DENTONS

WEBINAR SERIES

KEEPING UP WITH

CROSS-BORDER CLASS ACTIONS

Part 4:
Perspectives on data privacy from North America

June 12, 2025

Moderator:

Matthew Fleming
Partner, Toronto, Canada
+1 416 863 4634
matthew.fleming@dentons.com

Speakers:

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

Peter Stockburger
Partner, San Diego, United States
+1 619 595 8018
peter.stockburger@dentons.com

Canadian perspective

Privacy class action trends

Quick history of privacy 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.

Shifting landscape – 2022

- Prior to 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.

- The landscape started to shift 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 has intruded upon the privacy of customers: See *Owsianik v. Equifax Canada Co.,* 2022 ONCA 813.

- This interpretation was also confirmed by the Alberta Court of Appeal: *Setoguchi v. Uber B.V*., 2021 ABQB 18.

British Columbia charts its own course

- The British Columbia Court of Appeal has taken a slightly different approach.
  - While it had 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*: See *GD v. South Coast British Columbia Transportation Authority*, 2024 BCCA 252 and *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.

Cleaver v. The Cadillac Fairview Corporation Limited, 2025 BCSC 910
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 claims

- 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 obligations 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).

Risk areas to watch

01

Transfer vs Disclosure - including use of PI by service providers/third parties to train their AI

