Competition Bureau “Call Out”

- On September 9, 2019, the Competition Bureau announced it was is “seeking information from market participants about conduct in the digital economy that may be harmful to competition.”

Competition Bureau “Call Out”

- **Key question:** Have certain core digital markets, like online search, social media, display advertising and online marketplaces, become increasingly concentrated, to the detriment of consumers and businesses.
- The Call Out paper explores two potential, and possibly complementary, explanations:
  - **Tipping:** Digital markets may ‘tip’ to a dominant firm: characteristics of certain digital markets may favour the emergence of a single winner or a small group of winners
  - **Anti-competitive conduct:** Leading firms may not have achieved success by outperforming their competitors, but rather by executing anti-competitive strategies that target existing or potential rivals

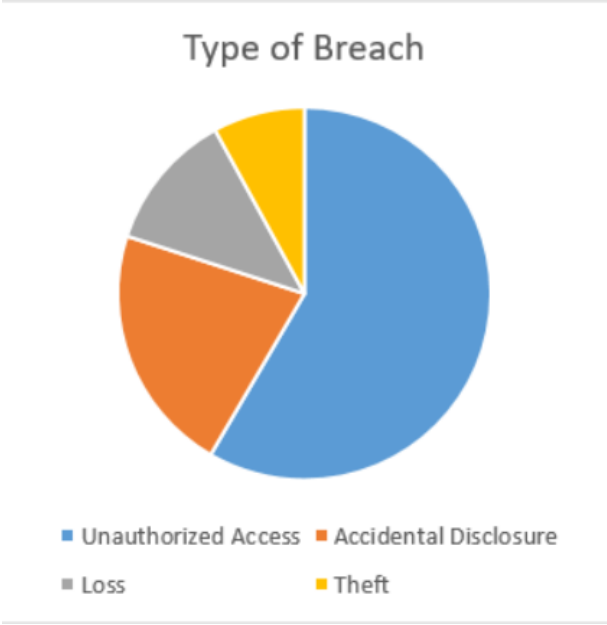
Critical Developments

Mandatory breach reporting requirements – 1 year later

The numbers

- The Office of the Privacy Commissioner has received **680** breach reports since November 1, 2018
  - **Six times** the number received in the same period the year before
  - Over **28 million** affected individuals

Type of incident	Total breach reports
Accidental disclosure	147
Loss	82
Theft	54
Unauthorized access	397
Grand Total	**680**



https://www.priv.gc.ca/en/blog/20191031/

Trends

- Significant rise in reports of breaches affecting a small number of individuals
- Employee snooping and social engineering hacks driving unauthorized access
  - ¼ of all incidents involved social engineering hacks like phishing and impersonation

See the Office of the Privacy Commissioner's **blog** for more information.

Critical issues

Breach notification and reporting: best practices

Best Practices

1. Be direct when describing the “circumstances of the breach”.

Keep it simple and understandable e.g., “Criminals illegally accessed our computer systems and stole some customer information” or “We inadvertently sent you information intended for another person”. No one needs to know you recently became vulnerable to an SQL injection attack that made it possible to execute malicious SQL statements controlling a database server behind a web application.

- Inside job? Be careful whether/how you disclose this as you could set yourself up for a vicarious liability claim.

Best Practices

2. Be certain about the types of information affected.

Most breach notification laws require you to identify the types of information affected. Try and be specific without bogging the reader down in details.

- Be ~~100%~~ ~~150%~~ **200%** certain before you commit to a list of data elements!
- If you are not 200% certain (or if different data elements were affected for each individual), use categories and weasel words (e.g., “financial information, such as the name of your local bank branch, your account number…).
- Highlight important information that **wasn’t affected** e.g., “At this time, we have no evidence that payment card information was affected.”

Best Practices

3. The number you choose will be the number you live with forever.

The moment you make a number public, that will be your line in the sand and the reference point for the incident.

- Play the numbers game: Avoid committing to any particular number unless you are required to say something. Use approximate numbers where you have some reasonably firm idea of the numbers (e.g., “At this time, we believe the information of approximately X individuals may be affected” or “We believe that fewer than 7,000 of our Canadian customers have been affected”).

