DENTONS

Understanding the legal landscape for biometric information in Canada and Québec

April 28, 2025

Grow | Protect | Operate | Finance

Speakers:

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

Alexandra Quigley
Senior Associate, Montreal
+1 514 878 5856
alexandra.quigley@dentons.com

Topics

1. Just what are biometrics?
2. Biometric data regulation in Canada, including PIPEDA
3. Québec’s legal framework for biometric information (LFIT & ARPPIPS)
4. The CAI's decision on a retailer’s use of facial recognition technology
5. Class action quickie
6. Best practices for compliance and privacy protection and practical insights

Just what are “biometrics”?

What are “biometrics”?

“Biometry: the measurement and analysis of unique physical or behavioral characteristics (as fingerprint or voice patterns) especially as a means of verifying personal identity.”

- Merriam-Webster Dictionary

““Biometrics” refers to the quantification of human characteristics into measurable terms. They are used for recognition and, less commonly, for categorization.

- Office of the Privacy Commissioner of Canada, Draft Guidance for processing biometrics – for organizations (October, 2023)

“ ”

- *Act respecting the protection of personal information in the private sector, CQLR c P-39.1*

29(2)“biometric information” means information derived from an individual’s unique personal characteristics, other than a representation of his or her photograph or signature.

- *Electronic Commerce Act, 2000, SO 2000, c 17*

“Biological and behavioural characteristic of an individual from which distinguishing, repeatable biometric features can be extracted for the purpose of automated recognition of individuals.”

- International Standards Organization (ISO)

Definitional precision

“Biometric” or **“Biometric Information”** – generic term with no precision, body measurements and calculations related to human characteristic.

Example: Someone who is 6’2” tall.

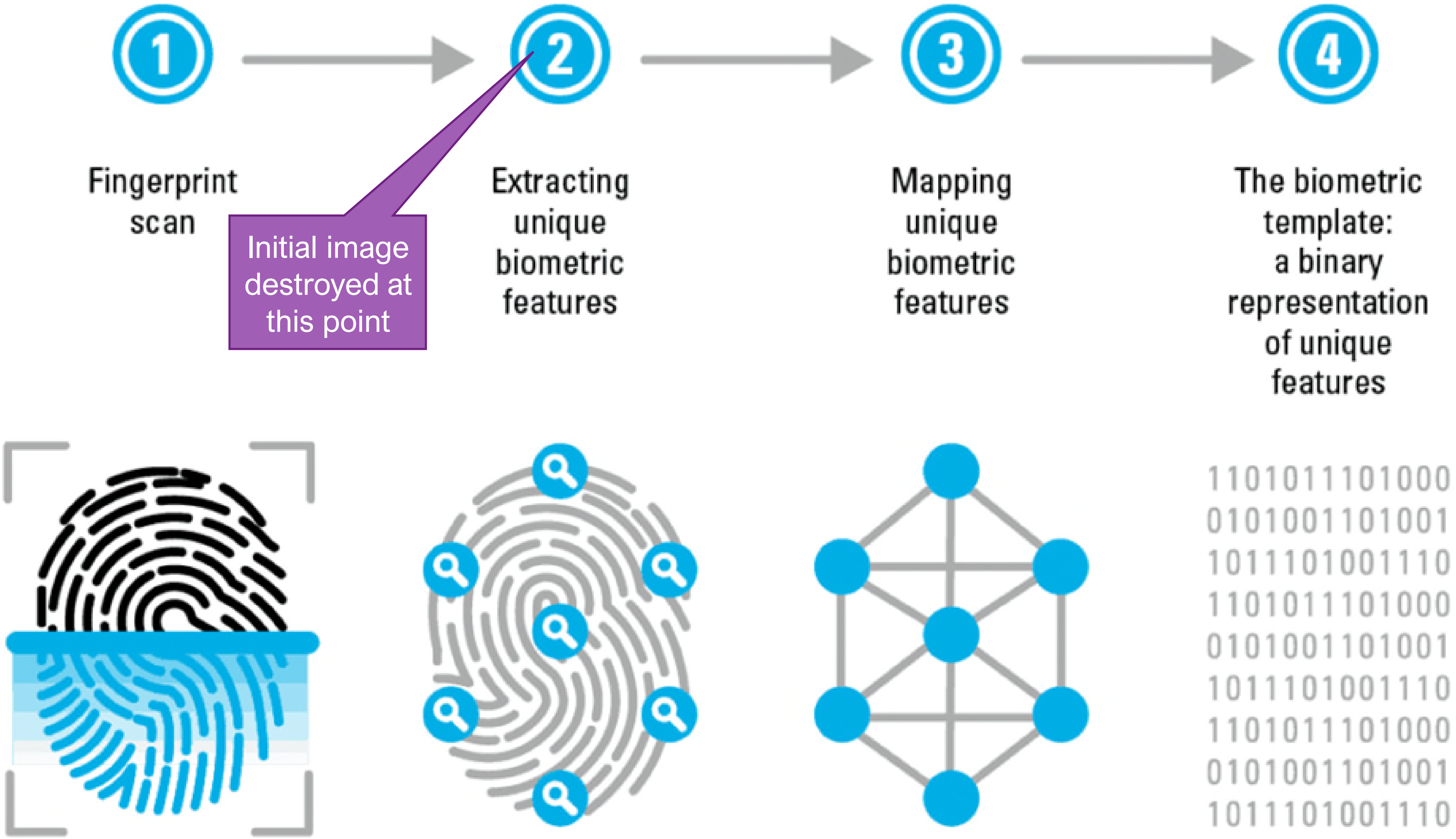
“Biometric Identifier” – distinctive, measurable characteristics used to label and ***describe unique individuals***.

