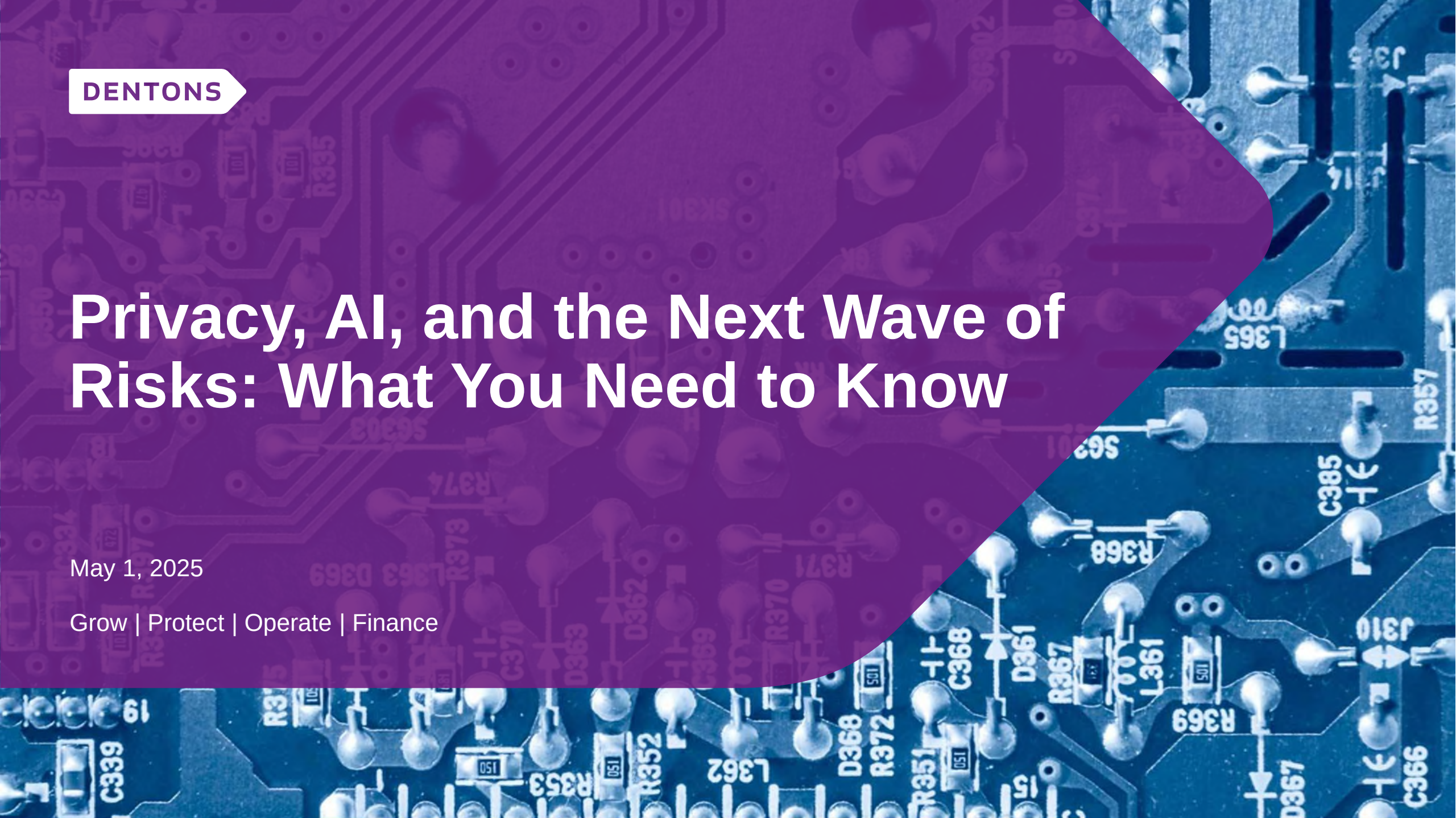
DENTONS

Privacy, AI, and the Next Wave of Risks: What You Need to Know

May 1, 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

Emma Irving
Partner, Vancouver
+1 604 648 6502
Emma.irving@dentons.com

Mitch Bringeland
Associate, Vancouver
+1 604 629 4991
Mitch.bringeland@dentons.com

Housekeeping

- **Accreditation.** For accreditation purposes, please note this session is eligible for 60 Substantive minutes with the Law Society of British Columbia; 60 Substantive minutes with the Law Society of Ontario; and, in our view, meets the CLE requirements of the Barreau du Québec. A contact email will be provided in the post event email to receive a certificate.