- Required to provide a number? Consider not doing so where at all possible, and simply go with “we are not sure at this time”.

Critical Developments
Privacy Class Action Update

Certification cases – Developing law

- Proliferation of privacy class actions

- Courts have allowed privacy class actions to proceed even where there is a question as to whether there is a reasonable cause of action:

  > The tort of intrusion upon seclusion *"is a relatively new tort and it should be allowed to develop through full decisions."*

Tucci v. Peoples Trust Company, 2017 BCSC 1525

Particular areas of risk

- Third party hacks
- Vicarious liability
- Lost devices
- Use without consent
- Vendor problems

External malicious actors

- *Kaplan v. Casino Rama Services Inc. (*anonymous hacker accessed the Casino's computer system and stole personal information relating to customers, employees and suppliers; after ransom demands unmet, the hacker posted the stolen data of 11,000 people on the internet)
- *Lozanski v. Home Depot (*payment card system was hacked by criminal intruders using custom-built malware to clandestinely breach Home Depot's computer system)
- *Tucci v. Peoples Trust Company (*cybercriminals gained unauthorized access to the defendant's databases and stole website users' personal information; unsolicited text messages were sent to users purporting to be from the defendant, as part of attempt to solicit money or information)

Vicarious liability a concern…

- *Ari v. Insurance Corporation of British Columbia*
  - Privacy breach by an **employee**. Judge certified a class proceeding against ICBC, as the vicarious liability claim was not bound to fail.

- *WM Morrison Supermakets PLC v. Various Claimants*
  - English Court of Appeal upheld lower court decision that Morrison was legally responsible for the data leak caused by the deliberate malicious actions of a **disgruntled employee**.
  - Morrison has been granted leave to appeal to the Supreme Court in first UK class-action case over a data leak.

- *Broutzas v. Rouge Valley Health System*

Lost Devices

- Loss of external hard drive *(Condon v. Canada*)
- Other examples might include lost or stolen laptops

Use without consent

- Use of class members' names and images without their knowledge or consent in an advertising program (*Douez v. Facebook)*
- Use of personal information of its data service customers for its own marketing initiative (*Tocco v. Bell Mobility)*
- Installation of software on computers, which had a security defect that would permit a hacker to obtain the user's private information, and that displays adds and affects computer performance (*Bennett v. Lenovo*)

Is there any good news?

- *Kaplan v. Casino Rama*, 2019 ONSC 2025
  - Casino Rama targeted in cyber-attack in November 2016. Hacker obtained personal information relating to customers, employees, and suppliers.
  - The casino refused a ransom demand and material posted online.
  - No provable losses, insufficient common issues among proposed class members. Motion for certification dismissed.

- *Broutzas v. Rouge Valley Health System,* 2018 ONSC 6315
  - Names of women who had just given birth were provided by nurses to sales persons for RRSPs.
  - No compensable privacy invasion.

AND…

- No decision on the merits in any privacy class action.

- In the meantime, there have been several settlements…
  - Terms depend on the type of information involved, the types of out of pocket expenses that may have been incurred, and what other harm may have incurred… as well as on defendant conduct.

Settlements

- Compensation for losses resulting from fraud or identity theft
  - Example: non-reversionary settlement fund for the documented claims of class members whose payment card information and/or email address was compromised, with payments to be distributed on *pro rata* basis if claims exceed fund
- Cash payments for other proven out-of-pocket expenses (payment of credit monitoring, time spent addressing the situation)
  - Example: Class members with documented losses, which may include time spent remedying issues relating to the data breach, may apply for reimbursement for time remedying issues (up to five hours at $15 per hour) through settlement administrator
- Credit monitoring
- Payment for costs of notice and administration
- Costs