Example: My fingerprints.

Three main categories of biometric identifiers used for recognition:

- Morphological biometrics – such as fingerprints, earprints, iris scan.
- Behavioural biometrics – such as keystroke patterns or gait.
- Biological biometrics – such as DNA or blood.

How “biometrics” work



1 Fingerprint scan

Initial image destroyed at this point

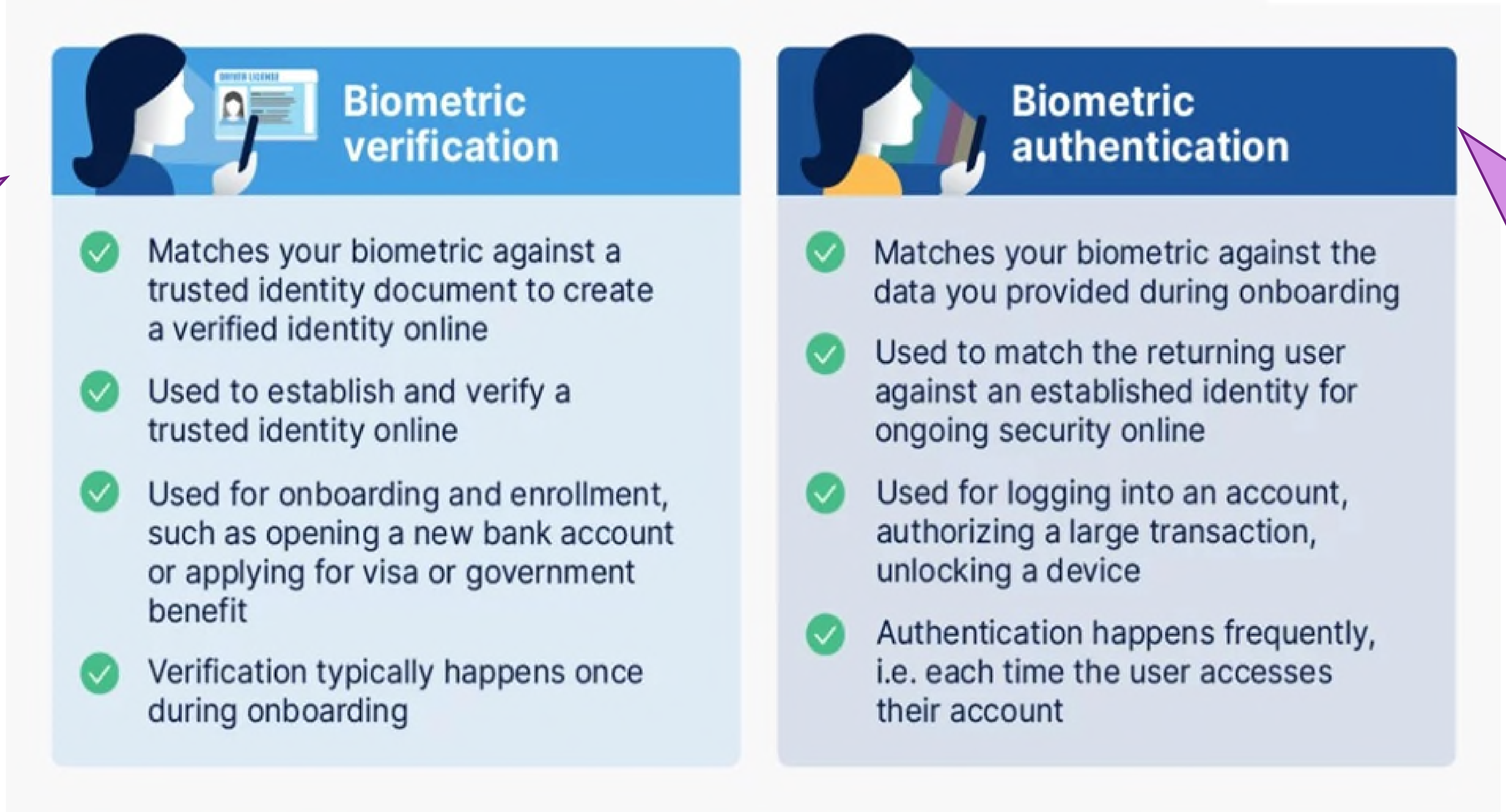
2 Extracting unique biometric features

3 Mapping unique biometric features

4 The biometric template: a binary representation of unique features

Use

Aka “enrollment stage”