02

Complex business models and Connectivity

03

Scope of Consent

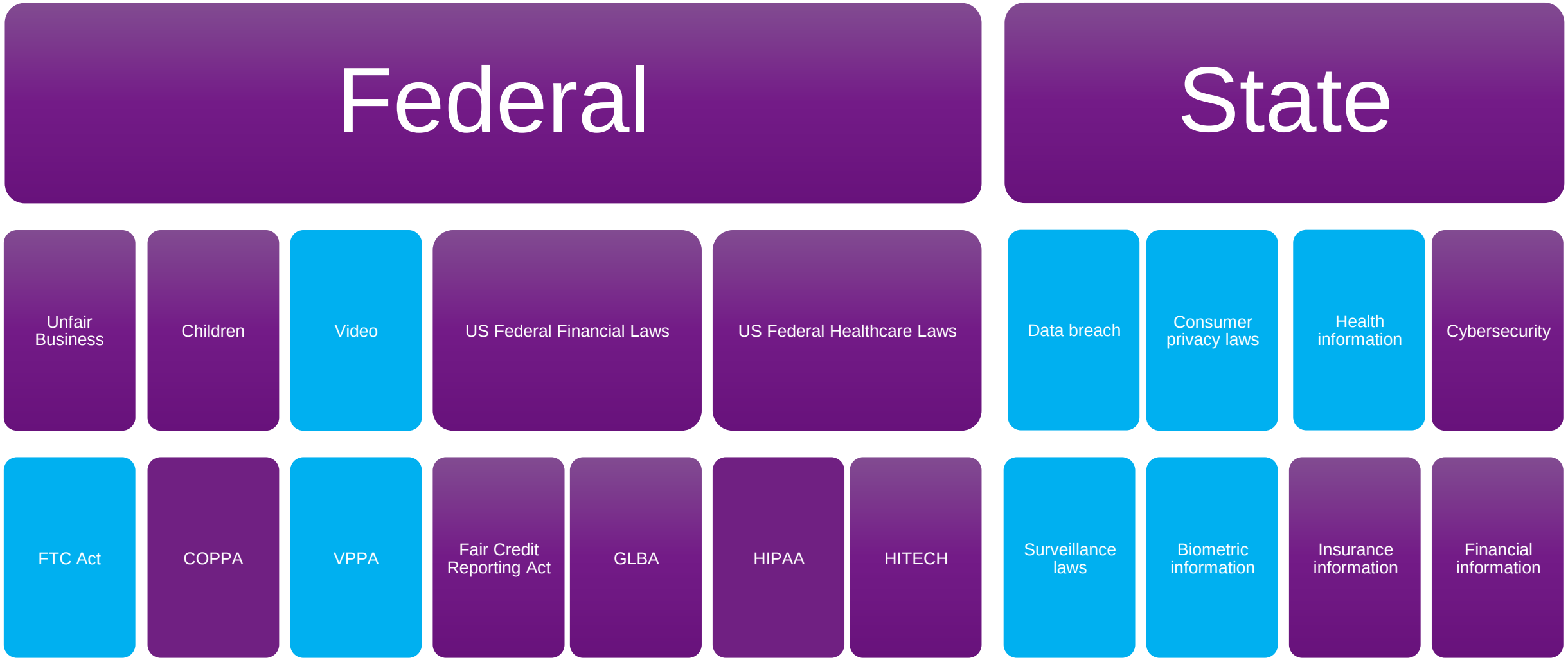
04

Regulatory updates and changes

US perspective

Privacy class action trends

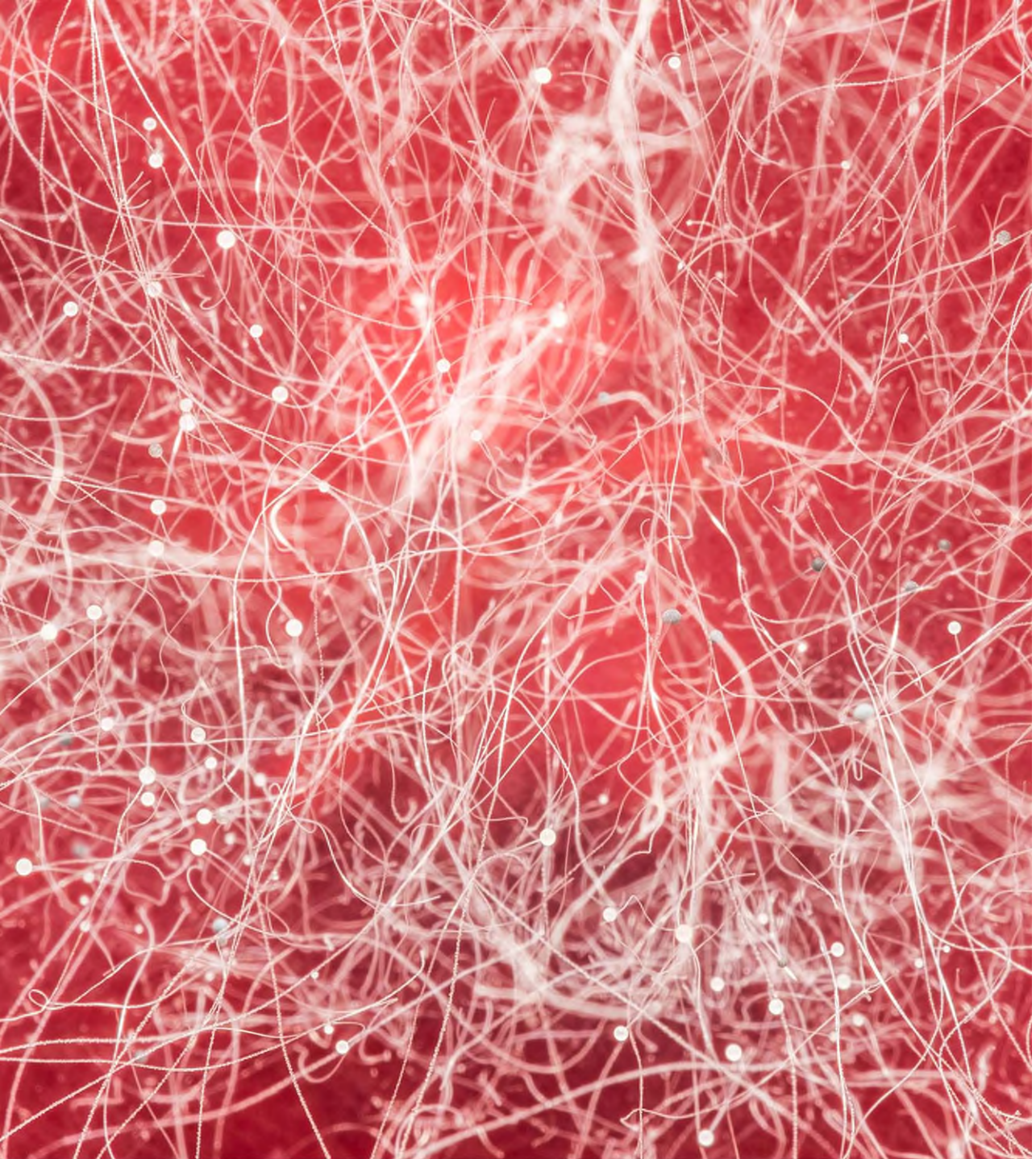
US privacy landscape



Website videos

Video Privacy Protection Act (VPPA)