Notice and Credit Monitoring

- What you do can be important to what the court perceives

- *Lozanski v The Home Depot*, Inc., 2016 ONSC 5447
  - Settlement approval case
  - Court looked at defendant's conduct – it "responded in a responsible, prompt, generous, and exemplary fashion to the criminal acts perpetrated on it by the computer hackers":
    - April-September 2014: payment card system was hacked by outside intruders
    - September 2014: provided notice to the federal, Alberta, BC and Quebec privacy commissioners (none of which found any breach of Canada's privacy laws and all of which closed their files)
    - September 2014: issued a press release and sent over 500,000 emails to customers to notify them that some customers' payment card information might have been compromised
    - November 2014: further notice regarding email accounts
    - Offered free credit monitoring and identity theft insurance
    - Spent several millions of dollars

What you can do

- Information technology security policy
- Data governance framework
- Cybersecurity incident response policy and checklist
- Regularly train employees on all policies
- Cybersecurity insurance policy
- Speak with Karl and Luca!

Critical issues
Third-party service providers

Third parties

Weakest link or most likely target?

- Prevalence of third party service providers the source of the data incident
- Continuous increase of malicious attacks to outsourced services

Obligations with third-parties

Principle 4.1.3 of PIPEDA

- An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing.
- PIPEDA requires organizations to use contractual or other means when using third-party service providers, to ensure a comparable level of protection of personal information.

Evolution of requirements

- Contracts in place with third-party service providers that provide guarantees of confidentiality and security of personal information and allow for oversight, monitoring, and auditing of the services being provided, as well as provisions to address sub-contracting.

Third party contracting

Core terms – check list

- ✓Defined Terms
- ✓Compliance
- ✓Ownership of Personal Information
- ✓Return of Personal Information
- ✓Restrictions relating to use of Personal Information
- ✓Restrictions relating to storage locations
- ✓Restrictions on subcontracting
- ✓Security administration
- ✓Improvements
- ✓Assurances / Audit Rights
- ✓Obligations with respect to Security Incidents
- ✓Obligations with respect to Access Requests
- ✓Obligations with respect to Judicial / Governmental Requests
- ✓Indemnification

Third party contracting
Non-negotiable

- Compliance with laws

Vendor represents, warrants, and covenants that it:

a) does and will comply with all Privacy Laws applicable to the Personal Information; and

b) has developed and implemented, and will maintain and monitor, a written and comprehensive information security program in compliance with this Agreement and applicable Privacy Laws; and

c) will certify, in writing, its compliance with the foregoing annually upon request from Company A.

- Security administration

Vendor shall and shall require its subcontractors to establish and maintain administrative, technical and physical safeguards to protect the security, integrity, confidentiality and availability of the Personal Information, including to protect the Personal Information against any anticipated threats or hazards and to protect against any loss of or unauthorized or unlawful access to, use of, or disclosure of the Personal Information.

Third party contracting

Non-negotiable – data incidents

*Vendor shall notify Company A promptly of a Security Incident and, in any case, within 24 hours of becoming aware of the Security Incident ("**Notification**"). In the event of a Notification of a Security Incident, Vendor shall and shall cause its Authorized Users and subcontractors to:*

a) fully cooperate with Company A and its third-party advisors in investigating and resolving the vulnerability giving rise to the Security Incident;

b) provide Company A with information regarding: (i) the Personal Information that is the subject of the Security Incident; (ii) the names and contact information (if known) of individuals who may be affected by the Security Incident; (iii) the steps taken to contain the Security Incident and to mitigate any harm to individuals as a result of the Security Incident; and (iv) any remedial actions taken to prevent further occurrences of the Security Incident;

c) fully cooperate with Company A with respect to: (i) reporting to, and responding to all inquiries from, the Security Incident to a Privacy Commissioner and any other governmental authority with jurisdiction; (ii) providing notification to individuals affected by the Security Incident; and (iii) providing notification or reports to other third parties who may assist in mitigating the possible harm to affected individuals.