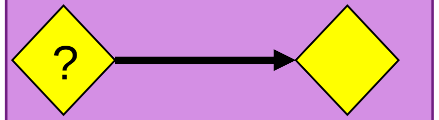
Biometric verification

- ✓ Matches your biometric against a trusted identity document to create a verified identity online
- ✓ Used to establish and verify a trusted identity online
- ✓ Used for onboarding and enrollment, such as opening a new bank account or applying for visa or government benefit
- ✓ Verification typically happens once during onboarding

Biometric authentication

- ✓ Matches your biometric against the data you provided during onboarding
- ✓ Used to match the returning user against an established identity for ongoing security online
- ✓ Used for logging into an account, authorizing a large transaction, unlocking a device
- ✓ Authentication happens frequently, i.e. each time the user accesses their account

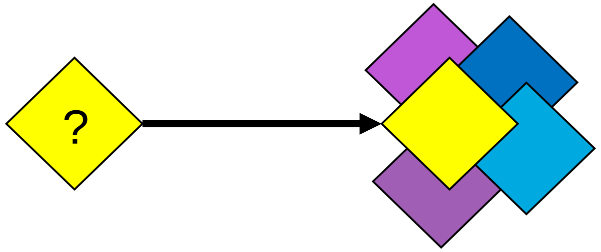
Compares a sample against a single stored template.
Also called a one-to-one (1:1) system
Typical application: fingerprint lock



Confirms you are you (but not *who* you are)

Contrast with *identification* (or *recognition*)

- Search a sample against a database of templates.
- Also called a one-to-many (1:N) system
- Typical application: identifying fingerprints



Privacy Commissioner of Canada

Draft Guidance for processing biometrics – for organizations (October 2023)

“**Biometrics**” refers to the quantification of human characteristics into measurable terms. They are used for recognition and, less commonly, for categorization.

Matching: A “probe” biometric is collected from the individual, and is usually converted into a template to allow for an automated comparison against the previously enrolled biometric for the purposes of:

- **Authentication:** by matching an individual’s probe biometric to the previously stored sample only (one-to-one comparison) to confirm <u>who they are</u>.
- **Identification:** by cross-referencing an individual’s biometric against a database (one-to-many comparison) to search for <u>who they are</u>.

BUT….

“Information that will generally be considered sensitive and require a higher degree of protection includes health and financial data, ethnic and racial origins, political opinions, genetic and **<u>biometric data</u>**, an individual’s sex life or sexual orientation, and religious or philosophical beliefs.”

- *Interpretation Bulletin: Sensitive Information*

Use cases for “biometrics”

Access control: Biometrics replace physical keys in areas like offices or laboratories, controlling who can enter specific zones.

Workplace time entry: A device that uses unique physical characteristics (such as fingerprints or facial recognition) to identify and track employees' work hours. This system eliminates the need for traditional time cards or punch clocks, and is promoted as a solution for “time theft” or “buddy punching”.

Workplace safety: Use of cameras enabled with AI and biometrics to monitor red zones, such as an area around heavy equipment or dangerous machinery.

Retail theft/fraud: Retailers create database of images of faces from CCTV showing incidents of suspected fraud/theft, and then equip CCTV entrance cameras with facial recognition to deny entry.

Identity verification: Biometrics are used in passports, driver's licenses, and government IDs to verify identity.

Payment systems: Authentication of users with fingerprint readers, eliminating the need for PINs.

Biometric regulation in Canada

Canada

- OPC ***Interpretation Bulletin: Sensitive Information*** (updated May 2022):

> “Information that will generally be considered sensitive and require a **higher degree of protection** includes health and financial data, ethnic and racial origins, political opinions, genetic and **biometric data**, an individual's sex life or sexual orientation, and religious or philosophical beliefs.”

- Information that is sensitive requires express (opt-in) consent.

- 2011 guidance ***Data at Your Fingertips Biometrics and the Challenges to Privacy*** *is* outdated, but says to considers recording summary information only, use local storage, and use verification instead of identification where possible.