Topics

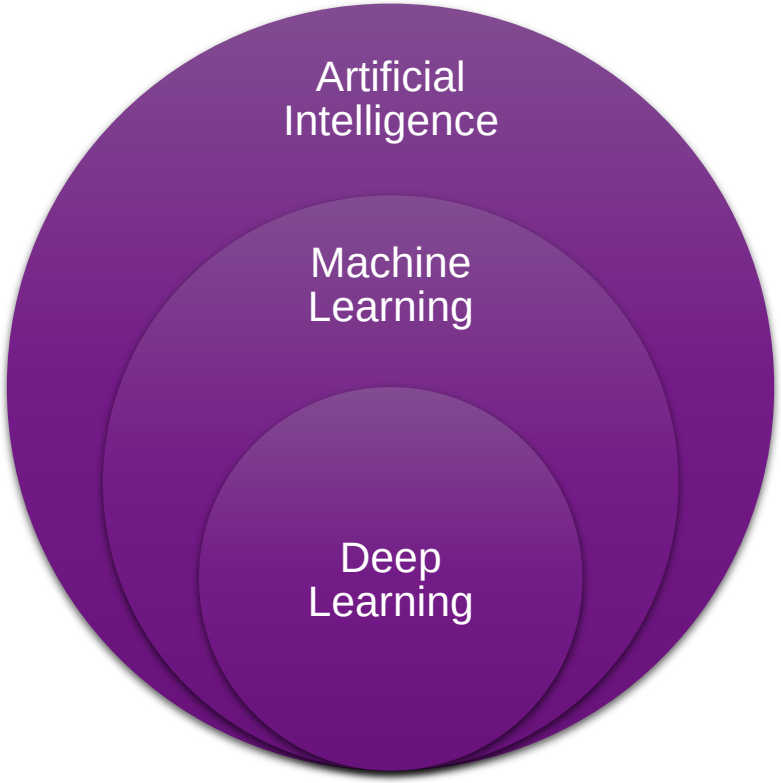
1. **AI under the microscope:** How to conduct effective PIAs on vendors (that use or may use AI).

2. **The next wave of class actions:** Why breaches aren't the only risk — actions based on inadequate consent and undisclosed sharing are on the rise.

3. **Where BC privacy law is going:** The BC OIPC's strategic priorities and what that means for enforcement, as well as an update on amendments.

AI under the microscope

What do we mean by “artificial intelligence”?



Machine Learning

A type of data processing that uses training data and statistical techniques to identify patterns.

Deep Learning

The use of large, multi-layer artificial neural networks that compute with continuous representations, similar to neurons in human brains.

Uses: computer vision, natural language processing, and speech recognition, which enable tasks like image recognition, machine translation, and virtual assistants.

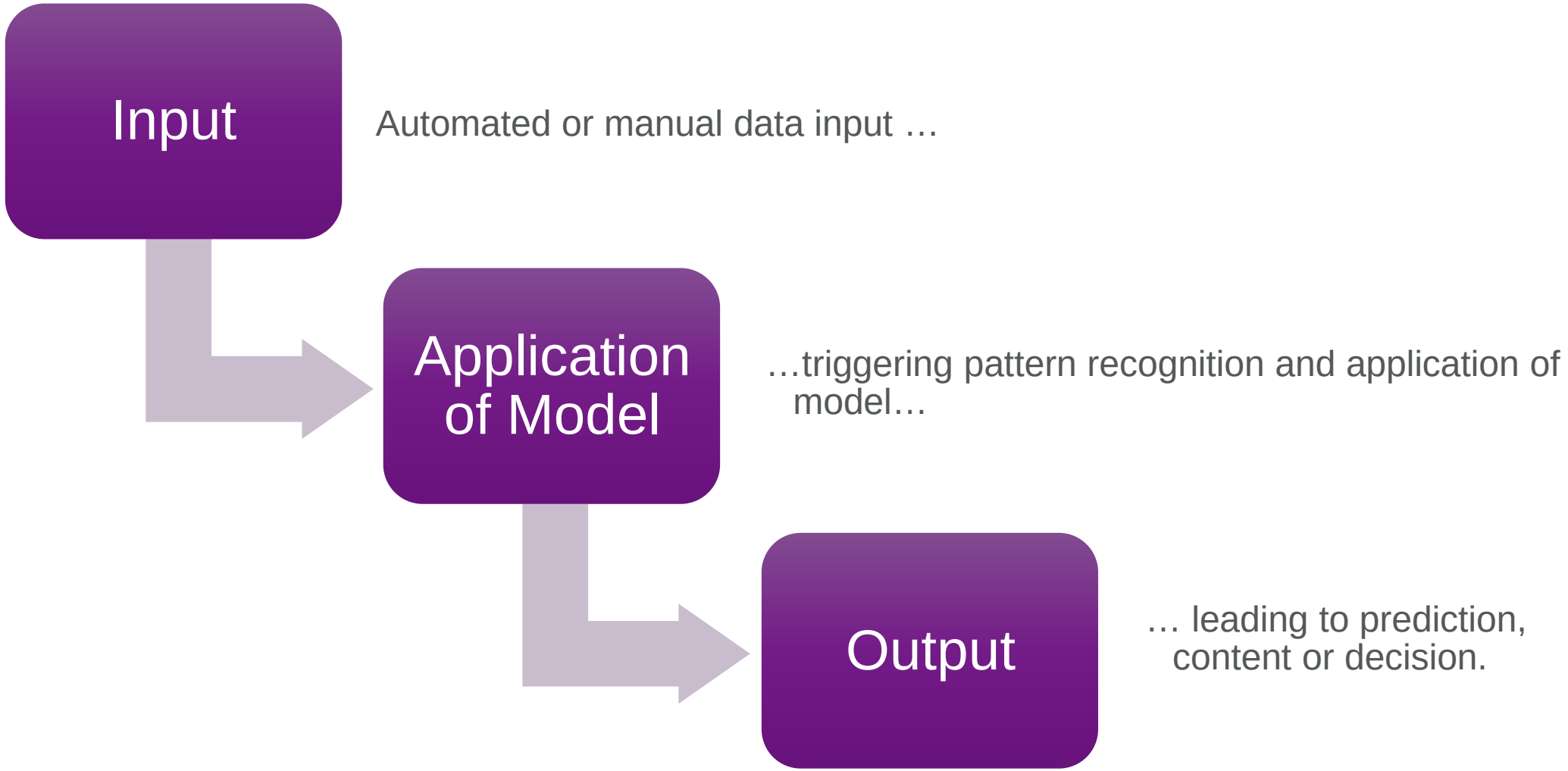
What do we mean by “artificial intelligence”?