- **Scope**. Federal legislation passed in 1998 following Bork video rental story. Permits a private right of action by a “consumer” against a “video tape service provider” for disclosing video watching history without consent.
- **Modern application**. Websites, mobile applications, and other video watching platforms.
- **Widespread litigation and penalties**. Lawsuits are increasing.
- **Mitigation**. Consumer minimizing the sharing of title of video or other content with third party advertising and marketing partners.



Cookies and pixels

Eavesdropping and wiretapping

- **Scope**. Several states (e.g., CA, MA, FL) have laws that prohibit third parties from engaging in "wiretapping" or "eavesdropping" on electronic communications without the consent of participants. Emerging "trap and trace" theory.
- **Modern application**. Websites, mobile applications, and other platforms deploying cookies, pixels, and other third-party tracking technologies.
- **Widespread litigation and penalties**. Lawsuits are increasing. Thousands of lawsuits and demand letters distributed.
- **Mitigation**. Consider a cookie banner and obtaining consent.

Genetic information

GINA and GIPA

- **Scope**. Genetic Information Nondiscrimination Act of 2008 (GINA) and the Illinois Genetic Information Privacy Act (GIPA) prohibit employers and other covered entities form requesting or requiring genetic information of an individual or family member of the individual, and prohibit discrimination based on the same.
- **Lawsuits**. A rise in lawsuits due to employers that require applicants or employees to undergo pre-employment physicals. EEOC focus under prior administration.
- **Mitigation**. Carefully interrogate the level of medical information being obtained from job applicants and employees.

Credit card information

Song-Beverly Credit Card Act

- **Legal requirement**. Enacted in 1971, the law prohibits retailers from requesting a consumer's "personal identification information" (PII) during or before a credit card transaction. PII is defined as any information that is not set forth on the credit card, such as address and telephone number.
- **Exceptions**. Verify identity or use for shipping, delivery, or servicing.
- **Lawsuits**. Multiple class action complaints have been filed against name brand retailers.
- **Mitigation tip**. Use the word "optional" or make clear the information is being used for shipping only. Ensure information is not used for secondary purposes on the backend.