Canada

Key findings from OPC:

> “Biometric information is sensitive in almost all circumstances, as it is intrinsically, and in most instances permanently, linked to the individual. It is distinctive, stable over time, difficult to change and largely unique to the individual.”
>
> *Joint investigation of the Cadillac Fairview Corporation Limited*
> *by the Privacy Commissioner of Canada,*
> *the Information and Privacy Commissioner of Alberta,*
> *and the Information and Privacy Commissioner for*
> *British Columbia*, 2020 CanLII 83156 (PCC)

> “Facial biometric information is particularly sensitive as it may allow for the identification of an individual through comparison against a vast array of images available on the internet or via surreptitious surveillance.”
>
> *Joint investigation of Clearview AI, Inc.*
> *by the Office of the Privacy Commissioner of Canada,*
> *the Commission d’accès à l’information du Québec,*
> *the Information and Privacy Commissioner for British Columbia,*
> *and the Information Privacy Commissioner of Alberta*, 2021 CanLII 9227 (PCC)

Canada

Other findings

Voiceprints:

- *Telecommunications firm failed to obtain appropriate consent for voiceprint authentication program*, 2022 CanLII 91035 (PCC)
- *Organization uses biometrics for authentication purposes*, 2004 CanLII 52853 (PCC)

Palm scanning:

- *GMAT Test-taker Objects to Palm-Vein Scanning (Re),* 2011 CanLII 99346 (PCC)
- *Test administrator revises measures aimed at preventing exam fraud (Re),* 2010 CanLII 99709 (PCC)
- *Law School Admission Council Investigation*, 2008 CanLII 28249 (PCC)

Provincial:

- Alberta – employee thumbprint scan: *Empire Ballroom (1208558 Alberta Ltd.); Investigation Report P2008-IR-005 (27 August 2008), Office of the Information and Privacy Commissioner of Alberta*

Canada

Test for implementation found in OPC *Guidance on inappropriate data practices: interpretation and application of subsection 5(3):*

> "[I]n addition to considering the **degree of sensitivity** of the personal information at issue, we consider the factors set out by the courts* in order to assist in determining whether a reasonable person would find that an organization's collection, use and disclosure of information is for an appropriate purpose in the circumstances. Specifically, we consider:
>
> a. Whether the organization's purpose represents a **legitimate need** / *bona fide* business interest;
>
> b. Whether the collection, use and disclosure would be **effective** in meeting the organization's need;
>
> c. Whether there are **less privacy invasive means** of achieving the same ends at comparable cost and with comparable benefits; and
>
> d. Whether the loss of privacy is **proportional** to the benefits."

* *Turner v. Telus Communications Inc*., 2005 FC 1601, paragraph 39, aff'd 2007 FCA 21. See also *Eastmond v. Canadian Pacific Railway,* 2004 FC 852, paragraph 129

Canada

OPC Draft Guidance for processing biometrics – for organizations (October 2023):

- **Identifying an Appropriate Purpose*** - sensitivity + necessity + effectiveness + proportionality + minimal intrusiveness
- **Consent** – must be express, must be free (not a condition of service, alternatives)
- **Limiting Collection** – use authentication before identification, minimum number of biometric characteristics, don't copy identity documents
- **Limiting Use, Disclosure, and Retention** – no secondary purpose, closed loop, de-link, limit retention, destroy raw info, delete biometric info on request
- **Safeguards** – sensitive so higher standard
- **Accuracy** – type of biometric fit for purpose
- **Accountability** – policies, etc.
- **Openness** – disclose in privacy policy (be specific), disclose transfers to 3rd parties

* *Turner v. Telus Communications Inc.*, 2005 FC 1601, paragraph 39, aff'd 2007 FCA 21. See also *Eastmond v. Canadian Pacific Railway,* 2004 FC 852, paragraph 129

Canada

Other mentions in Canadian statutes:

FIPPAs

Ontario and Alberta specifically include it as being personal information and define it

Immigration statutes

Immigration and related statutes have language authorizing collection of biometric characteristics:

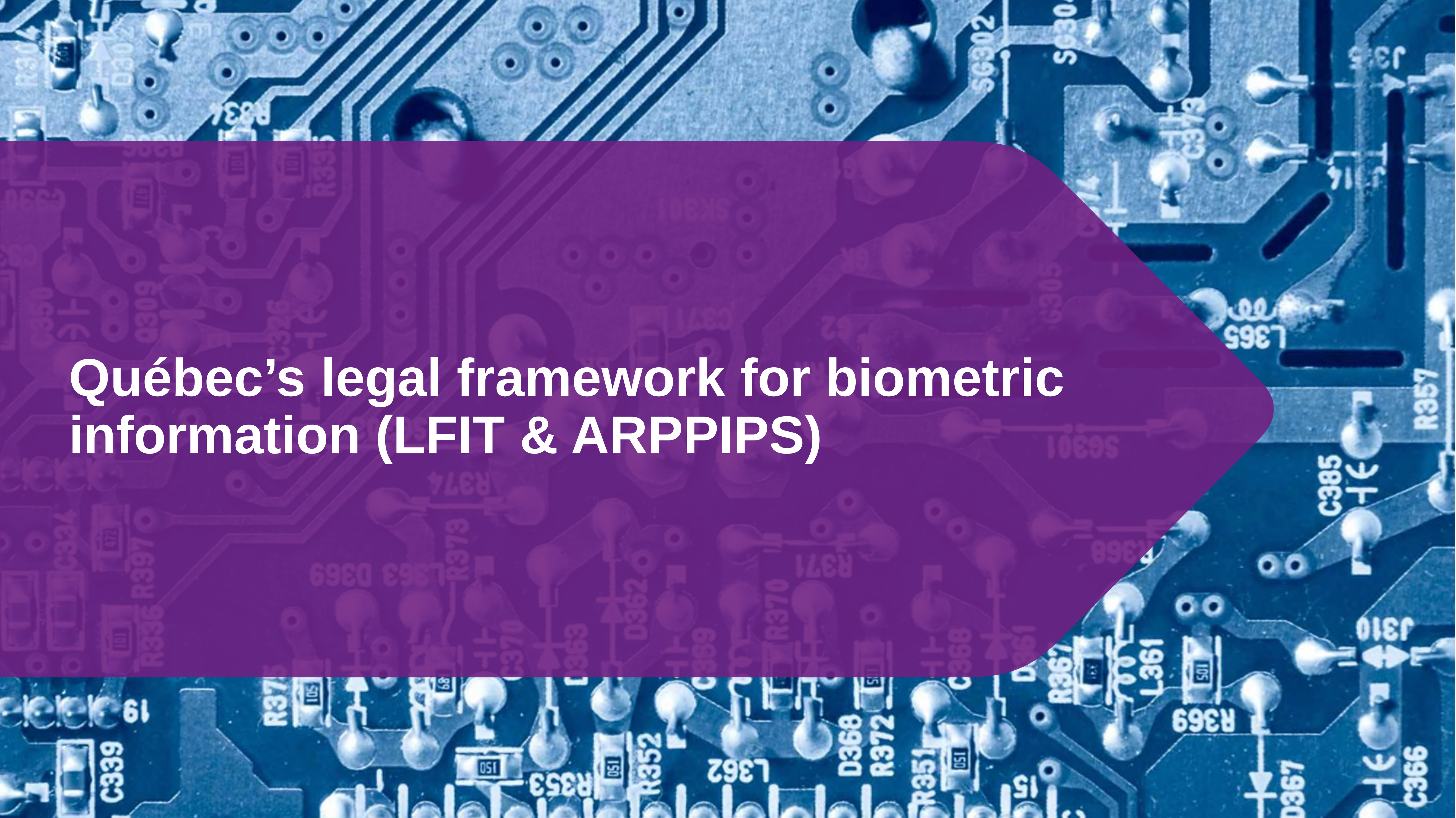
Immigration and Refugee Protection Act, SC 2001, c 27
Protecting Canada's Immigration System Act, SC 2012, c 17
Preclearance Act, 2016, SC 2017, c 27

Electronic commerce statutes

Alberta and Ontario carve out biometrics from the application of the statute

Ontario benefits statutes

Ontario Works Act, 1997, SO 1997, c 25, Sch A
Ontario Disability Support Program Act, 1997, SO 1997, c 25, Sch B



Québec’s legal framework for biometric information (LFIT & ARPPIPS)

Quebec – IT Act

Identity verification notice requirement

44. A person's **identity may not be verified or confirmed** by means of a process that allows biometric characteristics or measurements to then be used except where such verification or confirmation has been **previously disclosed** to the Commission d'accès à l'information **and** except with the **express consent** of the person concerned. Only the **minimum number of characteristics or measurements needed** to link the person to an act and only such characteristics or measurements as may not then be used without the person's knowledge may then be used for identification purposes.

No **other information revealed** by the characteristics or measurements recorded may be used as a basis for a decision concerning the person or for any other purpose whatsoever. Such information may only be disclosed to the person concerned, at the person's request.

The record of the characteristics or measurements and any notation relating thereto **must be destroyed** as soon as the purpose of verification or confirmation of identity has been met or the reason for the verification or confirmation no longer exists

Act to establish a legal framework for information technology, CQLR c C-1.1, section 44

Quebec – IT Act

Database disclosure requirement

45. The **creation of a database** of biometric characteristics and measurements must be disclosed to the Commission d'accès à l'information promptly and **not later than 60 days before it is brought into service**.