Models

Supervised	A model learns to make accurate predictions after “seeing” human-labelled data.
Unsupervised	A model learns to infer relationships from unlabeled data.
Reinforced	An agent learns action sequences that optimize its rewards, such as winning games, without explicit examples of good techniques.

What do we mean by “artificial intelligence”?

AI Systems



“Data”

- **Training Data:** Subset of the overall dataset in the model that is used to train the model and detect meaningful patterns.
  - **EU: Act:** “data used for training an AI system through fitting its learnable parameters.”

- **Testing Data:** Smaller, unseen subset used at the end of the training process to check whether model is working accurately
  - **EU Act:** “data used for providing an independent evaluation of the AI system in order to confirm the expected performance of that system before its placing on the market or putting into service.”

- **Input Data:** “Data provided to or directly acquired by an AI system on the basis of which the system produces an output”

Common use cases

Voice assistants, chatbots, and conversational AI	Uptime/reliability optimization	Customer service operations	**Personalization**
IT operations management	**Process automation**	Financial reporting and accounting	**Recruiting/hiring**

PIAs

- A privacy impact assessment (PIA) is a step-by-step review process that helps to identify and address potential privacy risks that may occur in a project. A PIA is used for information systems, administrative practices and policy proposals that relate to the collection, use or disclosure of individually identifying personal information.

- Use them for internal projects, or projects involving services/products/solutions provided by external parties (vendors, partners).

- Done prior to launch of project
  - May mean that you have to do at least a partial PIA as part of the procurement process

- Different from a cybersecurity questionnaire/data protection assessment

- Not (yet) legally required by private sector privacy laws (except Quebec)

PIAs and AI

PIAs for AI systems can be challenging due to their complexity, the large volume of data they process, and the potential for algorithmic biases and lack of transparency. Traditional PIAs may not be sufficient to address the unique issues posed by AI.

1. Complexity and Dynamic Nature of AI	• Large Datasets • Dynamic Nature • "Black Box" Effect
2. Algorithmic Bias and Lack of Transparency	• Biases in Algorithms • Lack of Transparency
3. Data Handling and Security	• Sensitive Data • Data Retention
4. Unique Challenges in AI PIAs	• Assessing the Full Impact • Addressing Ethical Concerns • Adapting to Technological Change
5. Need for a Holistic Approach	• Interdisciplinary Teams • Focus on Prevention • Continuous Monitoring

Content of a good AI PIA

Principle	Questions to ask	Considerations and impacts
Lawful	• Is the PI that is being collected for the AI system or project directly related to the function or activities being contemplated and **necessary** for that purpose? • Does the AI system or project collect PI beyond what is reasonably necessary for the project's function or activities? o Be sure to review **each** input. o The outputs of the AI system or project could be considered a "collection through creation" of PI. Consider whether those outputs are all reasonably necessary for the project's functions or activities. • Does the AI system or project clearly comply with the relevant legislation? • What data set was the AI system or project trained on? o Was consent from individuals obtained in order to lawfully use their information to train the AI system? An exception to consent? i o Was **data scraping** used to obtain training data?	Collecting data from other sources including from public sources like social media posts, or semi-public sources like a company register which charges a fee, is also an indirect collection of PI which can be unexpected, unfair or intrusive, and could also result in the collection of unsolicited information. When organizations enter into agreements to collect data from third party organizations, organizations should satisfy themselves that the data was collected from individuals lawfully and that the sharing to the agency is aligned with the original purpose of collection or individuals have consented. In addition, commonly used software applications are integrating AI features to collect user data 'behind the scenes' in a way which is often not obvious to users. Organizations should satisfy themselves when deploying software applications as to whether this is a feature of the software.