Biometric information

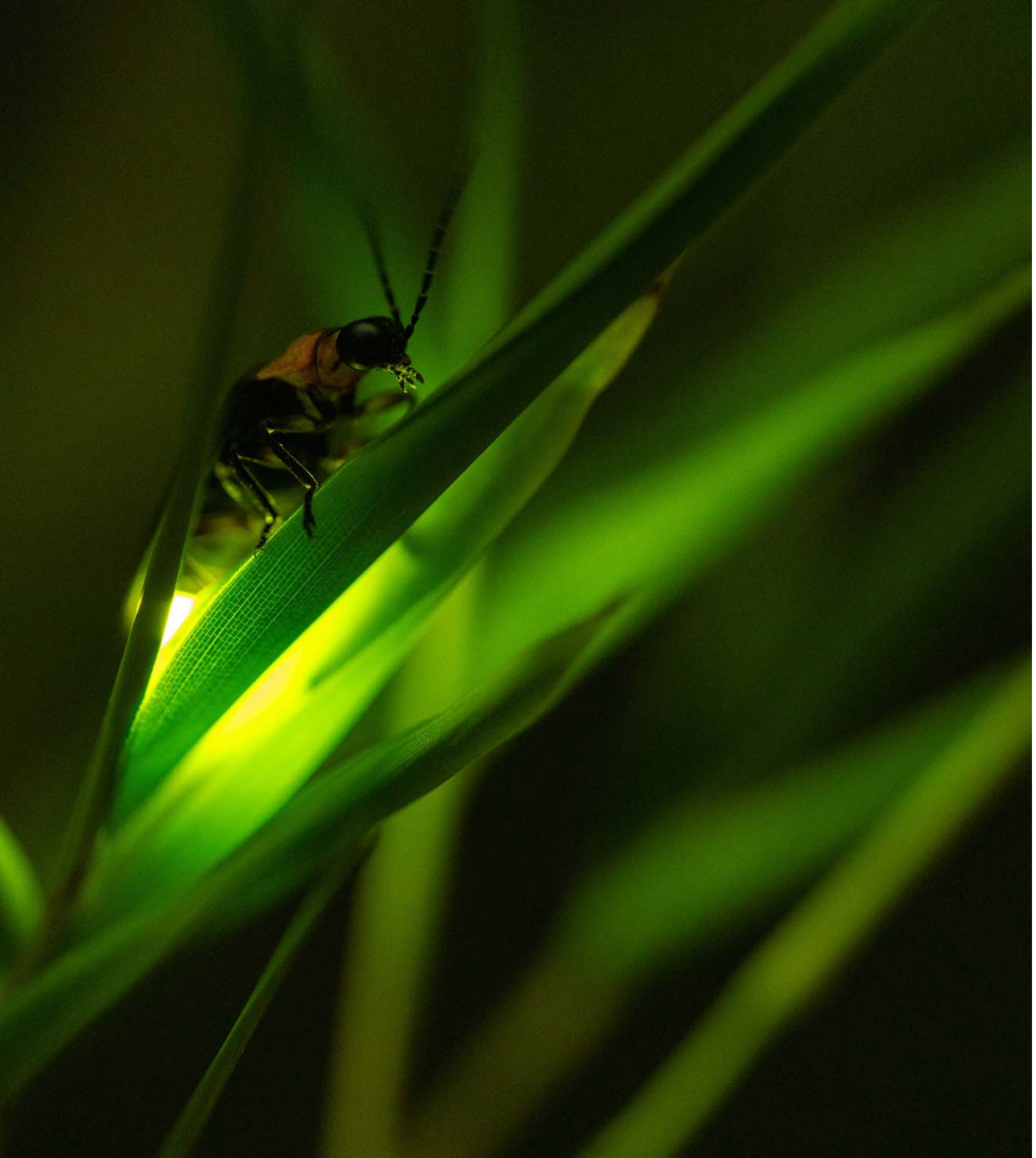
Lawsuits and risk

- **Scope**. Illinois Biometric Privacy Act has been the leading edge on plaintiffs' suits. Other states have laws (e.g., WA, TX, etc.) but no private right of action.
- **Modern application**. Employee face or fingerprint scan, consumer face scan on mobile application, increasing use of biometrics in retail contexts.
- **Widespread litigation and penalties**. Lawsuits and high penalties present a significant risk.
- **Mitigation**. Provide clear notice, obtain consent, and limit retention.

Cybersecurity

Data breach litigation

- **Reasonableness standard**. Nearly every state and regulatory regime requires organizations to maintain "reasonable" security controls around sensitive personal information. Lawsuits have been common post-breach for years.
- **Varied claims**. The claims that can arise from a data breach include negligence, breach of contract, or failure to maintain reasonable security.
- **Key issues**. Standing, offering of free credit, timing, and ignoring risk.
- **Risk mitigation**. Consistently interrogate cybersecurity controls and frameworks to ensure "reasonableness" is defensible.



Emerging trends

Health and AI

- **Washington**. Washington My Health My Data Act is in effect. Private right of action. Strict compliance regime over the collection and use of health data.
- **California**. Emerging trend of “Shine the Light” demand letters. Pre-litigation strategy emerging.
- **Misconfiguration**. Emerging trend of lawsuits alleging that the cookie banner does not operate as advertised (i.e., misconfiguration suits).
- **AI lawsuits**. Emerging trend on lawsuits relating to privacy breach re: training and eavesdropping re: agentic AI deployment.

Thank you

Matthew Fleming
Partner, Toronto, Canada
+1 416 863 4634
matthew.fleming@dentons.com

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

Peter Stockburger
Partner, San Diego, United States
+1 619 595 8018
peter.stockburger@dentons.com