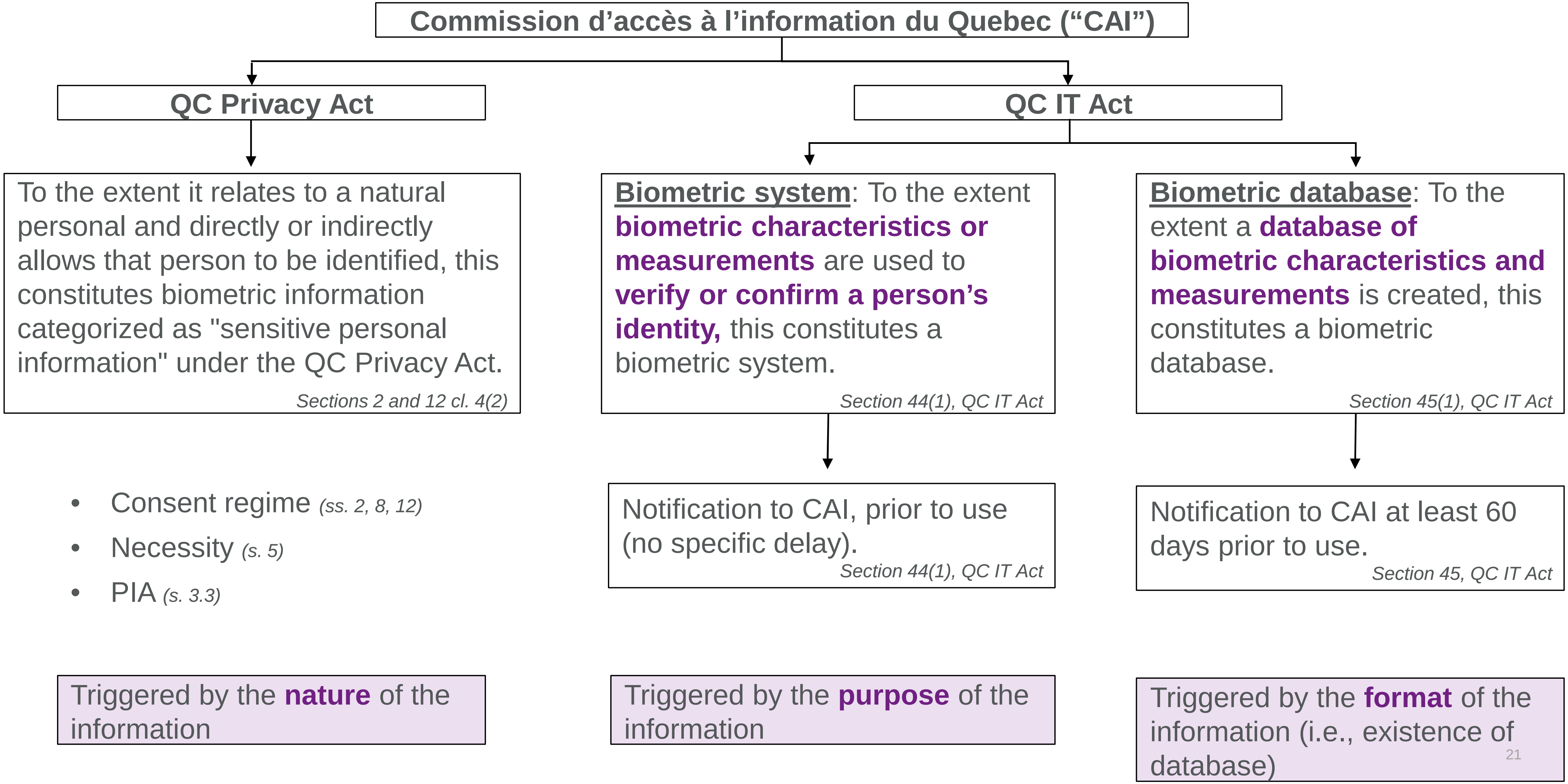
The Commission may make orders determining how such databases are to be set up, used, consulted, released and retained, and how measurements or characteristics recorded for personal identification purposes are to be archived or destroyed.

The Commission may also suspend or prohibit the bringing into service or order the destruction of such a database, if the database is not in compliance with the orders of the Commission or otherwise constitutes an invasion of privacy.

Act to establish a legal framework for information technology, CQLR c C-1.1, section 45

Quebec Privacy Act: s. 12 – information which is "biometric" in nature requires express consent AND you must give people an alternative for ID/verification via biometric processing

Canada - Quebec



Commission d’accès à l’information du Quebec (“CAI”)

QC Privacy Act

To the extent it relates to a natural personal and directly or indirectly allows that person to be identified, this constitutes biometric information categorized as "sensitive personal information" under the QC Privacy Act.

Sections 2 and 12 cl. 4(2)

- Consent regime *(ss. 2, 8, 12)*
- Necessity *(s. 5)*
- PIA *(s. 3.3)*

Triggered by the **nature** of the information

QC IT Act

Biometric system: To the extent **biometric characteristics or measurements** are used to **verify or confirm a person’s identity,** this constitutes a biometric system.

Section 44(1), QC IT Act

Notification to CAI, prior to use (no specific delay).

Section 44(1), QC IT Act

Triggered by the **purpose** of the information

Biometric database: To the extent a **database of biometric characteristics and measurements** is created, this constitutes a biometric database.

Section 45(1), QC IT Act

Notification to CAI at least 60 days prior to use.

Section 45, QC IT Act

Triggered by the **format** of the information (i.e., existence of database)

Canada - Quebec

- Québec CAI has published guidance
  - *The need for the information collected* (updated Sept 2022)
  - *Consent to the use of biometrics* (updated Sept 2022)
  - Documentation and forms
  - *Biometrics at work*

How to assess if collection of biometric information is necessary

Sets out requirements for valid consent. To be valid, consent must be:

- **manifest and express**: explicit and unequivocal, given by a positive gesture clearly manifesting the agreement (e.g., signing a document);
- **free:** given without being influenced by undue constraint or pressure;
- **informed:** given with full knowledge of the facts, with all the information necessary to measure its reach;
- **specific**: limited to clearly defined objectives;
- **limited in time:** given for a predefined time period.