Third party contracting

Non-negotiable – data incidents continued

The decision-maker should be clear:

- *Unless otherwise required by applicable Privacy Laws or other laws, the decision whether to make a report to a Privacy Commissioner and any other governmental authority or to notify individuals and third parties, and the content of any such reports and notifications shall be solely at the discretion and direction of Company A.*

Third party contracting

Common pushback - Improvements

Starting point

a) *If Vendor proposes to materially modify the process, method or means by which the Personal Information is stored, accessed or otherwise transmitted or handled, Vendor shall provide Company A at least sixty (60) days prior written notice. Company A shall have the right, acting reasonably, to determine if the modifications represent unacceptable risks to Personal Information and to prohibit Vendor from implementing such material modification until such time as the risks can be mitigated or an alternate provider of the services under the Agreement can be found.*

- Fallbacks

a) *Vendor shall provide Company A with written notice if Vendor materially modifies the process, method or means by which Personal Information is stored, accessed or otherwise transmitted or handled. Vendor's notice shall be no later than five (5) business days prior to the implementation of such modifications.*

Third party contracting

Common pushback – assurances / audit rights

- Starting point

Company A may, on reasonable prior notice to Vendor, visit and inspect any location from which Vendor accesses, uses or stores Personal Information. In connection with the inspection, Vendor shall and shall cause its subcontractors to:

a) make available for examination all applicable policies and procedures governing the operation of any location or equipment used to access, use or store Personal Information;

b) make available representatives of Vendor and any subcontractors to answer questions relating to the policies, procedures or equipment, subject only to limitations required for Vendor to comply with applicable laws or contractual obligations of confidentiality to third parties; and

c) permit and provide reasonable assistance in auditing, both physically and electronically, compliance by Vendor.

- Fallback

At least annually, Vendor shall obtain from a third party assessor, and shall provide to Company A, a certificate of compliance with the following standards: [insert appropriate standard ISO 27001, ISO 27018, SAE16 SOC1 Type II, SOC2 Type II]

Third-party contracting

Negotiable

- Indemnification

Monitoring third parties

- "*An organization cannot just enter into an agreement and then coast*" – the Office of the Privacy Commissioner of Canada

- Vendor Management Program
  - Establish internal policies and procedures in line with security requirements and acceptable risk
  - Vetting vendors
  - Privacy and / or security impact assessments
  - Audit rights
  - Renewal of agreements

Critical issues
Privilege

Best Practices: Privilege

Understand privilege.

The privacy commissioners have limited ability to obtain privileged information. Understand privilege and use it wisely and strategically.

(Privacy Commissioner) v. Blood Tribe Department of Health, 2008 SCC 44
Alberta (Information and Privacy Commissioner) v. University of Calgary, 2016 SCC 53

- Do not reference privileged materials in your letters/submissions to regulators! All you are doing is providing a roadmap for document requests by: (a) the regulator/other regulators; (b) plaintiffs' counsel.

- Or affidavits! You may inadvertently waive privilege.

Kaplan v. Casino Rama Services Inc., 2018 ONSC 3545

Best Practices: Privilege

Assume everything you provide to a regulator could be made public.

The privacy commissioners have a broad power to make things public, as well as being subject to *Access to Information*/*Freedom of Information* legislation.

- Assume that whatever you give to the OPC or its provincial counterparts can and will be made public. Draft accordingly.

- Assume that whatever you give to the OPC or its provincial counterparts will find its way into the hands of plaintiffs/plaintiffs' class action counsel and/or the media.

Best Practices: Privilege

- All of your internal investigations, forensic reports are discoverable *unless* you protect them with privilege.
- Lawyers who have experience in this area have literally seen hundreds of data incidents. We know what to expect, and we have relationships with the regulators. We know what the regulators will pounce on.
- Anything you say publically can (and will) be used against you in a court of law. Seriously. It will.
  - Your customer notices, your public statements, anything you file with the OPC, news releases, etc., will all find their way into plaintiffs' litigation materials if you get sued. Words matter. (e.g., we are currently litigating whether "affected" as used in a press release means people actually affected by the incident, or people potentially affected. The outcome will mean a difference of several million dollars).

Takeaways

- Be prepared for legislative changes
- Are you over reporting?
- Consider the short (reporting) and long (class action) game.
- Review vendor management program.
- Privilege!

Thank you

Chloe Snider
Partner
D +416 863 4674
E chloe.snider@dentons.com

Karl Schober
Senior Associate
D +416 863 4483
E karl.schober@dentons.com

Luca Lucarini
Associate
D +416 863 4735
E luca.lucarini@dentons.com