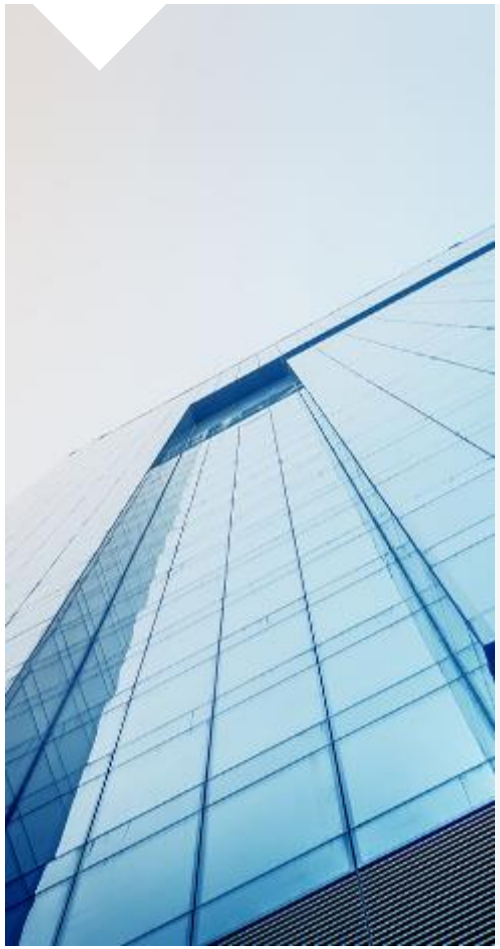
mcmillan

McMillan's Annual Privacy, Data Protection and Cybersecurity Seminar

November 10, 2021

Agenda



- Regulatory Guidance, Investigations and Litigation – What's New?
- Hot Topic #1 - Privacy in a Pandemic
- Hot Topic #2 - Data Breaches
- Hot Topic #3 -Using Technology to Aggregate & Anonymize Data
- Legislative Update - Recent and Anticipated Changes to Federal and Provincial Privacy Legislation
- Q&A

mcmillan

Regulatory Guidance, Investigations and Litigation – What's New?

Speakers:

Kristen Pennington, Gurp Dhaliwal, Julia Loney, Marie-Eve Jean, and Robbie Grant

Joint Investigation of Clearview AI, Inc.

Citation: *OPC PIPEDA-039525 / CAI QC-1023158 / OIPC BC P20- 81997 / OIPC AB-015017*

Joint investigation conducted by the following privacy regulators:

- Federal - the Privacy Commissioner of Canada (OPC)
- British Columbia - the Information and Privacy Commissioner for British Columbia (OIPC BC)
- Alberta - the Information and Privacy Commissioner of Alberta (OIPC AB)
- Québec - the Commission d'accès à l'information du Québec (CAI)

Joint Investigation of Clearview AI, Inc.

- Key Takeaways:
  - A physical presence in Canada isn't necessary for Canadian privacy laws to apply
  - Just because personal information is ostensibly "public" doesn't mean there are no restrictions on its collection and use
  - Biometric data is highly sensitive personal information, and express consent to collect, use and disclose such information is generally required

Alberta Investigation of Babylon

Citation: *Investigation Report P2021-IR-02*

- Two investigations: one under HIA (health privacy legislation) and one under PIPA (private sector privacy legislation)

- Key Findings:
  - Collection and use of certain information is more than what is reasonable for some purposes
  - Simpler methods exist which would be consistent with law
  - Problems with privacy policy
  - Problems with policies and practices re: collection, use, disclosure and storage of information, international service providers, and notices
  - Insufficient consent mechanisms

Alberta Investigation of Babylon

- Key Takeaways:

  - Privacy policies must:
    - be accessible, well drafted and current;
    - reflect jurisdiction(s) where business is being conducted;
    - accurately define personal information to be collected and purpose(s) for collection;
    - state when/how/why personal information is used, disclosed or stored outside Canada

  - Practices and operations must align with privacy policy and be consistently implemented

Alberta Investigation of Babylon

- Key Takeaways (cont'd):
  - Service providers must be aware of PIPA obligations
  - Organization is responsible for PIPA compliance of any service provider collecting, using or disclosing personal information on organization's behalf
  - Consent:
    - there is a difference between opt-out, implicit, explicit
    - muddled purposes and omnibus consent (particularly where integral vs. optional service)
    - individual cannot consent to unreasonable purpose

Owsianik v. Equifax Canada Co.

- Citation: *Owsianik v. Equifax Canada Co., 2021 ONSC 4112*

- Key Finding: Suggests tort of "intrusion upon seclusion" not available in cases where organizations suffer data breach at the hands of third party hackers

image: Flaticon.com

Owsianik v. Equifax Canada Co.

What is intrusion upon seclusion?

- Covers intentional or reckless invasions of personal privacy which a reasonable person would regard as highly offensive
- Available without proof of damages
- Until *Equifax*, no settled case law on whether businesses who are the victim of third party hackers can be liable

image: Flaticon.com

Owsianik v. Equifax Canada Co.

- Organizations can still be liable for breach of contract, negligence, and breach of consumer protection laws
- Organizations can also still be in breach of privacy legislation, which may come with fines or penalties
- Open question whether organizations can be vicariously liable for intrusion upon seclusion perpetrated by their own employees

image: Flaticon.com

Alberta Recognizes Tort of Public Disclosure of Private Facts

Citation: *ES vs Shillington, 2021 ABQB 739*

- Key Takeaways:
  - Organizations must implement appropriate safeguards to prevent breaches of personal information
  - Consider what is included in "private life"

Quebec's Guidelines re: Biometric Data

What is biometric data?

