大成 DENTONS

DENTONS IN SESSION
CPD WEBINAR SERIES

# Critical developments in data 2.0

Kelly Osaka, Partner, Calgary
Chloe Snider, Partner, Toronto
Karl Schober, Senior Associate, Toronto
Luca Lucarini, Associate, Toronto

# Our presenters

**Kelly Osaka**
**Partner, Calgary**
**+1 403 268 3017**
**kelly.osaka@dentons.com**

**Karl Schober**
**Senior Associate, Toronto**
**+1 416 863 4483**
**karl.schober@dentons.com**

**Chloe Snider**
**Partner, Toronto**
**+1 416 863 4674**
**chloe.snider@dentons.com**

**Luca Lucarini**
**Associate, Toronto**
**+1 416 863 4735**
**luca.lucarini@dentons.com**

大成 DENTONS

DENTONS IN SESSION
CPD WEBINAR SERIES

# PHIPA amendments

Luca Lucarini, Associate, Toronto

# The *Personal Health Information Protection Act* (PHIPA)

## Summary

- Ontario's *Personal Health Information Protection Act* (PHIPA) regulates the collection, use, and disclosure of **personal health information** ("PHI").
- PHIPA applies to PHI in the custody or control of:
  - **Health information custodians** ("custodians")
  - **Agents** of custodians
  - **Electronic Service Providers** ("ESPs")
  - **Health Information Network Providers** ("HINPs")

# PHIPA amendments

## Bill 188, *Economic and Fiscal Update Act, 2020*

1) Electronic audit logs
2) De-identification
3) Right to access PHI in electronic form
4) Consumer electronic service providers
5) Enhanced enforcement

# PHIPA amendments

## 1) Electronic audit logs

- Custodians using **electronic means** to collect, use, or disclose records of PHI must maintain **electronic audit logs**
- The logs must account for **every instance** where PHI is viewed, handled, modified, or otherwise dealt with
- Custodians must **audit** and **monitor** the logs
- IPC may compel **production** of the logs

# PHIPA amendments

## 1) Electronic audit logs

### Log content

- The type of PHI
- Date and time
- Identity of those accessing PHI
- Identity of individual to whom PHI relates

# PHIPA amendments

## 1) Electronic audit logs

### How to prepare

- **Inventory** electronic systems containing PHI
- **Assess** auditing capability of systems
- **Identify** priorities for creating or upgrading capabilities
- **Explore** audit log solutions

# PHIPA amendments

## 2) De-identification standards

- The definition of “**de-identify**” will be changed to mean “to remove, in accordance with such **requirements as may be prescribed**, any information**”**
- Other rules affected:
  - s. 11.2(1): prohibition on “re-identification”
  - s. 47(2): Disclosure to **health data institutes** for analysis of health system
- Information and Privacy Commissioner of Ontario, *De-identification guidelines for structured data* (June 2016)

# PHIPA amendments

## 3) Right to access PHI in electronic format

- PHIPA Decision 29 (June 8, 2016) : No right to request access of PHI in any particular medium
- Individuals will be able to request their records in electronic format meeting **requirements to be prescribed**

# PHIPA amendments

## 4) Consumer electronic service providers

- New entity: “**consumer electronic service provider**” (“CESP”)
- CESP: “a person who **provides electronic services to individuals at their request**, primarily for the purpose of allowing those individuals to access, use, disclose, modify, maintain or otherwise manage their records of PHI, (or for such other purposes as may be prescribed).”
- Both CESPs and custodians providing PHI to CESPs will be required to comply with requirements to be prescribed

# PHIPA amendments

## 4) Consumer electronic service providers

- IPC may issue order to cease providing PHI
- CESP may collect and use health numbers
- Custodian receiving a request for access to records of PHI from a CESP is not required to provide PHI to CESP in responding to request

# PHIPA amendments

## 5) Enhanced enforcement

### Administrative penalty regime

- IPC may now make order requiring any person to pay an administrative penalty for contravening PHIPA

### Penalties for offences doubled

- Maximum fines for offences for contraventions of PHIPA doubled from $100,000 to $200,000 (individuals) / $500,000 to $1,000,000 (organizations)
- Possibility of 1 year imprisonment

大成 DENTONS

DENTONS IN SESSION
CPD WEBINAR SERIES

# Internet-of-things guidance

Luca Lucarini, Associate, Toronto

# Internet-of-things

- **Internet-of-things devices**
  - “smart” appliances for use in the home such as lighting systems, smoke alarms, TVs, doorbells, locks, speakers, security cameras, thermostats, and air quality monitors;
  - connected cars, toys, watches, and health trackers
- **What do these devices collect?**
  - Heart rate, body temperature, movement
  - Temperature or energy usage in the home
  - Voice and facial recordings
  - Geolocation data
  - Behavioural patterns

