DENTONS

5TH ANNUAL DENTONS DATA SUMMIT

Privacy law and beyond: Navigating today's challenges and trends

September 27, 2023
12 - 4 p.m. ET

Grow | Protect | Operate | Finance

Around the world privacy update
(India, China and North Korea)

Speakers

- Ketan Mukhija, Partner (New Delhi)
- Pascal Jiang, Partner (Shanghai)
- Christina Jiwon Park, Partner (Seoul)

DENTONS

Thank you

Ketan Mukhija
Partner (New Delhi)
+91 11 4651 1000
ketan.mukhija@dentonslinklegal.com

Pascal Jiang
Partner (Shanghai)
021-20283815
pascal.jiang@dentons.cn

Christina Jiwon Park
Partner (Seoul)
+82 2 2262 6229
christina.j.park@dentons.com

Interactive – Two truths and a lie
(About Privacy game)

Speakers

- Rachel Macklin, Associate (Edmonton)
- Melika Mostowfi, Associate (Calgary)
- Jen Rees-Jones, Senior Manager, Privacy and Data (Toronto)
- Ana Qarri, Associate (Toronto)

DENTONS

Thank you

Rachel Macklin
Associate (Edmonton)
+1 780 423 7164
rachel.macklin@dentons.com

Melika Mostowfi
Associate (Calgary)
+1 403 268 7011
melika.mostowfi@dentons.com

Jen Rees-Jones
Senior Manager (Toronto)
+1 416 361 2379
jen.rees-jones@dentons.com

Ana Qarri
Associate (Toronto)
+1 416 863 4496
ana.qarri@dentons.com

Litigation update

Speakers

- Kelly Osaka, Partner (Calgary)
- Chloe Snider, Partner (Toronto)

Litigation Update

Privacy Class Actions Trends

Certification

- Courts dismiss three class action appeals arising out of cyberattacks:
  Breach of the defendants' systems affecting thousands of customers.
  Owsiniak v. Equifax Canada Co
  Winder v. Marriott International Inc
  Obodo v. Trans Union of Canada
- ***Setoguchi v Uber*** – Alberta Court of Appeal upheld the dismissal of certification; in the absence of any opportunity for compensable class-wide harm, class proceeding not the preferable procedure.
- ***Stewart v. Demme*** – Ontario Divisional Court denied certification as the threshold for intrusion upon seclusion was not met
- ***Chow v. Facebook, Inc*** – no basis in fact for all allegations

Litigation Update

Privacy Class Actions Trends

Settlement

- Very small per capita value of settlements

Decisions on the Merits

- ***Lamoureux v. OCRCVM*** – Québec Court of Appeal confirms dismissal of privacy class action on the merits
- ***Douez v. Facebook, Inc*** – BC summary judgment holding that defendant liable under BC privacy legislation; referring damages issues to full trial

Litigation Update

Privacy Class Actions Trends

Vicarious Liability

- BC Court of Appeal confirms grounds for *imposing vicarious liability* on an employer as a result of a rogue employee's breach of privacy – *Ari v. ICBC*
  - No need for the employer to foresee the specific wrong that occurs for vicarious liability to be imposed – sufficient that ICBC *knew that the personal information available to the rogue employee was vulnerable to abuse*

Consent

- OPC found that a hardware retailer did not obtain *valid meaningful consent* to share purchase information with a third party to measure the effectiveness of an ad campaign.
- BC Supreme Court found that a social media company *failed to obtain either direct or implied consent* for the use of users' names and profile photos in advertisements

DENTONS

Thank you

Kelly Osaka
Partner (Calgary)
+1 403 268 3017
kelly.osaka@dentons.com

Chloe A. Snider
Partner (Toronto)
+1 416 863 4674
chloe.snider@dentons.com

Show me the money:

Understanding enforcement powers/process, factors driving the imposition of fines/penalties, and how organizations can build due diligence programs to reduce penalties

Speaker

- Kirsten Thompson, Partner, National Practice Group Lead, Privacy and Cybersecurity (Toronto)

Agenda

1. **Penalty provision of the Act**
2. **What are AMPs? What are fines?**
3. **Which violations attract AMPs and/or fines?**
4. **AMPs**
   - Framework
   - Process
   - How does the CAI determine whether to impose a penalty?
   - How does the CAI determine the amount of the penalty?
5. **Fines**
   - When will the CAI favour criminal prosecution
   - Sentencing factors
6. **Undertakings**
7. **Reducing your risk**

1. Penalty provisions of the Act

Three different types of mechanisms to enforce compliance under the Private Sector Act: (1) administrative monetary penalties, (2) penal offences, and (3) a private right of action (punitive damages).