- Techniques used to analyze one or more of a person's unique physical/ morphological, behavioral or biological characteristics
- Highly sensitive information
- Automation of identification and authentication processes

Quebec's Guidelines re: Biometric Data

What are the risks?

- Highly sensitive personal information - permanent, distinctive and unique
- Allows an individual to be identified
- Can be used to deduce information other than a person's identity
- High risks in relation to identity theft
- If a database does not comply with the Commission's orders, or if it constitutes an invasion of privacy, the Commission can order its destruction

Quebec's Guidelines re: Biometric Data

Key Takeaways:

- Step 1: Conduct a privacy impact assessment before implementing a biometric system
  - Question the necessity of collecting biometric data
  - Purpose must be important, legitimate and real
  - Data collected must be proportional to use

- Step 2: Before implementing a biometric system, disclose project to the Commission

Biometric Data – What should we do?

Key Takeaways (cont'd):

- Step 3: Fulfill various obligations under privacy legislation during the implementation of the project
  - Obtain manifest consent from data subjects
  - Confirm individual identities
  - Assess whether other means of identification are available and offer such alternative means
  - Comply with the purpose for which the data is collected
  - Implement confidentiality and security measures
  - Ensure the safe and definitive destruction of information
  - Implement process for right of access and rectification requests

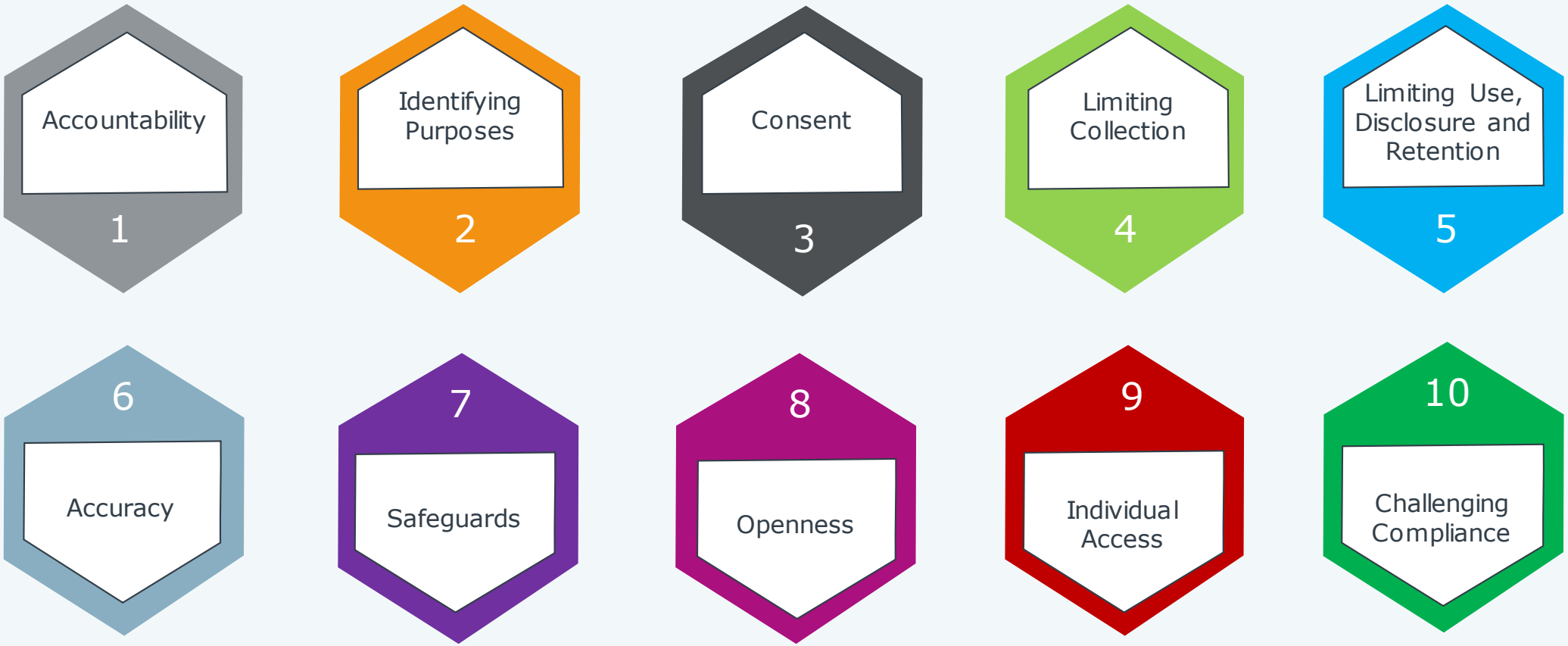
mcmillan

Hot Topic #1 - Privacy in a Pandemic

Speaker:

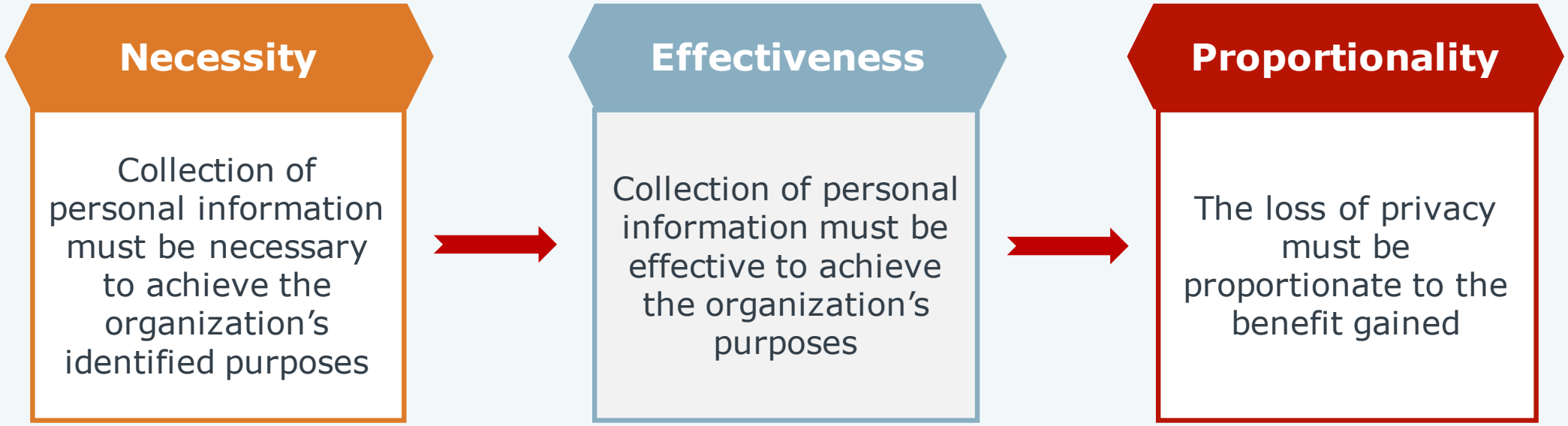
Lyndsay A. Wasser

Guiding Principles



Reasonableness

For example, PIPEDA Section 5(3) – "An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances."



Regulatory Guidance

- **Joint Guidance by Federal, Provincial and Territorial Privacy Commissioners**
  - Privacy and COVID-19 Vaccine Passports (May 19, 2021) - https://www.priv.gc.ca/en/opc-news/speeches/2021/s-d_20210519/
  - Reinforcing Privacy and Access to Information Rights During and After a Pandemic (June 2, 2021) - https://www.oipc.ab.ca/resources/joint-resolution-reinforcing-privacy-and-access-to-information-rights-during-and-after-a-pandemic.aspx
- **Federal**
  - Privacy and the COVID-19 outbreak (March 2020) - https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/health-emergencies/gd_covid_202003/
- **Alberta**
  - Privacy in a Pandemic (March 2020) - https://www.oipc.ab.ca/resources/privacy-in-a-pandemic.aspx
  - Pandemic FAQ: Customer Lists (June 2020) - https://www.oipc.ab.ca/resources/pandemic-faq-customer-lists.aspx
  - Pandemic FAQ: Proof of Vaccination (May 2021) - https://www.oipc.ab.ca/resources/pandemic-faq-proof-of-vaccination.aspx

Regulatory Guidance (cont'd)

- **Saskatchewan**
  - Updated Statement from the Office of the Information and Privacy Commissioner of Saskatchewan on COVID-19 (April 20, 2020) - https://oipc.sk.ca/statement-from-the-office-of-the-information-and-privacy-commissioner-of-saskatchewan-on-covid-19/
  - Advisory from the Office of the Information and Privacy Commissioner of Saskatchewan on questions, screening or testing by employers regarding COVID-19 (May 27, 2020)- https://oipc.sk.ca/advisory-from-the-office-of-the-information-and-privacy-commissioner-of-saskatchewan-on-questions-screening-or-testing-by-employers-regarding-covid-19/
  - Advisory from the Office of the Information and Privacy Commissioner of Saskatchewan on questions regarding vaccines for organizations, employers and health trustees (Updated March 3, 2021) - https://oipc.sk.ca/assets/UPDATED_ipc-advisory-on-questions-regarding-vaccines-for-organizations-employers-and-health-trustees.pdf
- **Manitoba**
  - Frequently Asked Questions: COVID-19 Issues (July 29, 2021) – https://www.ombudsman.mb.ca/uploads/document/files/faq-covid-19-issues-en.pdf

Regulatory Guidance (cont'd)

- **Newfoundland**
  - Public Bodies Collecting Proof of Vaccination from Employees (October 1, 2021) - https://www.oipc.nl.ca/pdfs/COVIDGuidanceOnProofOfVaccination.pdf
  - Covid-19 FAQ - https://www.oipc.nl.ca/pdfs/COVIDFAQ.pdf
- **Quebec**
  - Passeport vaccinal: entreprises et organismes publics (last updated September 8, 2021) – https://www.cai.gouv.qc.ca/covid-19-questions-frequentes/passeport-vaccinal-entreprises-organismes-publics/
  - Collecte des informations du passeport vaccinal: activités physiques et sportives (September 15, 2021) - https://www.cai.gouv.qc.ca/collecte-des-informations-du-passeport-vaccinal-activites-physiques-et-sportives/
  - Pandemic, privacy and protection of personal information (May 4, 2020) - https://www.cai.gouv.qc.ca/documents/CAI_Document_reflexion_ANG.pdf
  - COVID-19: Protection des renseignements personnels et sécurité de l'information (March 25, 2020) - https://www.cai.gouv.qc.ca/pandemie-de-covid-19-protection-des-renseignements-personnels-et-securite-de-linformation/

Regulatory Guidance (cont'd)

- **Northwest Territories**
  - Privacy in a Pandemic - https://atipp-nt.ca/wp-content/uploads/2020/03/Privacy-in-a-Pandemic.pdf
- **British Columbia**
  - Privacy and the BC vaccine card: FAQs (September 13, 2021) - https://www.oipc.bc.ca/guidance-documents/3577
  - Collecting personal information at food and drink establishments during COVID-19 (July 2020) - https://www.oipc.bc.ca/guidance-documents/2421
- **Yukon**
  - Guidance for HIPMA custodians during COVID-19 pandemic (April 23, 2020) - https://www.yukonombudsman.ca/uploads/media/5ea218f8166c4/Guidance%20for%20custodians%20during%20COVID%20pandemic%20April%2023%202020.pdf?v1