Includes *Biometrics: principles to be respected and legal obligations of organizations* (guide for public bodies and businesses, Sept 2022). Also includes mandatory forms for registration and a sample consent.

Discussing employer obligations when implementing biometrics

The CAI's decision on a retailer’s use of facial recognition

Biometrics in retail

- The CAI received from a supermarket chain (Retailer) a declaration of intent to create and use a bank of biometric information,
  - The Retailer wanted to set up a bank of biometric characteristics or measurements (database), as a pilot project, to support implementation of facial recognition systems in some of its stores.
  - The purpose was to counter shoplifting and fraud in some of the Retailer’s stores
  - Facial recognition would be used on images captured by CCTV at entrances. These images would be algorithmically compared to reference images contained in the Retailer’s database.
  - If there is a match between the image captured by the CCTV cameras and one in the database, an alert will be sent to the team managing the database
  - The database would consist of reference images collected from Retailer's CCTV of prior shoplifting or fraud events involving people of legal age and which have been the subject of police intervention.

Commission d’accès à l’information du Québec,
Dossier 1037199-S

Biometrics in retail

- The CAI prohibited implementation of the Retailer’s planned bank of biometric characteristics or measurements for the purpose of identifying, by means of facial recognition, persons who have already been involved in shoplifting or fraud in the Company’s stores.
- The Retailer argued it did not seek to actually verify or confirm the exact identity of individuals, but rather to prevent shoplifting and fraud based on a “match” of faces entering the store with faces captured from CCTV shoplifting and fraud incidents.
- The CAI nonetheless found that the act of confirming whether or not individuals belonged to a specific group of people constructed verification of identity within the meaning of the applicable legislation.

Commission d’accès à l’information du Québec,
Dossier 1037199-S

Workplace decisions of the CAI

- A hotel used biometric information for payroll processing. The purpose was improved efficiency of payroll processing (saving over 400 hours/year). The CAI agreed the purpose was legitimate and stemmed from a real problem, but concluded the company had not demonstrated that this purpose was sufficient to justify the collection of biometric information. The CAI found **improved efficiency of the payroll system, which is a common and intrinsic objective in the management of any company, and was not sufficient on its own to demonstrate necessity.**

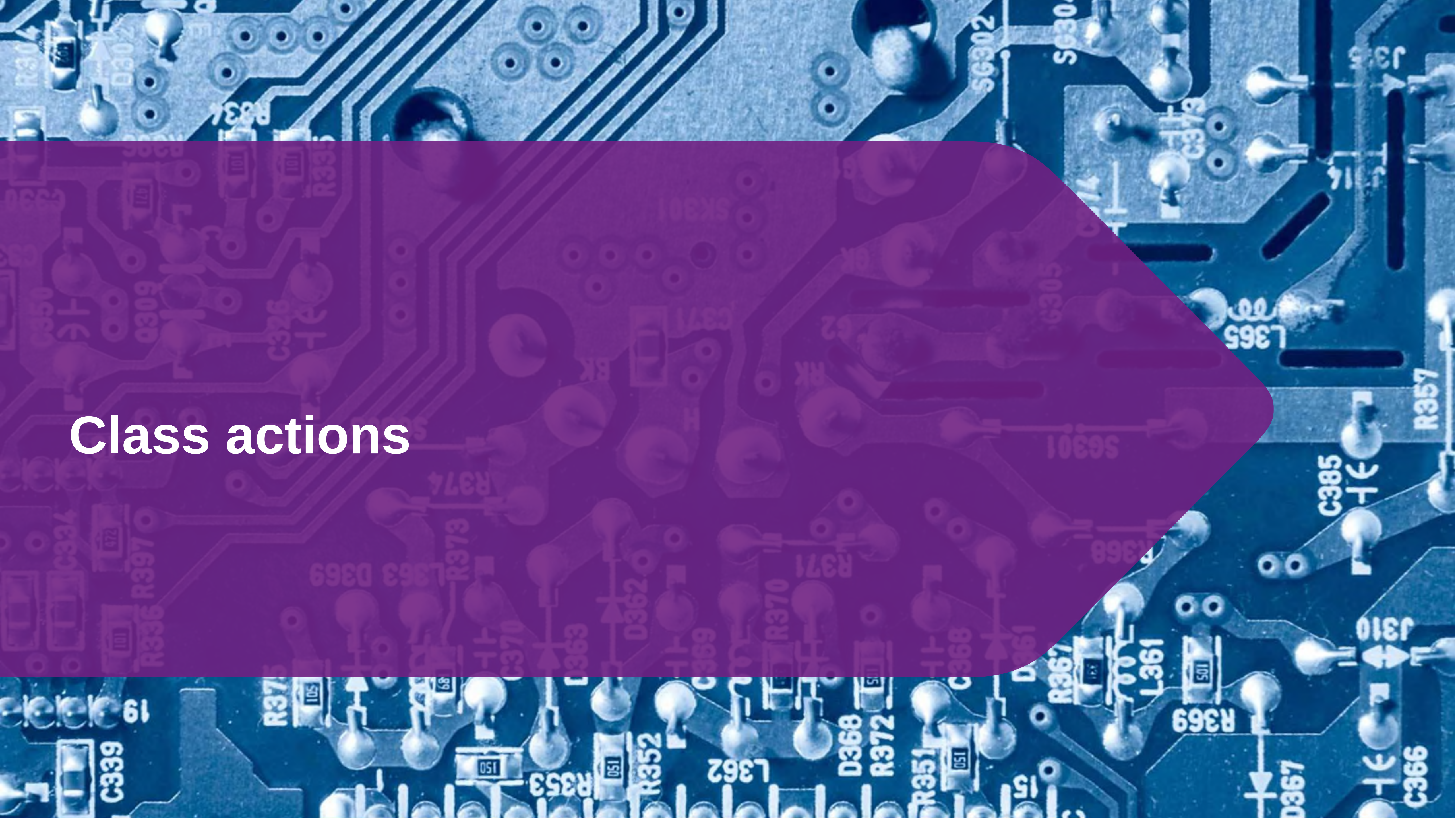
Auberge du lac Sacacomie inc., CAI 1014137-S, April 7, 2022