1. **Administrative monetary penalty** (“**AMP**”)
    - administered by Québec’s privacy regulator, the Commission d’accès à l’information (“**CAI**”)
    - a “person designated by the Commission, but who is not a member of any of its divisions” (“**Designated Person**”) will have the power to impose AMPs on organizations that contravene the law of up to $10 million or 2% of worldwide turnover.
2. **Fines/penal proceedings**
    - offences for which the CAI may institute penal proceedings and which may be sanctioned by a fine of up to $25 million or 4% of worldwide turnover (imposed by the Court of Québec).
3. **Private right of action/punitive damages**
    - individuals can sue!

2. What are AMPs? Fines?

AMPs

- **Civil penalty** imposed by a regulator for a contravention of an Act, regulation or by-law.
- Issued upon discovery of an unlawful event, and is **due and payable** subject only to any rights of review that may be available under the AMP's implementing scheme.
- It is **regulatory in nature**, rather than criminal, and is intended to secure compliance with a regulatory scheme.
- It is **not a punishment**, so fewer procedural protections (including the protections provided under s.11 of the Charter e.g., right to be presumed innocent, right to informed of the specific offence, etc.).
- However, normal standards of **judicial review apply.**
- Administrative Tribunal of Quebec has recognized that a person can bring forward the "reasonable, prudent and diligent person" **defence** that exists in civil law against the imposition of AMPs.

2. What are AMPs? Fines?

Fines/Penal sanction

- Any pecuniary penalty or pecuniary forfeiture or pecuniary compensation **payable under a conviction**.
- Fines are **intended to punish** offenders.
- Requires a pleading or finding of **guilt in a court proceeding**.
- Where a penalty's purpose or effect is punitive, this will trigger Charter rights.

- Penalties can be so high they may become punitive, but the mere amount of a penalty won't be enough to make it so.
  - In the *Guindon* case, the Supreme Court articulated a balancing test to determine whether an outcome is punitive: "Whether this is the case is assessed by looking at considerations such as the magnitude of the fine, to whom it is paid, whether its magnitude is determined by regulatory considerations rather than principles of criminal sentencing, and whether stigma is associated with the penalty."

3. Which violations attract AMPs and/or fines?

Violation	AMPs	Fines	Punitive damages
Collects, uses, discloses, retains or destroys personal information in contravention of the Act	X	X	X
Fails to adequately inform affected individuals in accordance with s. 7 and s. 8) (e.g., failure to have an adequate privacy policy/notice)	X		X
Fails to take appropriate security measures to ensure the protection of personal information in accordance with s. 10	X	X	X
Fails to report a confidentiality incident presenting a risk of serious harm to the CAI or to the persons concerned	X	X	X
Failure to inform the individual affected by a decision based on an automated processing of personal information or provide an opportunity submit observations	X		X
Identifies or attempts to identify a natural person from de-identified information without the authorization of the person holding the information or from anonymized information		X	X
Impede the progress of an investigation, an inspection or the hearing of an application by the CAI		X	
Take a reprisal against an individual on the ground that the individual has, in good faith, filed a complaint with the CAI or cooperated in an investigation		X	X
Failure to comply with a request for production of documents issued by CAI within the specified time		X	
Fail to comply with an order from the CAI		X	

4. AMPs

Framework

- As required by the Act, the CAI has developed a general framework ("**Framework**") for the application of AMPs specifying:
  - The objectives pursued by the sanctions;
  - The criteria to determine the decision to impose a penalty when a violation is found and the determination of the amount of the penalty;
  - The circumstances in which the criminal remedy is prioritized;
  - Other modalities for the imposition of sanctions.
- Based on the above, the Framework specifies that the CAI will seek two objectives in imposing AMPs:

  (1) encourage the person in default to take rapid corrective measures; and

  (2) dissuade recidivism.

4. AMPs

Process

Notice of Compliance

- CAI issues Notice of Compliance to encourage person in default to take immediate remedial action (s.90.3)
- CAI must give person in default the opportunity to submit observations
- No timelines provided for response before CAI can issue a Notice of Claim

Notice of Claim

- The CAI imposes AMPs through issuance of a Notice of Claim (s. 90.5)
- The person in default has the right to request a review of the decision by the oversight division of the CAI (s. 90.5)
- The right of review must be exercised within 30 days of notification of the Notice of Claim

Decision on review

- Reviewing decisions may confirm, reverse or modify original decision in Notice of Claim (s. 90.7)
- Person in default has the right to contest the decision in Court of Quebec (s. 90.8)
- Right must be exercised within 30 days of notification of the reviewed decision (s. 90.9)

NOTE: the CAI has a **two years** from the date of a violation to impose any AMPs (s. 90.10).