Collection of health information about visitors and other non-employees (e.g., contractors, members of the public)

- Do you have legal authority to collect the information?
  - Legal obligation? Public health order?
  - Consent – May provide sufficient authority.
  - Quebec – Specific, serious and legitimate purpose.
- What purposes are you trying to accomplish?
- Do you need the information to accomplish those purposes?
  - Could you achieve the same purposes with less impact on privacy?
  - Consider factual circumstances, including whether effective health and safety protocols could eliminate/reduce the need to collect sensitive health information.

Collection of health information about visitors and other non-employees (cont'd)

- If it is necessary to collect health information, apply the guiding principles:
  - Minimize collection, use and disclosure.
  - Provide a clear notice. [Note: Consider the OPC's meaningful consent guidelines, and specific statutory notices required in some jurisdictions.]
  - Implement strong physical, technological and organizational safeguards to protect health information.
  - Consider whether it is necessary to keep any records (or whether a "show and go" approach is sufficient). If so, destroy/delete information when it is no longer required (i.e., for identified purpose(s) or compliance with legal obligations).
  - Implement appropriate policies and procedures for compliance with obligations related to accountability, access and complaints.

Collection of health information about employees

- Unique considerations for employers:
  - Legal requirements and restrictions vary by jurisdiction.
  - Privacy considerations must be balanced with other legal obligations (e.g., occupational health and safety).
  - Greater risk of exposure / COVID-19 transmission due to time on premises and mobility within workspaces.

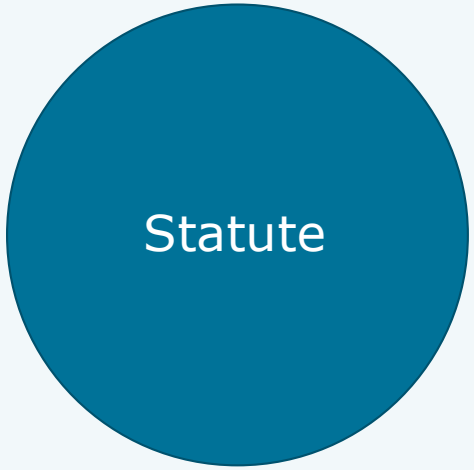
Collection of health information about employees

- Tips for employers:
  - Consider available options (e.g., continuing to work from home).
  - Provide an appropriate notice to employees [Note: Consider any specific statutory requirements.]
  - Store vaccination and other health information separate from general HR file.
  - Designate an individual (or small team) that will be responsible for COVID-19 protocols, and limit access to such individual(s).

Hot Topic #2 – Data Breaches

Speaker:
Mitch Koczerginski

Strategic Considerations – Source of Legal Obligations

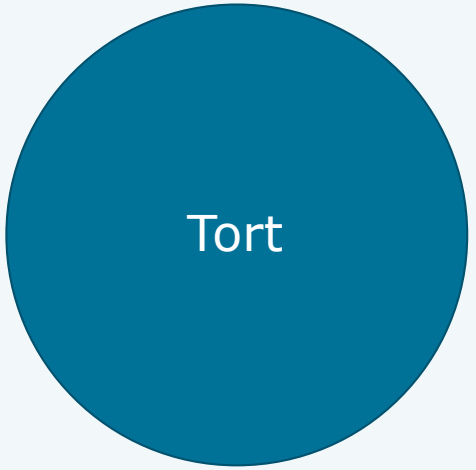


Potential requirements:

- Reporting to Regulator
- Notice to Individuals
- Record keeping
- Timeliness

Potential requirements:

- Defined by agreement



Potential requirements:

- Defined by common law

Strategic Considerations – Legal and Practical Risks

Potential risks:

- Investigative reports
- Communications about incident
- Documents and memoranda

Potential risks:

- Competing regulatory requirements
- Inconsistent dissemination of information

Potential risks:

- Operational disruptions
- Misuse of information
- Non-compliance with legal obligations

Strategic Considerations – Readiness

- Take inventory of information under your control
- Develop a comprehensive incident response plan
- Designate internal and external escalation contacts to manage legal and practical risks
- Be cautious of unintentional waivers of legal privilege

mcmillan

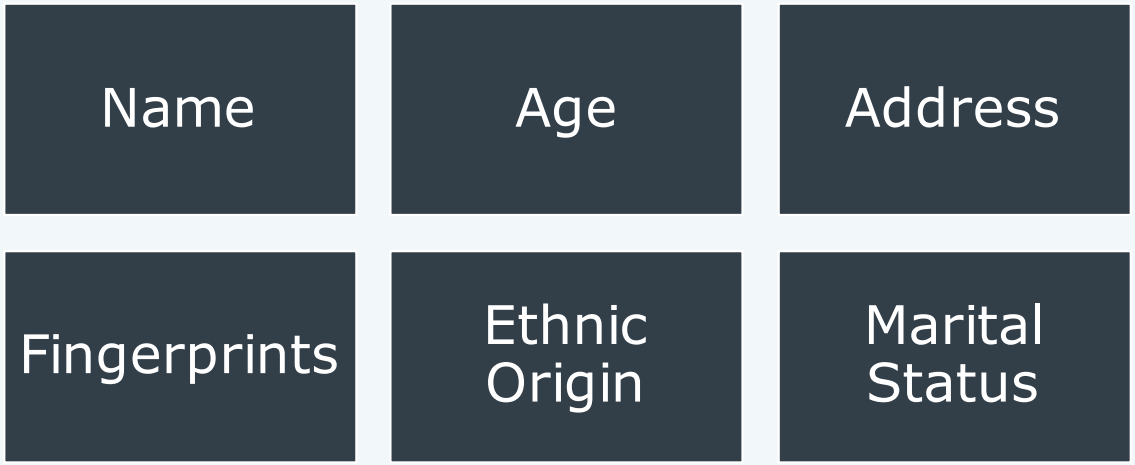
Hot Topic #3 - Using Technology to Aggregate & Anonymize Data