Content of a good AI PIA

Principle	Questions to ask	Considerations and impacts
Open	• Are individuals notified that their PI is being collected, the purposes for the collection and the intended recipients of their PI? • Consider third party providers managing the AI system. • Consider whether the individual is notified of any PI created through the use of the AI system. • Consider whether PI is being used to train the AI system, and whether that training is restricted to use on the organization's system or also benefiting the third party provider, and whether that purpose should be disclosed to the individual at the time of collection. • Is it clear whether the collection is required by law or is voluntary, and any consequences if the individual chooses not to provide the information?	AI technology may involve data collection that is covert or not obvious such as recording behaviour of users on a website or capturing data from a person's voice or movements to ascertain their emotional state. Organizations should ensure individuals are informed in the manner that is most effective in the context of the collection. Third party providers managing AI systems that receive an individual's PI may need to be mentioned in privacy notices in such circumstances. If an organization is using an AI system that will use PI solely for enhancing the organization's service, a privacy statement or notice should include this. If the PI is used beyond this, for example to allow the AI vendor to enhance their product, seek consent from affected individuals. Generally, using PI to train AI systems outside of an organization's own use case is high risk and should be avoided wherever possible. Consider how to communicate to individuals about novel forms of PI collection. Example: where an AI-powered chatbot is engaging in a human-like conversation, a just-in-time pop up notice is appropriate (not posted on a web page privacy policy which the user may not see it).

Content of a good AI PIA

Principle	Questions to ask	Considerations and impacts
Relevant	o Is all the PI collected for the AI system relevant to the purpose of collection? o Review each data point/input for relevance. • How are you ensuring the PI being collected is accurate, complete, up-to-date and not excessive? o Consider the source of the PI being collected. Can it be relied on? o Are there measures in place to ensure all required PI is provided? What are the impacts if the individual provides only some of the required PI? o Will the individual be prompted to provide all the required information? o Will the individual be prompted to provide the PI in an appropriate format? o Is old information that may be out of date being used or relied upon?	Using poor quality information such as records which are out-of-date could result in unfair or wrong decisions. This is particularly concerning where it could limit an individual's access to a service, opportunity or benefit, or result in a penalty. Some AI tools, such as chatbots, may need to prompt an individual to provide PI. It is important that this prompting occurs in a way that elicits relevant, accurate, complete and up to date information. When using AI technology, it can be easy to collect more information than is required and automated collection may not be subject to the same quality assurance that applies to PI collected through other means. Organizations should guard against collecting excessive amount of data just because it is there or easy to do with the use of technology. If an AI tool needs to be fed data held by the organization, it should be limited to what is strictly required for a specific outcome. Organizations should consider whether the use of free text fields is necessary, as there can be a heightened risk of collecting unsolicited PI. There is less risk in using structured data fields.

Content of a good AI PIA

Principle	Questions to ask	Considerations and impacts
Secure	• Is PI being stored securely within the AI system? • Who has access to the PI handled within the AI system? • Is there a risk that an individual may see PI of another individual when using the AI system? • Have retention periods and appropriate data disposal methods been defined and implemented? • If a third party is handling PI, what due diligence has been undertaken to ensure the PI is protected from unauthorized use or disclosure?	Data in an AI tool will need to be securely managed as it would in any other platform or system, on-premise or cloud-hosted. Data retention policies will need to incorporate mandatory minimum retention periods as required by legislative requirements. Contracts should be in place with third-party providers containing binding clauses on data security and compliance with privacy laws. Contracts should consider and account for obligations such as breach notification, DSAR requests, and audits. **Use caution in using AI tools provided by third parties on the basis of standard terms**. These terms are unlikely to require third parties to handle PI in accordance with Canadian privacy laws.