4. AMPs

How does the CAI whether to impose a penalty?

The Designated Person must, in deciding **whether** to impose a sanction, consider the following criteria (s.90.2(2)):

(a) the **nature, seriousness, repetitiveness** and **duration** of the violation;

(b) the **sensitivity** of the personal information concerned by the violation;

(c) the **number of persons affected** by the failure and the **risk of serious harm** to which they are exposed;

(d) the measures taken by the person in default to remedy the violation or **mitigate its consequences**;

(e) the **degree of cooperation** provided to the Commission to remedy the violation or mitigate its consequences; and

(f) the **compensation offered** by the person in default, as restitution, to every person affected by the violation;

(g) the **ability to pay** of the person in default, given such considerations as the person's assets, turnover and revenues.

4. AMPs

How does the CAI determine the amount?

The Designated Person has discretionary power as to the amount (up to the maximum). To determine the appropriate and proportional amount of the penalty, the Designated Person applies a 2-step method.

Step 1: Categorization

Categorization of the breach according to the criteria below determines the base amount, depending on who (person or organization) committed the breach.

- The **nature** of the breach;
- The objective **seriousness** of the breach;
- The **repetitive** nature and **duration** of the breach;
- The **sensitivity** of the personal information affected by the breach;
- The **number** of people affected by the breach;
- The **risk of serious harm** to which these people are exposed;

4. AMPs

How does the CAI determine the amount?

Categories	Criteria	Base Amount (Person)	Base Amount (Organization)
A	In general, minor administrative failings with no or only minor consequences.	$500	$1,000
B	Moderate non-compliance with the rules governing the protection of personal information, the apprehended consequence of which is moderate.	$1,500	$4,000
C	Serious breach which, because of its nature, is prejudicial to the general objectives of the protection of personal information, the apprehended consequence of which is major.	$3,000	$8,000
D	Very serious breach of the integrity of the protection of personal information, the apprehended consequence of which is major, real and/or irreparable.	$5,000	$15,000

4. AMPs

How does the CAI determine the amount?

Step 2: Aggravating/Mitigating Factors

This basic amount from Step 1 is then increased or reduced according to certain aggravating and mitigating factors, including the following:

- The **repetitive** nature and **duration** of the violation;
- The **sensitivity** of the personal information affected by the violation;
- The **number** of people affected by the violation;
- The **risk of serious harm** to which these people are exposed;
- Measures taken by the defaulting party to remedy the violation or **mitigate** its consequences;
- The degree of **cooperation** offered to the CAI to remedy the violation or mitigate its consequences;
- **Compensation offered** by the defaulting party to any person affected by the violation;
- The person in default's **ability to pay**, taking into account his or her assets, sales or income.

The amount determined by the designated person may not exceed the maximum amount provided by the Act, which is $50,000 for an individual and, for an organization, $10 million or 2% of worldwide turnover for the previous fiscal year, whichever is higher.

5. Fines

When will the CAI favour criminal prosecution?

The CAI will favour criminal prosecution where:

- The actual or apprehended **consequences of the offence are serious or very serious**, particularly if there is evidence of significant damage or a high risk of significant damage:
  - To the privacy of the people affected;
  - To vulnerable customers/persons;
  - In light of the sensitivity of the personal information concerned;
- **Failure to comply** with an order of the CAI;
- **Adequate measures have not been taken** to remedy the violation despite the imposition of one or more AMPs or the exercise of other administrative measures;
- The person in default has acted **intentionally, negligently or recklessly**;
- A CAI investigation or inspection has been **obstructed**, or the organization has provided **false or inaccurate information** or has **failed to provide information** required by the CAI;
- **Several breaches or violations** of the Act have been committed by the same organization or are recurrent over time.

A member of the CIA's surveillance section decides whether to institute criminal proceedings, which are initiated by a Statement of Offence.

5. Fines

Sentencing factors

Where an organization is found guilty, the judge must consider the following in determining the amount of the fine (s. 92.3):

- The **nature, gravity, repetitive nature** and **duration** of the offence;
- The **sensitivity** of the personal information to which the breach relates;
- Whether the offender acted **intentionally or was negligent or reckless**;
- The **foreseeability of the violation** or the failure to act on recommendations or warnings to prevent it;
- The offender's **attempts to conceal the offence** or the offender's **failure to attempt to mitigate** its consequences;
- The fact that the **offender failed to take reasonable steps** to prevent the commission of the offence;
- The fact that the offender, by committing the offence or failing to take measures to prevent its commission**, increased or intended to increase revenues or reduce expenses;**
- The **number** of persons affected by the infringement and the **risk of harm** to which they are exposed.