Speaker:

Robert Piasentin

Introduction to Identifiable Data

- Privacy protections are limited to "personal information", or information about an identifiable individual



- Anonymization attempts to remove personally identifiable information from a data set

Risks and Challenges of Anonymization

- Re-identification is a real risk

- Various practices available to reduce the risk of re-identification
  - "White noise"
  - Obfuscation
  - BUT increased anonymization can reduce data utility

- Data from IoT devices
  - Challenging to anonymize
  - More prone to re-identification

The Implications of Aggregate Data

- Data collected by IoT devices
  - May not be directly identifiable
  - But may create an identifiable profile in the aggregate – substantial inferences about private behaviours an individual never intended to share
  - Ability of AI to extract data trends exacerbates this risk

- Sensor fusion risk: where data from two sensing devices reveal more information when the data is combined
  - IoT devices could be used for unintended or unexpected purposes

- De-identification does not necessarily eliminate these risks

Can You Freely Use Anonymized And Aggregated Data?

- Approximately 99.98% of anonymized data may be capable of re-identification
- Risks remain present even with largely incomplete datasets
- Legal uncertainty: how do you decrease liability risk from re-identification?
  - GDPR: incorporated re-identifiable data under privacy protections
  - BC: proposed amendments to FIPPA signal a shift towards more flexibility and a focus on competitive advantage for BC-based companies
  - Federal: CPPA sought to introduce a prohibition against re-identifying data
    - Not clear whether de-identified data would have been captured

Key Takeaways

Be diligent, intentional and deliberate in the steps you take to anonymize data.

Carefully consider how you will subsequently use anonymized data.

Trap of false sense of security - through anonymization, a business has significantly mitigated privacy risk.

Modern technology makes true anonymization very difficult.

Aggregating anonymized data materially heightens the risk of anonymized data becoming re-identifiable to a particular individual.

With multiple sensors collecting data, even greater risk of anonymized and/or aggregated data becoming re-identifiable.

mcmillan

Legislative Update - Recent and Anticipated Changes to Federal and Provincial Privacy Legislation

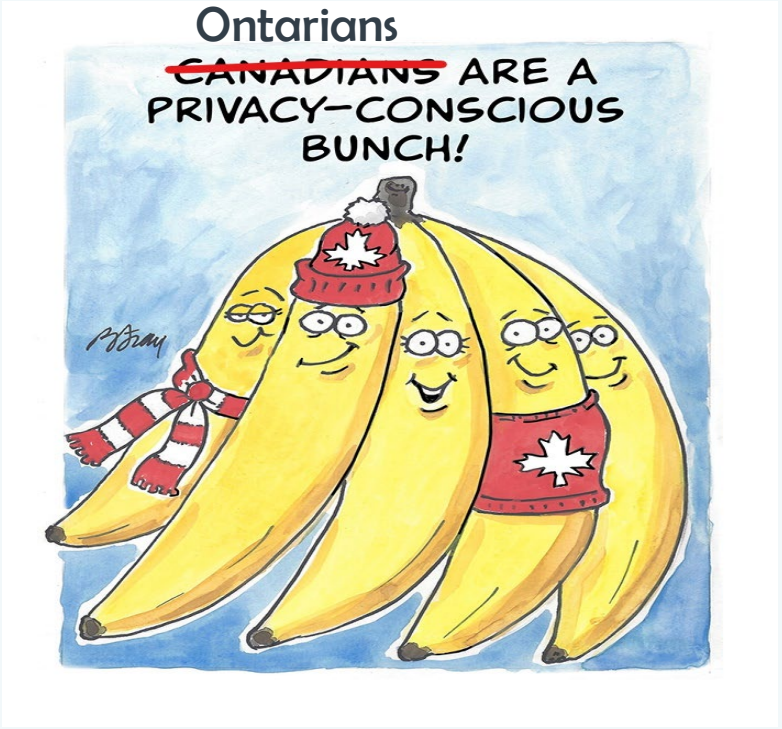
Speakers:

Lyndsay Wasser, Mitch Koczerginski, Gurp Dhaliwal, Julia Loney, and Marie-Eve Jean

Ontario – New Private Sector Privacy Law Coming?

- **White Paper – Modernizing Privacy in Ontario**
  - Issued by Ministry of Government and Consumer Services
  - Possible Ontario-specific private sector privacy law depending on Federal privacy reform
  - Provides samples for legislative language

- **IPC Comments on White Paper**
  - Supports Ontario-specific privacy law regardless of federal reform
  - Provides important insights on proposals for reform



Cartoon reproduced from Office of the Privacy Commissioner of Canada website. Original version available at https://www.priv.gc.ca/en/

Ontario – Key Proposal 1: Expanded Scope of Regulation

- **Proposal**: to expand the scope of the Ontario privacy law to apply to:
  1. Charities, non-profit organizations, trade unions and other non-commercial organizations; and
  2. Provincially-regulated employers

- **IPC Comment**: supports expanded scope, but suggests explicit application to political parties

Ontario – Key Proposal 2: Privacy as a Fundamental Right

- **Proposal**: to recognize **Privacy** as a **fundamental right**
- **IPC Comment**: supports recognition, but suggests explicit reference to **transparency**, **accountability**, and **strong & independent oversight**

Preamble

Privacy is a foundational value in society. Every individual is entitled to a fundamental right to privacy and the protection of their personal information.