Content of a good AI PIA

Principle	Questions to ask	Considerations and impacts
Transparent	• How is the organization explaining to the person what PI about them is being stored, why it is being used and any rights they have to access it? • Can you describe what, how and why an individual's PI is being used in relation to the AI system?	Organizations should ensure clear information is made obviously and prominently available in a way that is appropriate to the situation, whether it is a website, in a live chat, on a sign in a public place or in a personal email addressed to the individual.
Accessible	• Are you prepared to meet requests for access to PI, including insights or inferences, derived from the use of AI systems. • Are you allowing people to access their PI without excessive delay or expense? o Consider whether the AI system will enable or delay an individual's access to their PI.	Organizations should consider whether arrangements with platforms or vendors and the data types and formats they use would allow for an extract of PI to be provided in the event such a request was received.
Correction	• How can an individual update, correct or amend their PI where necessary in relation to the AI system or project? • Can you ensure the AI system or project will make decisions based on the updated PI?	Organizations should consider whether arrangements with platforms or vendors and the data types and formats would allow for correcting of PI in the event such a request was received.

Content of a good AI PIA

Principle	Questions to ask	Considerations and impacts
Accurate	• What measures are in place to ensure the PI is relevant, accurate, up to date and complete before being used by the agency? o Consider whether additional checks are required if relying on AI generated outputs. o Should AI generated outputs be limited to specific, low risk use by the agency?	AI technology such as automated decision-making can be used to make decisions or to recommend decisions to agency staff which will affect an individual's access to a service, opportunity or benefit, or result in a penalty. AI may produce outputs that are sufficiently reliable for some purposes (such as recommending a service), but not for other purposes (such as approving an application). Consider the accuracy of the information when deciding how it will be used. Poor system design, or the use of poor-quality information such as historical agency records could result in biased, unfair or wrong decisions. Organizations must ensure training data and systems are reviewed with these risks in mind, especially where the AI system informs or makes decisions. Organizations should ensure that decisions made by an AI tool are explainable. If there is uncertainty about the reasons why the technology is making certain decisions or recommendations, it should not be used. Organizations should ensure that there is human validation of any AI process that uses PI.

Content of a good AI PIA

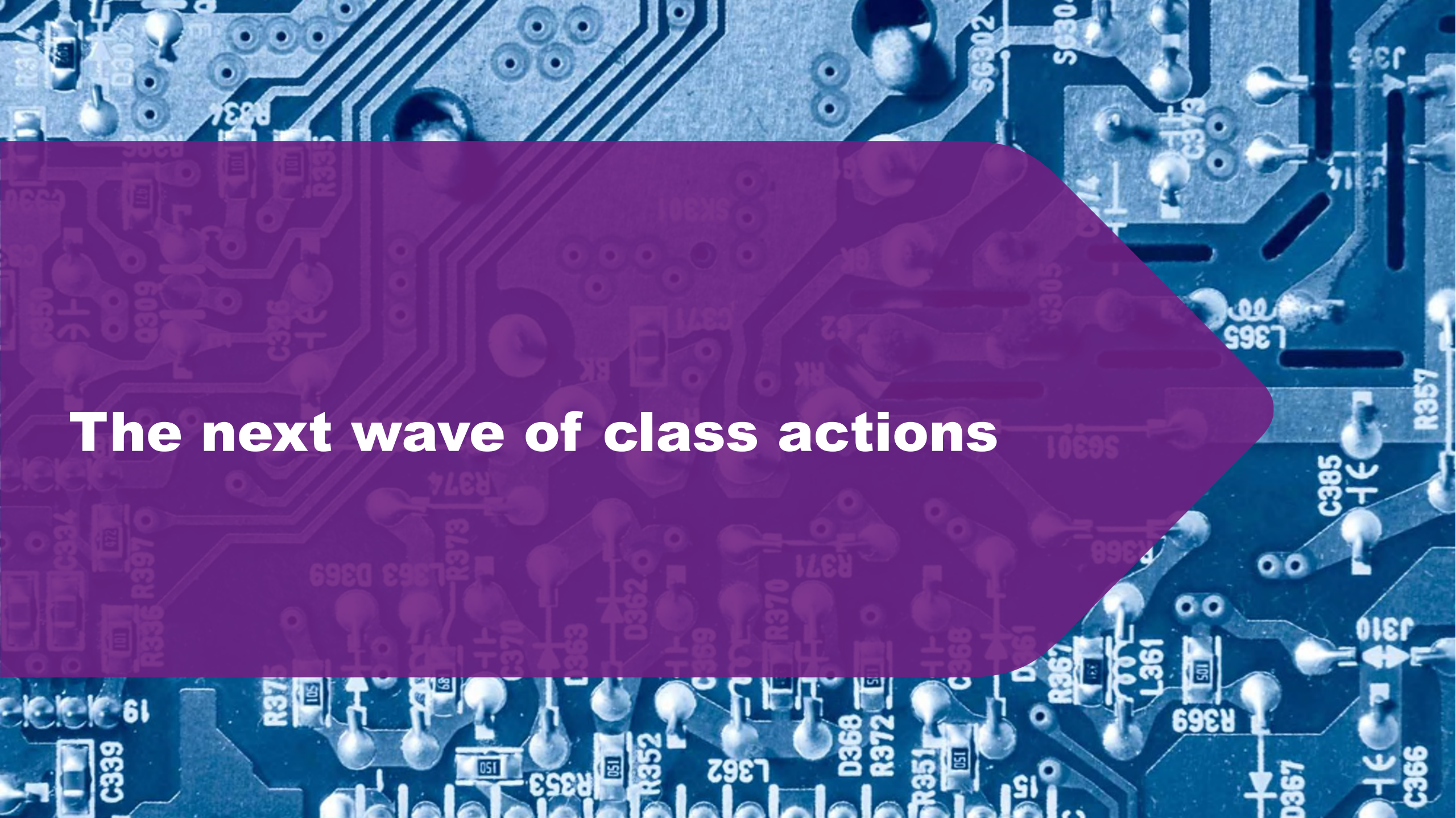
Principle	Questions to ask	Considerations and impacts
Limited Use	• Are you only using the PI for the purpose it was collected unless the person has given their consent, or the purpose of use is directly related to the purpose for which it was collected, or to prevent or lessen a serious or imminent threat to any person's health or safety? • If using a third-party provider, have you ensured an individual's PI is not being used by that third party for their own purposes? o This includes use of the PI by a vendor/third party to train its own system. • When it comes to training AI models have you considered ways this can be done without using PI?	AI systems can make it easy for organizations to use data for multiple purposes. For example, a database of facial images for security passes should not be used for training AI without a separate assessment. Organizations should refrain from using PI collected for a specific purpose for a different purpose unless individuals give their consent or an exemption applies. It is also common that AI system providers seek to use their customer's data for their own purposes, such as training their AI models. This is distinct from an organization using PI for training an AI system exclusively for internal purposes. Organizations should ensure external use of PI does not occur unless affected individuals give consent or an exemption applies. Generally, using PI to train AI systems outside of an organization's use case is high risk and should be avoided.