NOTE: In the event of a **subsequent offence**, the Act provides that the fines are **doubled.**

NOTE: The CAI has **five years** from the commission of the offence to initiate criminal proceedings.

NOTE: Directors and officers may be found guilty if they ordered, authorized, or consented to the act or omission constituting the offence (s. 93).

6. Undertakings

Why/why not?

- Undertakings (U/T) are available for AMPs (also available for punitive damages; not available for fines)
- Following a violation of the Act for which AMPs are available (see s. 90.1), a person may, at any time, undertake to the Commission to take the necessary measures to remedy the breach or mitigate its consequences.
- The U/T must set out the acts and omissions that constitute the violation(s) and the provisions in question.
- The U/T may also include any conditions the CAI deems necessary, and include an obligation to pay a sum of money.
- If the U/T is accepted by the CAI and complied with, the person operating the business may not be subject to an AMP in respect of the acts or omissions referred to in the U/T.

Pros	Cons
May avoid having to pay an “AMP”	Payment could still be part of U/T
No AMPs for those violations in the U/T	Could still be subject to AMPs for anything not identified in U/T or new acts/omissions (or failure to comply with U/T)
Could end the matter	More likely a term of U/T will include ongoing supervision
Could thwart punitive damages (class action?)	--

6. Reducing your risk

- Comply.
- Tidy up the Triple Jeopardy categories.
  - Collects, uses, discloses, retains or destroys personal information in contravention of the Act
  - Fails to take appropriate security measures to ensure the protection of personal information in accordance with s. 10 (section 10: security measures necessary to ensure the protection of the personal information collected, used, communicated, kept or destroyed and that are reasonable given the sensitivity of the information, the purposes for which it is to be used, the quantity and distribution of the information and the medium on which it is stored.)
  - Fails to report a confidentiality incident presenting a risk of serious harm to the CAI or to the persons concerned
- Reduce the personal information you have (esp. sensitive information).
- Review your processes at least annually (self-audit, or have an outside party audit you).
  - Pro-tip: you may want to use a law firm to preserve privilege over findings).
- Actively monitor your privacy inbox/complaints process to fix things quickly and have a robust internal investigation process.

DENTONS

Thank you

Kirsten Thompson
Partner, National Practice Group Lead, Privacy and Cybersecurity (Toronto)
+1 416 863 4362
kirsten.thompson@dentons.com

Vendor service agreement checklist:

Both controllers and processors have new obligations and new risks

Speaker

- Danielle Dudelzak, Associate (Calgary)

DENTONS

Thank you

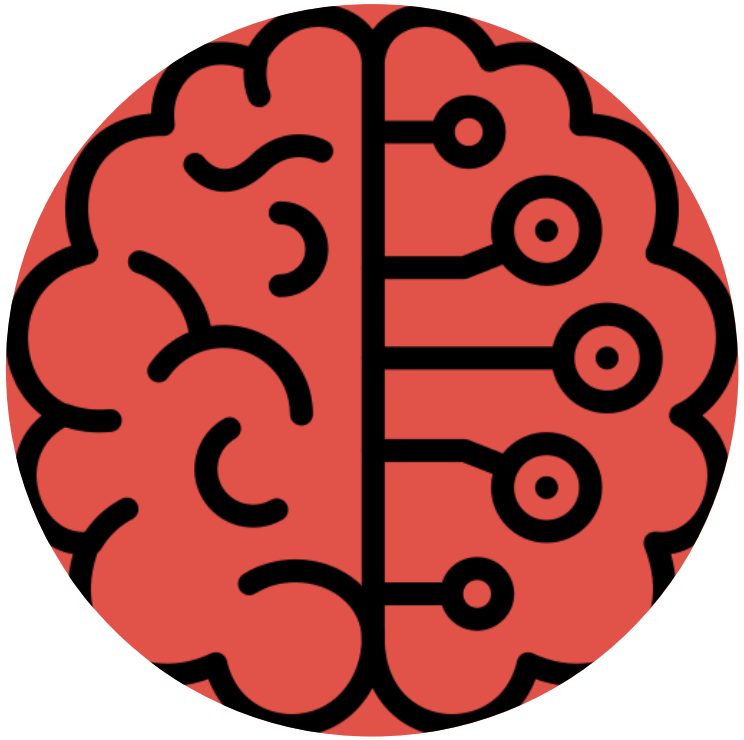
Danielle Dudelzak
Associate (Calgary)
+1 403 268 6312
danielle.dudelzak@dentons.com

Using de-identification and anonymization to unlock new uses of personal information – Can you? Should you?