Changes in technology have allowed organizations to easily collect vast amounts of personal information about individuals, often undermining the control that an individual has over their personal information.

To establish the trust and confidence of individuals, organizations must be subject to rules, guided by principles of proportionality, fairness and appropriateness with respect to the collection, use or disclosure of personal information.

Ontario – Key Proposal 3: ***Fair*** and Appropriate Purposes

- **Proposal**: to limit the collection, use or disclosure of personal information for purposes that a reasonable person would consider ***fair*** and appropriate

- **IPC Comment**: supports "fairness" requirement and recommends:
  - considering "context" when assessing volume, nature and sensitivity of PI; and
  - considering "effectiveness" when assessing whether personal information is necessary to achieve the legitimate needs of an organization; and
  - considering who "benefits" when considering whether the benefit is proportionate to the individual's loss of privacy

Appropriate purposes

(1) An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider fair and appropriate in the circumstances.

Factors to consider

(2) The following factors must be considered in determining whether the purposes referred to in subsection (1) are fair and appropriate:

1. The volume, nature and sensitivity of the personal information, including whether the organization has taken steps to de-identify the personal information.

2. Whether the collection, use or disclosure is necessary to achieve the legitimate needs of the organization.

3. Whether there are less intrusive means of achieving those purposes at a comparable cost and with comparable benefits.

4. Whether the individual's loss of privacy is proportionate to the benefits in light of any measures, technical or otherwise, implemented by the organization to mitigate the impacts of the loss of privacy on the individual.

Ontario – Key Proposal 4: Expanding Lawful Uses of PI Without Consent

- **Proposal**: to reduce "consent fatigue" by permitting organizations to rely on implied consent in certain prescribed circumstances

- **IPC Comment**: supports legislating codifying the instances where implied consent is permitted, but that it should expressly require organizations to comply with information disclosure requirements regarding withdrawal of consent.

Cartoon reproduced from Office of the Privacy Commissioner of Canada website. Original version available at https://www.priv.gc.ca/en/

Ontario – Key Proposal 5: Oversight & Enforcement

- **Proposal**: stronger enforcement regime as compared to PIPEDA, including the ability for the IPC to initiate and conduct investigations and audits, issue binding orders and levy monetary fines of up to CAD $50,000 for individuals and the greater of CAD $10 million or 3% of gross global revenue in prior financial year for organizations

- **IPC Comment**: broadly supportive of enforcement regime, but recommends:
  1. authorizing it to issue orders and fines to both service providers (in addition to organizations)
  2. Increasing the maximum penalty for individuals to $100,000
  3. that it's orders be subject to judicial review, rather than appeal

Ontario – Other Key Proposals Include…

- **Right to be forgotten** (i.e. right to deletion, including possibly a requirement to de-index search results containing PI posted by third parties)
- **Automated decision-making** (i.e. disclosure obligations in connection with the use of automated decision making systems)
- **Protection of Children** (i.e. various privacy protections relating to PI about minors under the age of 16)
- **Right to Data Portability** (i.e. right to ask organizations to transfer PI to another organization)
- **Among others…**

Legislative Updates - British Columbia

- ***Personal Information Protection Act ("PIPA")***
  - A Special Committee has been appointed to review *PIPA.* The Committee will issue a report on its proposed changes to the Legislative Assembly by December 8, 2021.

  - The Privacy Commissioners of B.C. and Canada have provided the Special Committee with recommendations for proposed changes to *PIPA*, including:
    - Mandatory breach reporting
    - Modernizing consent requirements
    - Clarity on automated decision-making processes
    - Increased enforcement and investigation ability for the Commissioner
    - Harmonization on a national and international level
    - Enhancing the ability for regulatory cooperation

Legislative Updates - British Columbia

- ***Freedom of Information and Protection of Privacy Act ("FIPPA")***
  - Bill 22 was introduced on October 18th, 2021 to amend *FIPPA*. The proposed changes include:
    - Allowing public bodies to store and disclose personal information outside of Canada
    - New offences that apply to service providers
    - Requiring public bodies to develop privacy management programs
    - New privacy breach notifications
    - Clarification of Privacy Impact Assessment requirements
    - Exemptions for disclosure of personal information that may be harmful to interests of Indigenous people
  - For further information see our publication on the proposed changes to *FIPPA* https://mcmillan.ca/insights/proposed-changes-to-fippa-two-steps-forward-one-step-back/

Alberta and Saskatchewan

- Recent Updates
  - Engagement by Ministry of Service Alberta on PIPA and FOIP
  - Saskatchewan Privacy Commissioner's "Change is in the Air" annual report

- Anticipated Changes
  - Updating and modernizing legislation
  - Reflecting technology and digitization of information

Bill 64 – *An Act to modernize legislative provisions as regards to the protection of personal information*

- Adopted by Québec's National Assembly on September 21, 2021
- Received assent on September 22, 2021
  - Beginning of implementation period
- *Act respecting the protection of personal information in the private sector*, CQLR P-39.1
  - Adopted in 1994
  - Last significant amendments in 2006
- New obligations for organizations doing business in Québec
  - Addresses shortcomings of the previous *Act*
  - Adds severe enforcement mechanism
- Requirements will come into effect in three phases throughout the next three years