# Internet-of-things

## Commissioner's guidance

- Office of the Privacy Commissioner, *Privacy guidance for manufacturers of Internet of Things devices* (August 2020)

# Internet-of-things guidance

## Identifying purposes and openness

- Principle 2 of PIPEDA ‘Identifying Purposes’: organizations to **identify purposes** for which personal information is collected
- Principle 8 of PIPEDA ‘Openness’: organizations to **make readily available specific information** about its policies and practices relating to the management of personal information

# Internet-of-things guidance

## Identifying purposes and openness

- Privacy policies in product packaging and product website
- Active notification about device's privacy policy
- Privacy policy to include:
  - List of device sensors,
  - Length of time the device will receive security updates
  - Whether ongoing updates to safeguard consumer information
- Use product design to communicate information handling practices
  - E.g. reminders that device is capturing information

# Internet-of-things guidance

## Limiting collection and retention

- Principle 4 of PIPEDA ‘Limiting Collection’**:** collection of personal information shall be **limited to that which is necessary** for the purposes identified by the organization.
- Principle 5 of PIPEDA ‘Limiting Retention’: Personal information shall be retained **only as long as necessary** for the fulfilment of purposes for which it was collected.

# Internet-of-things guidance

## Limiting collection and retention

- Limit collection through product design
- Consider information necessary for the device to function
  - E.g. smart speaker that collects audio data can require a triggering event to activate – preferable to continuous collection
- Enable consumer to control amount of information collected
  - E.g. ‘do-not-collect’ switch in form of mute button or software toggle
- Where information is collected over and above what is needed for the device to function, such collection should be communicated to the consumer and consent obtained for the collection.

# Internet-of-things guidance

## Safeguards

- Principle 7 of PIPEDA ‘Safeguards’: organizations to maintain **appropriate physical, technical and administrative safeguards** over personal information.

# Internet-of-things guidance

## Safeguards

- Design devices to minimize risk of breaches:
  - Limit microphone sensitivity and range;
  - On/off mute control;
  - Audio filter
  - Camera disable function
  - User option to take device offline
  - User option to disassociate and remove identifying information

# Internet-of-things guidance

## Safeguards

- Encryption
- Ongoing assessment
- No default passwords
- Password standards
- Factory reset / wipe; and
- Regular firmware updates

# Internet-of-things guidance

## Safeguards: third party vendors

- Revisit vendors agreements to assess component security
- For new suppliers – vet source code
- Remember – manufacturers ultimately accountable

大成 DENTONS

DENTONS IN SESSION
CPD WEBINAR SERIES

# Legislative overhaul and a new watchdog: A bedtime story

Karl Schober, Senior Associate, Toronto

# Competition Bureau expands its oversight into privacy/data

- First enforcement action against social media platform; $9 million penalty
- Section 74.01(1) of the Competition Act – the truth in advertising provisions
- What does “free” really mean?
- “in a material respect”
- Key takeaways

# Canada’s privacy modernization

- PIPEDA 2.0
- British Colombia, Alberta…and Ontario?
- Quebec Bill 64 – *An Act to Modernize Legislative Provisions Respecting the Protection of Personal Information*

大成 DENTONS

DENTONS IN SESSION
CPD WEBINAR SERIES

# Privilege update

Chloe Snider, Partner, Toronto

# Privilege

## Protecting expert reports post breach

- When responding to a cyberattack, an organization will likely need to retain external cybersecurity, ransomware or digital forensics experts.
- Any expert report may become the **subject of a production request** by either a regulator or a plaintiff in litigation.
- Anything produced to a regulator may become public through an access request.
- Importance of considering **in advance** if and how such work product may be protected by **privilege** – so that there is evidence to support a claim of privilege.

# Privilege

## PHIPA Decision 114 – March 30, 2020

Facts

- Cyber attackers penetrated the networks of one of Canada's largest health diagnostics companies and extracted data and demanded a ransom.
- In its investigation following the breach, the Information and Privacy Commissioner of Ontario (IPC) requested certain documents, including:
  - An incident report generated by a CrowdStrike (a cybersecurity IT company);
  - A penetration test conducted by CrowdStrike after the incident; and
  - Communications between the cyberattackers and Cytelligence (a firm retain to engage the cyberattackers).
- The company asserted litigation and solicitor-client privilege over the documents.