Content of a good AI PIA

Principle	Questions to ask	Considerations and impacts
Limited Disclosure	• Does the AI system or project disclose PI to another person or organization? • If so, o Is the disclosure directly related to the purpose the information was collected, and the individual is unlikely to object to the disclosure? or o Is the individual reasonably likely to have been aware of this disclosure? or o Has the individual consented to the disclosure (and it is reasonable)? or o Is the disclosure necessary to prevent or lessen a serious and imminent threat to the life or health of an individual?	Where AI technology vendors, platform providers, or any other external organization, will have access to PI being processed by the technology, this could be considered a disclosure, and the organization should ensure it is able to satisfy one or more of the criteria in privacy laws to permit the disclosure. Where organizations provide their contracted service providers, including AI system vendors, with access to PI for the **sole purpose** of carrying out a contracted service on behalf of the agency, this is likely to be a transfer/use. Organizations should also consider whether staff or users of a system may be able to view information of other individuals and implement measures to prevent this or ensure it occurs only with authorization from the individual. Organizations should consider what information needs to be provided to individuals who are users of a system and what consents might be needed if they are partnering with a third-party vendor. In the PIA, organizations should document the disclosures which are intended and the rationale for how they comply with privacy laws. For example, AI vendor tech support is provided by a team of five staff who will have access to all data including PI. This is a directly related purpose to which it may be assumed there is no objection if appropriate contractual obligations, access controls and security measures are in place.

Content of a good AI PIA

Principle	Questions to ask	Considerations and impacts
Safeguarded	o Have you ensured PI relating to an individual's ethnic or racial origin, political opinions, religious or philosophical belief, sexual activities or other sensitive PI are not being disclosed or used inappropriately? • Is the PI being disclosed or otherwise being moved outside Canada? • Consider the location of any third-party providers engaged to support the AI system or project. • In the event the AI system or project involves sensitive PI, can you achieve your objectives without using unique identifiers?	Organizations should refrain from disclosing datasets automatically and should ensure there is human review of data before it is disclosed. Organizations should design systems and processes to remove sensitive information if it is included in chatbot or other free text fields. Organizations may also consider clear user guidance or notifications to deter users from entering sensitive information that is not required. Facial images may be considered 'sensitive information' because it is potentially PI about racial or ethnic origin or can indicate a person's religion. Sensitive information points can be inferred from other PI. Organizations should only use unique identifiers (such as DL number) if it is reasonably necessary to carry out the activity efficiently. If a unique identifier is required, consider a randomly assigned number which is used temporarily for a specific purpose and then deleted.


The next wave of class actions

Quick history of breach class actions

Initially, Canadian courts applied a broad and liberal approach to the certification of data breach class actions (i.e., unauthorized actors gain access to companies' databases and obtain personal information).