- An organization **failed to demonstrate how the privacy invasion was minimized or how the benefits of the biometric time clock outweighed the significant invasion of employee rights.** The organization stopped using the biometric time clock and destroyed all biometric information it had collected.

Investigation into Selenis Company Canada, CAI 1016217-S, January 14, 2022

- During COVID, a printing company implemented an authentication system featuring facial recognition and body temperature measurement. The company's objective was 1) to ensure the safety of its employees/premises by limiting the spread of the virus; and 2) to comply with trade certification standards. In 2023, the company stopped taking temperatures and destroyed collected data. However, it continued to collect biometric data through its facial recognition system. The **CAI found the company failed to demonstrate the necessity of collecting *biometric* information to ensure either safety or compliance with the law.**

Imprimeries Transcontinental inc., CAI 1024350-S, September 4, 2024



Class actions

Common Law

- United States - BIPA in Illinois leading focus
- Canada – only a few cases so far, grouped generally as follows:

The social media cases (intrusion upon seclusion claims related to tagging, faceID, photo grouping and AI functions)

- *Situmorang v Google* LLC, 2022 BCSC 2052 (rev'd, 2024 BCCA 9)
- *Homsy c. Google,* 2021 QCCS 4213
- *Thomas v ByteDance Ltd., Tiktok Ltd.*, 2022 BCSC 297

The Privacy-Commissioner-got-it-wrong-cases

- *Turner v. Telus Communications Inc.,* 2005 FC 1601
- *Wansink v. TELUS Communications Inc.* (F.C.A.), 2007 FCA 21
- *Cleaver v. Cadillac Fairview* (moving to certification)

The Cambridge Analytica cases

- *Kish v Facebook Canada Ltd.,* 2021 SKQB 198
- *Simpson v Facebook,* 2021 ONSC 968
- *Doan c. Clearview AI* inc., 2024 QCCS 213

Best practices to mitigate risk

Best practices

- Conduct a PIA which is focused on the collection and biometric information
- Consider closely the criteria of **necessity** (is it truly necessary?) and whether there are **less privacy invasive means** of achieving the same ends at comparable cost and with comparable benefits.
  - These are the most frequent elements of the test for which organizations fail.
    - Don’t drink the corporate Kool-Aid: consider having an impartial 3rd party evaluate necessity.
    - Consider (and test) alternatives to establish costs and benefits.
  - Can you **document (and provide evidence**) of the above? Organizations often fail to make a compelling case not because they don’t meet the test, but because they have failed to document how they meet the test.
- **Consent must be detailed and granular.**
  - Organizations typically display a real reluctance to disclose all the information required, to avoid alarming customers/employees. This almost always backfires (customers/employees feel they have been lied to) and will negate any consent you have collected.

Thank you

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

Alexandra Quigley
Senior Associate, Montreal
+1 514 878 5856
alexandra.quigley@dentons.com

Thank you for attending!

Dentons On-Demand

DENTONS

Dentons On-Demand

Your guide to the latest trends and topics impacting your business

Grow | Protect | Operate | Finance

Missed a webinar? We have you covered! Dentons On-Demand is your one-stop-shop for CPD/CLE-accredited national webinars highlighting the latest trends and topics which impact you and your business.

Visit our Dentons in Session page for all upcoming CPD accredited seminars or scan the QR code to access our brochure. https://www.dentons.com/en/about-dentons/news-events-and-awards/events/dentons-in-session.