Bill 64 – New Obligations as of September 22, 2022

Appointment of a Privacy Officer (section 3.1)

- Person in the organization with the highest authority is, by default, the "person in charge of the protection of personal information"
- Role can be delegated **in writing** to any other person
- Responsibilities:
  - Ensure the organization's compliance with the *Act*
  - Handle access and rectification requests
  - Address any questions or complaints concerning the processing of personal information
- Post title and contact information on the organization's website

Bill 64 – New Obligations as of September 22, 2022

Breach Reporting (sections 3.5 to 3.8)

- Confidentiality incident: access to, use, or communication of personal information not authorized by law, as well as the loss or any infringement of the protection of such information
- As soon as you have reason to believe that a confidentiality incident involving PI in your custody has occurred, **immediately** take reasonable measures to reduce any risk of harm and to prevent similar incidents

Bill 64 – New Obligations as of September 22, 2022

Breach Reporting (sections 3.5 to 3.8) [cont'd]

- If there is a risk of serious injury, promptly notify the CAI and the person concerned
  - You can also notify any third party that is likely to reduce the risk of harm
- Assessment of "risk of serious injury":
  - Similar factors to the "real risk of significant harm" test under PIPEDA
    - Sensitivity of information concerned
    - Anticipated consequences of use
    - Likelihood that information will be used for injurious purposes
- Implement and maintain a register of confidentiality incidents
  - Must be provided to the CAI upon request

Bill 64 – New Obligations as of September 22, 2022

Commercial Transactions [section 18.4]

- You can communicate PI that is necessary to conclude a commercial transaction to another party involved in the transaction without the concerned person's consent subject to a **written Agreement**, which stipulates that the:
  - information will only be used to conclude the transaction;
  - you will not disclose the PI without the consent of the person concerned, unless authorized by the *Act;*
  - you will take the measures required to protect the confidentiality of the PI; and,
  - you will destroy the PI if the transaction is not concluded or if using the PI is no longer necessary for concluding the transaction.

Bill 64 – New Obligations as of September 22, 2022

Study, Research and/or Statistics [sections 21, 21.0.1 and 21.0.2]

- You can communicate PI without consent to any person or body who intends to use it for study/research and/or statistical purposes
- Subject to an assessment of the privacy-related factors, which must concluded that:
  - the objective of the study/research/statistics can be achieved only if the PI is communicated in a form allowing the persons concerned to be identified;
  - it is unreasonable to require the person/body to obtain consent;
  - the objective of the study/research/statistics outweighs, in light of the public interest, the impact of communicating and using the PI on the privacy of the persons concerned;
  - the PI is used in a manner that ensures confidentiality; and,
  - only the necessary PI is communicated.
- Also subject to a prior written agreement that must be shared to the CAI one (1) month prior to communicating the PI
- Request for use of PI for study/research/statistics

Bill 64 – New Obligations as of September 22, 2023

Policies, Procedures and Practices [section 3.2]

- Establish and implement policies and practices regarding the protection of PI that:
  - provide a framework for the protection and destruction of the PI;
  - define the roles and responsibilities of the members of the organization's personnel throughout the life cycle of the PI; and,
  - provide a process for dealing with complaints.
- Framework must be approved by the Privacy Officer
- Publish details about policies and practices on your website in clear and simple language

Bill 64 – New Obligations as of September 22, 2023

Privacy Impact Assessments ("PIA") [sections 3.3 and 3.4]

- Conduct a PIA if you acquire, develop and/or redesign any information system or electronic service delivery project that involves the collection, use, communication, protection or destruction of PI
- PIA must be proportionate to the:
  - sensitivity of the PI;
  - purpose for which it is to be used; and,
  - amount, distribution and format of the PI.
- Consult the Privacy Officer in connection with such a project

Bill 64 – New Obligations as of September 22, 2023

Transparency [sections 8 and 8.2]

- When collecting PI, advise the individual of the:
  - purposes of the collection;
  - means of the collection
  - rights of access and rectification; and,
  - right to withdraw consent to the communication or use of the PI collected.
  - If applicable, also inform them of the:
    - name of the third party for whom the PI is being collected;
    - categories of third parties to which it is necessary to communicate the PI for the purposes of the collection (for example, service provides); and,
    - possibility that PI could be communicated outside of Québec.

Bill 64 – New Obligations as of September 22, 2023

Transparency and Technology [sections 8, 8.1 and 8.2]

- Publish a privacy policy on your website if you collect PI through technological means
  - Draft it in clear and simple language; and,
  - notify users of any amendment to the policy.
- If you collect PI using a technology that includes functions allowing an individual to be identified, located or profiled, inform the individual:
  - of such collection; and,
  - about the means available to **activate** such functions.

Bill 64 – New Obligations as of September 22, 2023

Consent [sections 8.3, 12 and 14]

- If an individual provides PI after receiving an adequate privacy notice, they are deemed to have consented to the use and communication of the PI provided for the purposes indicated in the notice
- Obtain consent that is clear, free and informed for the processing of PI:
  - provide specific purposes for processing of PI;
  - request consent for each purpose in clear and simple language; and,
  - request consent separately from any other information provided to the individual.

Bill 64 – New Obligations as of September 22, 2023

Consent [sections 8.3, 12 and 14]

- Obtain express consent to use sensitive PI
- What is sensitive information?
  - Information is sensitive if, due to its nature, including medical, biometric or otherwise intimate information, or the context of its use or communication, it involves a high level of reasonable expectation of privacy
- Minors under the age of 14
  - Consent must be given by the person having parental authority or by the tutor
- New exceptions – can use PI for another purpose without consent for:
  - purposes consistent with those for which it was collected (direct and relevant collection with initial purpose);
  - the benefit of the person concerned;
  - the necessary prevention and detection of fraud or the evaluation and improvement of protection/security measures;
  - the necessary supply or delivery of a product of the provision of a service; and,
  - necessary research, study or production of statistics where the PI is de-identified.