Almost any data breach incident would result in a class proceeding.

However, as such incidents became more frequent, the courts began scrutinizing these claims more closely.

This has made it increasingly difficult for plaintiffs to achieve certification in data breach class actions, especially in Ontario and Alberta.

Courts in British Columbia, meanwhile, have shown mixed views on the matter.

As a result, some class action lawyers are shifting tactics.

Rather than targeting breaches by external actors, they are pursuing claims focused on how companies themselves handle personal data—specifically, alleging that businesses are misusing or improperly collecting their customers' information in ways that violate privacy rights.

Historical (2012 – 2022)

A key factor behind the prevalence of data breach class actions was the plaintiffs' ability to use the tort of "intrusion upon seclusion."

This legal claim proved advantageous because it allowed for liability and damages without requiring proof that the plaintiff experienced actual harm.

Jones v. Tsige, 2012 ONCA 32

As a result, plaintiffs faced fewer barriers in getting class actions certified, since courts could move forward with certification even in the absence of evidence that class members had suffered any financial losses.

Post-2022

- The landscape shifted in 2022, when the Ontario Court of Appeal issued three key rulings narrowing the scope of intrusion upon seclusion. The Court found companies whose databases were breached by third-party hackers could not be held liable under this tort because it was the external actors—not the companies themselves—who had intruded upon the privacy of customers.

Owsianik v. Equifax Canada Co., 2022 ONCA 813
Obodo v. Trans Union of Canada, Inc., 2022 ONCA 814
Winder v. Marriott International, Inc., 2022 ONCA 815

- This interpretation later affirmed by the Alberta Court of Appeal.

Setoguchi v. Uber B.V., 2021 ABQB 18

- With intrusion upon seclusion no longer applicable in these circumstances, plaintiffs in Ontario and Alberta have been left to pursue negligence claims. However, these require proof that members of the proposed class actually experienced measurable financial loss.
- Emotional or psychological distress from a breach is not enough on its own to sustain such claims.

Quantz v. Ontario, 2025 ONSC 90

- This legal shift has significantly reduced the number of viable data breach class actions and, as a result, dampened the enthusiasm of class counsel to pursue them.

BC's *Privacy Act*

- The British Columbia Court of Appeal has taken a slightly different approach compared to courts in Ontario and Alberta.
  - While it agreed that the common law tort of intrusion upon seclusion cannot be applied to companies that have been victims of hacking, it left the door open for claims under the *Privacy Act*, which creates a separate privacy tort.
  - Specifically, the Court held that organizations whose systems are breached by third parties may still face liability for violating statutory privacy rights under the BC Privacy Act.

GD v. South Coast British Columbia Transportation Authority, 2024 BCCA 252
Campbell v. Capital One Financial Corporation, 2024 BCCA 253

- In a more recent decision, the court certified only the *Privacy Act* claims and dismissed those based on intrusion upon seclusion, breach of contract, and unjust enrichment.

Hvitved v. Home Depot of Canada Inc., 2025 BCSC 18

- The Court of Appeal also noted that, similar to intrusion upon seclusion, the *Privacy Act* may not require plaintiffs to demonstrate actual harm in order to obtain damages. This suggests that courts in British Columbia may still be open to certifying data breach class actions against companies, even in cases where no quantifiable harm to the class has been shown.

Pivot to Data Misuse Claims

- As traditional data breach class actions face increasing legal hurdles (especially in ON and AB), some class counsel have pivoted toward claims involving alleged **misuse of personal information**. These cases often argue that companies are collecting or using or sharing an individuals' data in ways that are either unauthorized or go beyond what users consented to.

- The legal treatment of these claims remains uncertain.

Some courts have emphasized their gatekeeping function at the certification stage, and have dismissed actions that lacked sufficient merit. In particular, certification has been denied where there was no evidence that a breach had occurred or where the plaintiffs failed to show that class members experienced any compensable harm.

Kish v. Facebook Canada Ltd., 2021 SKQB 198
Chow v. Facebook Inc., 2022 BCSC 137
Simpson v. Facebook, 2021 ONSC 968

On the other hand, some courts appear to be taking a more permissive approach to these kinds of cases at certification. For instance, in a recent proposed class action against Google in B.C., the plaintiff alleged that Google used its facial recognition technology to collect and store users' personal information and made it accessible to third parties, absent sufficient user consent.

Situmorang v Google, LLC, 2024 BCCA 9

Quebec

- The threshold for authorization in Quebec is very low, making it easier for plaintiffs to initiate proceedings.
- Quebec is also seeing a growing number of class actions related to the misuse/mishandling of personal information. These cases commonly involve claims of overcollection of data, unauthorized sharing with third parties, and improper management of sensitive categories of information, such as health or biometric data.
- With new obligation under Law 25 (and a private right of action), class counsel are expected to increasingly rely on this legislation to support their arguments.
- Taken together, Quebec's low barrier to class action authorization and the new provisions of Law 25 will mean a likely uptick in data misuse/mishandling class actions initiated there (and emphasize the importance for businesses to maintain strong privacy compliance and proactive data protection measures).