Speaker

- Luca Lucarini, Associate (Toronto)

Use cases



*Information will be about an identifiable individual where there is a **serious possibility** that an individual could be identified through the use of that information, either alone or in combination with other information.*

- *Gordon v Canada*, 2008 FC 258

Spectrum of identifiability

	Explicitly Personal	Potentially Identifiable	Pseudonymous	De-identified	Anonymized
Direct Identifiers	Intact	Partially Masked	Eliminated / Transformed	Eliminated / Transformed	Eliminated / Transformed (Irreversible)
Indirect Identifiers	Intact	Intact	Intact	Eliminated / Transformed	Eliminated / Transformed (Irreversible)

De-identification techniques

- ***Suppression:*** Removing data prior to dissemination.

- ***Blurring***: Reducing precision of data by combining one or more data elements (e.g. aggregation / generalization).

- ***Masking:*** Replacing one data element with either a random or made-up value, or with another value in the data set (e.g. perturbation / encryption / noise and differential privacy).

Privacy legislation

Personal Information and Protection of Electronic Documents Act (**PIPEDA**)

- No concept of “de-identified” or “anonymized” information.

- Office of the Privacy Commissioner of Canada (**OPC**): Personal information that has been **de-identified** does not constitute **anonymous information** if there is a **serious possibility** that someone could link the de-identified data back to an identifiable individual.

Privacy legislation

Bill C-27: *Consumer Privacy Protection Act* (**CPPA**)

- **De-identify:** “To modify personal information so that an individual cannot be directly identified from it, through a risk of the individual being identified remains.”
- **Anonymize:** To “irreversibly and permanently modify personal information, in accordance with generally accepted best practices, to ensure that no individual can be identified from the information, whether directly or indirectly, by any means.”

Privacy legislation

Bill C-27: *Consumer Privacy Protection Act* (**CPPA**)

- May use personal information without knowledge or consent to de-identify the personal information, and then use that de-identified information for **internal research, analysis and development purposes**.
- Must ensure that “technical and administrative measures applied to the information are **proportionate** to the **purpose** for which the information is de-identified and the **sensitivity** of the personal information.”

Privacy legislation

Quebec: **Law 25**

- Personal information initially collected for one purpose may be used **within an organization**, without consent, for **study, research or the production of statistics** if the information is **de-identified.**
- Personal information is de-identified if “it no longer allows the person concerned to be **directly identified**”.
- Personal information is **anonymized** when “it is at all times reasonable to expect in the circumstances that it **irreversibly** no longer allows the person to be identified **directly** or **indirectly**.”

Risks

- Unauthorized **use** or **disclosure** contrary to privacy legislation.
- Failure to provide **notice** of purposes for collection.
- Information being subject to **data breaches** – class action risk as well as breach of security safeguards required by legislation.
- Violation of prohibition against **re-identification.**

Risks

- Joint investigation of OPC, BC Privacy Commissioner, Alberta Privacy Commissioner, Commission d'accès à l'information du Québec into franchisor's collection, use and disclosure of geolocation data (June 2022)
- Franchisor deployed app provided by vendor that collected granular location data.
- Service agreement authorized vendor to use data "to improve and enhance the Services and for other development, diagnostic and corrective purposes **in connection with** the Services and **other Company offerings**" and that the vendor could disclose "such data solely in aggregate or other de-identified form **in connection with its business**."

Mitigating Risks

- OPC Investigation into use of de-identified mobility data (May 2023)
- Public Health Agency of Canada collected, from mobile operators, mobile cell-tower data and geolocation data transmitted by mobile devices
- OPC found safeguards implemented reduced risk of re-identification below “serious possibility”.
  - Stripping out direct identifiers
  - Aggregation
  - Contractual clauses
  - Data release model

Mitigating Risk

Technical Standards and Guidelines

- National Institute of Standards and Technology (**NIST**) 'De-Identifying Government Datasets: Techniques and Governance' (September 2023)
- ISO/IEC 27559:2022 'Privacy enhancing data de-identification framework' (November 2022)
- Office of the Information and Privacy Commissioner of Ontario, 'De-identification Guidelines for Structured Data' (June 2016)

Mitigating Risk

Contracting

- Is aggregation/anonymization/de-identification permitted?
- If so, by who and for what purpose(s)?
- Access controls.
- Consider representations and warranties with respect to re-identification or other misuse.
- Consider anonymization as alternative to destruction.
- Indemnities that properly address misuse of “de-identified” data.

DENTONS

Thank you

Luca Lucarini
Associate (Toronto)
+1 416 863 4735
luca.lucarini@dentons.com