# Privilege

## PHIPA Decision 114 (cont'd)

Decision

- IPC found that the **documents were not protected by litigation privilege** – there was insufficient evidence that the documents had been created for the dominant purpose of litigation:
  - Company would have had to respond to the incident under its statutory obligations to identify, contain, investigate and remediate potential privacy breaches; and
  - IPC characterized actions taken in response to these obligations as "operational needs" independent of litigation.
- IPC also found that **documents were not protected by solicitor-client privilege** as the company did not:
  - Explain which of the communications (if any) were made to/from either in-house or external counsel; or
  - How they were made for the purpose of seeking or giving legal advice.

# Privilege

## U.S. District Court for the Eastern District of Virginia: Privilege Decision (E.D. Va., No. 1:19-md-02915)

- U.S. judge **ordered a financial institution to disclose a forensic report prepared by a third party cybersecurity consultant following a data breach.**
- The judge rejected the claim that because its law firm formally engaged the expert following the breach and the report was delivered to counsel, the report was entitled to work product protection.
    - Company failed to establish that the report would not have been prepared in substantially the same form but for the prospect of litigation; and
    - The preparation of the report was called for by a **pre-existing statement of work** between the company and the expert, and **distributed to many non-legal employees of the bank as well as external auditors and regulators**.

# Privilege

## Takeaways

- Consider privilege issues at the time of retaining an expert.
- Engage external counsel as soon as possible:
  - This emphasizes the *legal (and litigation)*, rather than the *business or operational,* nature of the advice.
- **Expert retainers and communications should be through counsel so that, where appropriate, steps can be taken to show the communications and report were prepared in the context of impending litigation and/or seeking legal advice.**
  - Retainers with third-party experts should be carefully worded and have their scope precisely defined – can reference defending anticipated litigation.
  - Have a **separate retainer** from any existing retainer. It should distinguish between the post-security incident services from previous services.
  - **Communications should be through counsel** and marked as privileged.
  - This should be treated as a **legal expense**.

# Privilege
## Takeaways

- **Limit sharing of privileged material within the organization**
  - The report should only be shared as necessary – and only for legal purposes (not business purposes).
  - Consider copying counsel and marking communications and documents as privileged and confidential (although not determinative).
- **Limit sharing externally**
  - Voluntary production could constitute waiver of privilege.
  - Avoid inadvertent references to the report and findings.

大成 DENTONS

DENTONS IN SESSION
CPD WEBINAR SERIES

# Private Right of Action

## Statutory tort regimes across Canada

Kelly Osaka, Partner, Calgary

# Provincial privacy legislation – statutory torts

| | British Columbia | Manitoba | Saskatchewan | Newfoundland and Labrador |
|---|---|---|---|---|
| **Provincial Legislation:** | *Privacy Act*, RSBC 1996, c 373 | *The Privacy Act*, RSM 1987, c P125 | *The Privacy Act*, RSS 1978, c P-24 | *Privacy Act*, RSN 1990, c P-22 |
| **Common Elements:** | • In each province, it is a tort to **violate a person's privacy without a claim of right**.<br>• In each province, **proof of damages is not a required element** of the tort.<br>• The violation must be **wilful** in BC, SK, and NL.<br>• In BC, SK, and NL, "**the nature and degree of privacy to which a person is entitled** in a situation or in relation to a matter **is that which is reasonable in the circumstances**, giving due regard to the lawful interests of others."<br>• In each province, the **unauthorized use of the likeness** of a **person for the purposes of advertising** is a tort. | | | |
| **Common Defences:** | • In each province, **defences to the tort include**, inter alia, **consent** (express or implied), **defence of person**/property, **authorized by law**, and otherwise lawful **journalistic publications**. | | | |
| **Derogation from other Rights of Action** | • In SK, MB, and NL, **the statutory tort does not derogate from any other right of action** available to a plaintiff. | | | |

# Common law right of action in British Columbia

- There is a series of **British Columbia Court of Appeal cases** which are often cited for the proposition that is **no common law right of action for breach of privacy** in BC

- ***Tucci v Peoples Trust Company***, 2020 BCCA 246 makes clear that **a common law right of action for breach of privacy may exist in BC.**

- In *Tucci*, the British Columbia Court of Appeal stated that:

  "The thread of cases in this Court that hold that there is no [common law] tort of breach of privacy, in short, is a very thin one. There has been **little analysis in the cases**, and, in all of them, the **appellants failed for multiple reasons**."

# Common law right of action in British Columbia

- The Court in *Tucci* stated:

  "Today, **personal data has assumed a critical role in people's lives**, and a failure to recognize at least some limited tort of breach of privacy may be seen by some as anachronistic. For that reason, **this Court may well wish to reconsider** … **the issue of whether a common law tort of breach of privacy exists in British Columbia**."