Next wave of risk

01

Biometrics

02

Use of PI by service providers/third parties to train their AI

03

Complex business models

04

Connectivity (internet of things, partner networks)

05

Transfer vs. disclosure

Where BC privacy law is going

Theme 1: BC PIPA likely to be amended soon

- BC's Personal Information Protection Act (PIPA) governs how provincially-regulated private sector organizations (including businesses and non-profit organizations) collect, use, disclose and retain personal information of individuals (including employees and members of the public) within British Columbia.

- PIPA is subject to mandatory periodic reviews by a special committee of the Legislative Assembly. Special committee reports in 2008 and 2015 included recommendations for numerous changes to PIPA that the Legislative Assembly did not implement.

- In April 2021, the Legislative Assembly appointed a special committee to review PIPA. In December 2021, the Special Committee published a report titled *Modernizing British Columbia's Private Sector Privacy Law* (with 34 recommendations for significant changes to PIPA.

- The BC Privacy Commissioner announced his support for the Report.

Theme 1: BC PIPA likely to be amended soon

The following is a summary of some of the Special Committee's recommendations for amendments to PIPA:

- **Alignment/harmonization:** Align PIPA with the EU GDPR and an amended PIPEDA.
- **New/emerging Issues:** Specifically address issues such as de-identification and re-identification of data, automated decision-making, and biometrics.
- **Consent:** Require explicit consent for sensitive information (e.g., biometric data, medical information, and information about children/youth), align consent exceptions with those in the GDPR.
- **Breach notification:** Introduce mandatory breach reporting/notification.
- **Data portability:** Introduce a right for individuals to obtain their PI in a structured, commonly used, machine-readable format.
- **PIAs:** Require organizations to conduct PIAs for new projects involving sensitive information
- **Employees:** Strengthen employee privacy; address use of employees' personal devices in the workplace.
- **Data controllers/processors:** Confirm that controllers are responsible for the PI they transfer to processors, and require controllers to use contractual or other means to ensure PIPA compliance.
- **Enforcement:** Enhance BC OIPC's enforcement powers, including powers to conduct audits/investigations, issue findings/orders, enter into compliance agreements, and impose penalties.
- **Health information:** Create new legislation for health information in the public and private sectors.
- **Data retention/destruction:** Define data destruction requirements and require data retention periods and methods be stated in privacy policies.

Theme 2: Expansion of reach

PIPA applies extra-territorially

- BC OIPC has won a court case in which confirmed BC PIPA has **extra-territorial application**.
- Privacy Commissioners investigated Clearview AI and make recommendations in their Report. Clearview refused to comply with the Report's recommendations, causing the BC Commissioner to issue an order to enforce the recommendations as they apply to individuals in BC.
- Clearview challenged the order, saying that because it has no employees, offices or servers in B.C., it is not subject to BC PIPA.
- The Court upheld the Commissioner's Order saying BC PIPA applies to out-of-provinces companies that have a "real and substantial" connection to B.C.:
  - Clearview provided services to organizations located in BC, including law enforcement agencies
  - an essential part of Clearview's business is to collect, use and disclose PI from websites, including that of a vast number of individuals in Canada; and
  - Clearview carried out business and marketing in B.C.
- Notably, the Court emphasized that even if Clearview did not market or provide its services in B.C., the **simple act of collecting, using and disclosing personal information of individuals in BC from the Internet would create a sufficient connection to B.C. for BC PIPA to apply to Clearview**.

Clearview AI Inc. v. Information and Privacy Commissioner of British Columbia, 2024 BCSC 23112

Theme 2: Expansion of reach

ALL organizations captured

- BC PIPA applies to all types of organizations.
- BC OIPC ruled a complaint from an individual in respect of the federal political parties could be investigated because, on a plain reading of BC PIPA (which simply refers to “organizations”), even federal political parties were caught.
- Court upheld the BC OIPC’s decision.
- BC Court of Appeal will hear the case this June.

Liberal Party of Canada v The Complainants, 2024 BCSC 814

Theme 3: Focus on children's privacy

Consistent with global themes
BC OIPC previously expressed enthusiasm for UK Children's Code (design practices)

Thank You!

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

Emma Irving
Partner, Vancouver
+1 604 648 6502
Emma.irving@dentons.com

Mitch Bringeland
Associate, Vancouver
+1 604 629 4991
Mitch.bringeland@dentons.com

DENTONS

Thank you for attending!

Dentons On-Demand

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.