Bill 64 – New Obligations as of September 22, 2023

Privacy by Default [section 9.1]

- If you collect PI by offering to the public a technological product or service that has privacy settings, ensure that those settings provide for the **highest level of confidentiality by default**
- This requirement does not apply to cookies

Bill 64 – New Obligations as of September 22, 2023

Automated Processing [section 12.1]

- If you use PI to render a decision based exclusively on an automated processing of the PI:
  - inform the individual of such use; and,
  - provide the individual with an opportunity to submit observations to a member of the organization that has the authority to review the decision.
- If the individual requests it, also inform them of:
  - the PI used to render the decision;
  - the reasons and the principal factors and parameters that led to the decision; and,
  - their right to have the PI used to render the decision corrected.

Bill 64 – New Obligations as of September 22, 2023

Cross-border Transfers [section 17]

- If you communicate PI outside of Québec, conduct a PIA **prior to communicating information** to assess whether the PI will receive "adequate protection" in compliance with "generally accepted data principles" in the recipient jurisdiction
- The PIA must consider:
  - the sensitivity of the PI;
  - the purposes for which it will be used and the protection measures, including contractual ones, that would apply to it; and,
  - the legal framework applicable in the foreign jurisdiction in which the PI would be communicated, including the data protection principles applicable in that jurisdiction.
- Prepare and conclude a written agreement that considers the results of the PIA and outlines any measures to mitigate risks identified in the PIA (if applicable)

Bill 64 – New Obligations as of September 22, 2023

Outsourcing [section 18.3]

- If your organization transfers PI to a service provider, enter into a written agreement with the service provider that includes:
  - a description of the measures taken by the service provider to ensure the confidentiality of the PI;
  - an obligation for the service provider to only use the PI for the purposes of rendering the services;
  - an obligation not to keep the PI after the expiry of the agreement;
  - an obligation for the service provider to immediately notify the Privacy Officer of any actual or attempted violation of the confidentiality of the PI; and,
  - the Privacy Officer's right to conduct any verification relating to confidentiality requirements.

Bill 64 – New Obligations as of September 22, 2023

Retention and Destruction [section 23]

- Destroy PI as soon as the purposes for which PI was collected or used are achieved
- Anonymize the PI if you need to use it for a **serious and legitimate purpose**
  - What is anonymization?
  - Must be anonymized in accordance with:
    - Generally accepted best practices; and,
    - criteria and procedures prescribed by regulation.

Bill 64 – New Obligations as of September 22, 2023

De-indexation Right [section 28.1]

- Individuals can request that you cease disseminating PI and de-index any hyperlink attached to their name that provides access to the PI by technological means if the dissemination contravenes the law or a Court order
- Can also request same or re-indexation where:
  - the dissemination of the PI causes the person concerned serious injury in relation to their right to the respect of their reputation or privacy;
  - the injury is clearly greater than the interest of the public in knowing the PI or the interest of any person in expressing themselves freely; and,
  - the cessation of dissemination, re-indexation or de-indexation requested does not exceed what is necessary to prevent the perpetuation of the injury.
- If you grant a request, the Privacy Officer must attest to the cessation of dissemination of the PI or the de-indexation or re-indexation of the hyperlink

Bill 64 – New Obligations as of September 22, 2024

Data Portability Right [section 27]

- Individual can request that PI collected from them be communicated to them in a structured, commonly used technological format
  - Can also request that it be communicated to another organization
- These requests exclude PI that you have created or inferred from the individual's PI
- You can refuse the request if it raises serious practical difficulties
- You are not required to destroy the PI after processing the request

Bill 64 – Enforcement

Compliance mechanisms

- Reformed complaint and investigative procedures
- Administrative monetary penalties enforced by the CAI
  - Up to $10 million or 2% of an organization's worldwide turnover
- Penal offences with significant fines
  - Up to $25 million or 4% of an organization's worldwide turnover
- Private right of action allowing individuals to sue an organization for damages

Thank You

Q&A

Lyndsay Wasser

Privacy & Data Protection

Toronto

416.865.7083

lyndsay.wasser@mcmillan.ca

Kristen Pennington

Privacy & Data Protection

Toronto

416.865.7943

kristen.pennington@mcmillan.ca

Gurp Dhaliwal

Business Law

Vancouver

236.826.3060

gurp.dhaliwal@mcmillan.ca

mcmillan

Julia Loney

Environment

Calgary

403.531.4717

julia.loney@mcmillan.ca

Marie-Eve Jean

Litigation & Dispute Resolution

Ottawa

613.691.6108

marie-eve.jean@mcmillan.can.ca

Robbie Grant

Privacy & Data Protection

Toronto

416.865.7154

robbie.grant@mcmillan.ca

mcmillan

Mitch Koczerginski

Privacy & Data Protection

Toronto

416.865.7262

mitch.koczerginski@mcmillan.ca

Robert Piasentin

Technology

Vancouver

604.893.7636

robert.piasentin@mcmillan.ca

mcmillan

Get in Touch

EMAIL

info@mcmillan.ca

LINKEDIN

@mcmillanllp

INSTAGRAM

@mcmillanllp

TWITTER

@mcmillanllp

If you have any questions about McMillan, or how we may help you with your legal needs, please get in touch with us.