- The BCCA in *Tucci* **strongly signals** that **a common law right of action may exist** in parallel with the statutory tort.

# Corporations' rights under statutory torts

- The question of whether a corporation has a right of action under the BC statutory tort arose in ***Madco Investments Ltd v Western Tank & Lining Ltd***, 2017 BCSC 219.
- The Court in *Madco* undertook an exercise in **statutory interpretation**, and concluded that, under the BC *Privacy Act*, **corporations may commence a claim under the statutory tort for breach of privacy**.
- Even in jurisdictions where a corporation can bring a claim, the **claim should be based on the interests of the corporation**, and not solely that of others including employees. See *Facilities Subsector Bargaining Association v BCNU,* 2009 BCSC 1562 at para 62

  "Plaintiffs have no entitlement to bring an action based on a violation of another person's privacy."

大成 DENTONS

DENTONS IN SESSION
CPD WEBINAR SERIES

# Class action lawsuits in the privacy context

Chloe Snider, Partner, Toronto

# Class actions – categories

## Cases involving third party hackers – examples:

- Anonymous hacker accessed a defendant's computer system, took personal information of customers, employees and suppliers and, when ransom demands were not met, posted the information on the internet; and
- Cybercriminals gained unauthorized access to defendant's databases, took user personal information, and attempted to solicit money and information.

## Cases involving employees – examples:

- **Innocent loss of data:** loss a storage device with personal information.
- **Intentional misconduct:** a "rogue" employee intentionally took personal information collected by his employer in an effort to seek retribution or otherwise harm the employer.

## Cases involving use without consent – examples:

- Defendant alleged to have use class members' names and images without their knowledge or consent in an advertising program.
- Defendant alleged to have used personal information of customers for a marketing initiative.

# Class actions – vicarious liability

- Exception to the common law principle that only the participants of unlawful conduct are legally bound by their actions
- Liability imposed by common law resulting from the following:
  - A tortious act or omission by another;
  - Some relationship between the actual tortfeasor and the defendant whom it is sought to make liable; and
  - Some connection between the tortious act or omission and that relationship.
- Three exceptions that qualify as the relationship included in the second bullet:
  1. Master and servant
  2. Principal and Agent
  3. Employer and independent contractor

# Class actions – vicarious liability

- There has not yet been a merits decision in Canada on vicarious liability in the privacy context – BUT:
  - Privacy class actions involving claims of vicarious liability have been **certified**.
  - Companies should be aware of the **significant risk posed by internal actors** and should take steps to protect against such risks.
- Recent decision of the UK Supreme Court (April 2020) denying liability :
  - **Court declined to find that the defendant was vicariously liable for rogue employee's theft of payroll data** of nearly 100,000 employees, which he posted online in to harm the company.
  - Court considered whether tortious acts were sufficiently closely connected to his employment by the company and his employment duties, that it would be fair and just to hold the company vicariously liable for the same
  - Employee was acting distinctly from his employer's interests, not furthering them.

# Class actions – vicarious liability

*Ari v Insurance Corporation of British Columbia,* 2020 BCSC 1087

- Class action against insurance company – former employee accessed and sold personal information of the insurer's customers to a criminal organization resulting in arson, shooting and vandalism attacks on the homes of customers.
- Action was certified: **the vicarious liability claims were not bound to fail**.
- **6 years after class action was started**, and after certification, **insurer issued a third party notice** against former employee and vandals, seeking contribution and indemnity.
- Plaintiff and third party applied for a declaration that the notice was a nullity because it was filed out of time and without the leave of the court.
- **Court denied leave to file the third party notice and set it aside**. The question of whether a class proceeding should include third party claims should be raised at or before certification.
- Court dismissed the insurer's application to have the class action and separate action against the third parties heard at the same time.

# Class actions – carriage motions

- The court may, if there are multiple proceedings involving the same or similar subject matter and some or all of the same class members, permit one to proceed and stay the others… (*Class Proceedings Act, 1992*)
- In 2020, the Ontario Superior Court of Justice decided carriage issues in two different sets of class actions that involved data breaches.
  - *MacBrayne v LifeLabs Inc*., 2020 ONSC 2674: The main factors considered in determining the carriage motion in this case were: (1) overall approach; and (2) proposed fee arrangements.
  - *Del Giudice v Thompson*, 2020 ONSC 2676: The ultimate deciding factor was the case theory of each class counsel.
- This may be a sign of the importance and prevalence of privacy class actions among the class actions bar.

# Class actions – Ontario Bill 161

## *Smarter and Stronger Justice Act*, 2020

- Introduces changes to the *Class Proceedings Act, 1992.*
- Purpose: to make class actions more fair, transparent and efficient.
- Came into force on October 1, 2020.
- Changes to test for certification, which may make it **more onerous**: A class proceeding is the preferable procedure for the resolution of common issues only if, at a minimum,

a) it is **superior to all reasonably available means of determining the entitlement of the class members** to relief or addressing the impugned conduct of the defendant… and

b) the questions of fact or law common to the class members **predominate** over any questions affecting only individual class members.

大成 DENTONS

DENTONS IN SESSION
CPD WEBINAR SERIES

# Regulatory update

Kelly Osaka, Partner, Calgary

# Mandatory breach notifications 2019-2020 Annual Report

## Breaches of Security Safeguards

- 2019-2020 was the first full year of mandatory breach reporting under PIPEDA (previously organizations reported breaches to the OPC on a voluntary basis)

- An organization subject to PIPEDA must report to the OPC any breach of security safeguards involving personal information under its control **if it is reasonable in the circumstances to believe that breach creates a real risk of significant harm to the individual**

- To determine if a breach meets the threshold, organizations must consider:
    - the sensitivity of the personal information involved; and
    - the probability that the personal information has been, is being, or will be misused.

# Mandatory breach notifications 2019-2020 Annual Report

## Statistics

- In 2019-2020, the OPC received 678 breach reports with 87% appearing to have met the mandatory breach notification threshold [OPC 2019-2020 Annual Report to Parliament on the *Privacy Act* and *Personal Information Protection and Electronic Documents Act*]

- Examples of breaches include:
  - unauthorized access by malicious actors or insider threats, often as a result of employee snooping or social engineering hacks
  - malicious actors using social engineering to take over a customer's phone number and gain access to their phone calls and text messages
  - employees make errors when emailing or mailing personal information, or fail to follow an authentication process

- Targeted social engineering campaigns involving phishing and impersonation schemes continue to be a leading cause of breaches

# Global transfer of data 2019-2020 Annual Report

- **Organizations transferring personal data to third parties**, including to those which are across international borders, **are responsible for the protection of that information** under Principal 4.1.3 of Schedule 1 set out in the PIPEDA.

- **Principal 4.1.3** requires that the transferring organization **use** "**contractual or other means to provide a comparable level of protection** while the information is being processed by a third party".

- The Office of the Privacy Commissioner (OPC) guidance on protecting cross boarder data transfers states that "**comparable level of protection**" **means** that the personal information should receive **generally equivalent protection** while **under the control of the third party**, **as it would receive had it not been transferred**. Although, "comparable level of protection" does not mean that the protection should be generally equivalent.

# Global transfer of data 2019-2020 Annual Report

- The OPC investigated a financial institution and **found that the technological controls, coupled with the terms of its contract with the third party service provider and associated monitoring and enforcement** of those contractual requirements provided a level of protection comparable to that set out in the 2009 guidelines

- Good practices included:

  - Undertaking a **risk assessment** prior to signing a contract to identify and mitigate potential risks

  - Requiring the service provider to **control its work environment** to prevent copying or sharing information

  - Using contractual terms and robust safeguards to **strictly limit the service provider's access to and use** of personal information; and

  - Proactively **monitoring the service provider's safeguards** and practices to ensure compliance with the contract

# Global transfer of data 2019-2020 Annual Report

- OPC investigated a grocery store regarding the collection and use of personal information for the purposes of cross-border data transfers
- The investigation found that the grocery store was **sufficiently transparent** about its cross-border data transfers in it written communications to customers
- The organization was not required to obtain additional consent to transfer name and address information to the third party provider for processing as it had **already obtained consent to use the information for the purpose** for which it was to be used by the processor
- The grocery store agreed to take steps to **limit the sensitive personal information** it was collecting as part of the program

# Upcoming Events

Dentons in Session

**Tuesday, November 24** - Budgeting for privacy modernization – what every company needs to know

**Thursday, December 3** - Lessons learned from the GDPR

# Thank you

**Kelly Osaka**
**Partner, Calgary**
**+1 403 268 3017**
**kelly.osaka@dentons.com**

**Karl Schober**
**Senior Associate, Toronto**
**+1 416 863 4483**
**karl.schober@dentons.com**

**Chloe Snider**
**Partner, Toronto**
**+1 416 863 4674**
**chloe.snider@dentons.com**

**Luca Lucarini**
**Associate, Toronto**
**+1 416 863 4735**
**luca.lucarini@dentons.com**