

REFORMS OF BC'S FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT (FIPPA): WHAT YOU NEED TO KNOW

Webinar
January 20, 2023

CLARK WILSON

Speakers:
Scott Lamb, Partner
Jeff Holowaychuk, Partner
Lauren Zeleschuk, Associate

AGENDA

PART I:

- Mandatory Breach Notification
- Privacy Management Programs

PART II:

- Data Residency Rules
- Privacy Impact Assessments (PIA's)
- Indigenous Cultural Protection

PART III:

- FOI Requests
- Penalties and Fines

CLARK WILSON 2

FIPPA Legislation

- BC has lagged international developments, the Federal government and other provincial governments in imposing reforms to privacy law on private and public sector organizations
- However, BC has responded last year (November 25, 2021) in passing significant reforms to BC's public sector privacy legislation, *Freedom of Information and Protection of Privacy Act* ("FIPPA")
- FIPPA governs how government and public bodies:
 - collect, use, store and disclose personal information; and
 - manage and respond to FOI requests

CLARK WILSON 3

PART I:
Mandatory Breach Notification
Privacy Management Programs

Scott Lamb, Partner
 604 643 3103
 slamb@cwilson.com

CLARK WILSON

Mandatory Breach Notification


- Since November, 2021 the federal private sector legislation has required organizations to notify the Federal Privacy Commissioner's office and affected individuals of data breaches of personal information held by those organization. Prior to that, since May 1, 2010, Alberta's privacy legislation has made breach notification mandatory for its private sector organizations.
- In BC, both FIPPA (with respect to government and public bodies) and the *Personal Information Protection Act* (PIPA) (with respect to private sector organizations) have until the recent FIPPA reforms in 2022 failed to make data breach notification mandatory.
- Section 36.3 of FIPPA for mandatory breach notification will come into force February 1, 2023.

CLARK WILSON

Mandatory Breach Notification

What is a "privacy breach"?

- Theft or loss, or the collection, use or disclosure of personal information in the custody or under the control of a public body that is not authorized.
- A "head of a public body" must notify an affected individual and the BC Privacy Commissioner's when a privacy breach occurs.



CLARK WILSON

Mandatory Breach Notification

When must a “head of public body” make notification?

- Notification must be made “without unreasonable delay”
- Notification to an affected individual and the Privacy Commissioner must be made where it “could reasonably be expected to result in significant harm to the individual, including identity theft or significant:
 - bodily harm,
 - humiliation,
 - damage to reputation or relationships,
 - loss of employment, business or professional opportunities,
 - financial loss,
 - negative impact on credit record, or
 - damages to, or loss of, property”

CLARK WILSON

7

Mandatory Breach Notification

“Significant Harm”

- Oddly, the language in FIPPA of triggering notification upon an expectation of “significant harm” differs from the Federal PIPEDA legislation which triggers notification where there is a “real risk of significant harm”
- Query whether there is any practical difference?



CLARK WILSON

8

Mandatory Breach Notification

“Significant Harm”

- Also, the Federal PIPEDA legislation sets out relevant factors in assessing whether there is a “real risk of significant harm”:
 - The sensitivity of the personal information involved in the breach.
 - The probability that the personal information has been – is being – or will be misused.
- This is a helpful definition of what is a “real risk of significant harm” and it is hoped that for consistency and clarity, it is adopted to guide the meaning of “significant harm” under FIPPA.

CLARK WILSON

9

Mandatory Breach Notification

- Oddly, an exception from mandatory breach notification for situations where disclosure of the breach could compromise a criminal investigation was not included in the FIPPA provisions as it has been in other jurisdictions in Canada.
- Further guidance on mandatory breach notification from the BC Privacy Commissioner and BC government.

On-line: **Guidance in Mandatory Breach notification Template for Information Incident Check-list Privacy Management Program Guidance for BC Public Bodies (December 2022)**

CLARK WILSON 10

Mandatory Breach Notification

Evaluation Process should include:

- Review of data that has been breached:
 - More sensitive the data the higher the risk (e.g. health information, government-issued identification (social insurance number, drivers licence, health care number and financial account numbers)
 - A combination of personal information is typically more sensitive than a single piece of information

CLARK WILSON 11

Mandatory Breach Notification

Evaluation Process should include:


- Cause and extent of breach:
 - What caused breach?
 - Is there a risk of ongoing or further exposure?
 - What is extent of unauthorized collection, use or disclosure? (i.e. likely number of recipients, risk of exposure in mass media or on-line)
 - Was information lost or stolen?
 - Has the information been recovered?
 - Is this a systemic problem or isolated incident?

CLARK WILSON 12

Mandatory Breach Notification

Evaluation Process should include:

- How many and who are affected by the breach?
 - Numbers matter but do not assume a small number affected is determinative – extent of harm can be qualitative



Data Breach
The Dangers of a Data Breach

CLARK WILSON 13

Mandatory Breach Notification

Evaluation Process should include:

- Foreseeable Harm
 - Who is in receipt of the information” (i.e. Is it a stranger who accidentally receives personal information and voluntarily reports it?)
 - What is the relationship between unauthorized recipients and person whose personal information has been disclosed?
 - What harm to individual could result from breach?
 - What harm to the public body could result from breach?
 - What harm to the public could occur due to breach?

CLARK WILSON 14

Mandatory Breach Notification

Notification

- Key Considerations
 - Legislation requires notification
 - Contractual obligations require notification
 - Contact law enforcement and obtain advice as to whether notification should be delayed in order not to impede a criminal investigation
 - Direct notification preferred (i.e. by phone, letter or in person)
 - Indirect notification where necessary to avoid further harm unreasonable costs or contract information is lacking (i.e. by websites, posted notices or media reports)
- FIPPA Regs – Order in Council (November 28, 2022)

CLARK WILSON 15

Mandatory Breach Notification

- What should be included in notification to individuals affected?
 - Name of public body
 - Date of breach – what occurred
 - Description of breach
 - Description of information inappropriately accessed, collected, used or disclosed and period during which breach occurred
 - Risk to the individual caused by the breach
 - Steps taken to control or reduce harm
 - Future steps planned to prevent further privacy breaches
 - Steps individual can take to mitigate risk of harm

CLARK WILSON 16

Mandatory Breach Notification

- Contact information of person in public body who can answer questions or provide information
- Privacy Commissioner contact information and right to complain to Privacy Commissioner
- Confirmation that Privacy Commissioner has been or will be notified.

CLARK WILSON 17

Mandatory Breach Notification

- What should be included in notification to Privacy Commissioner?
 - Name of public body
 - Date of breach
 - Description of information inappropriately accessed, collected, used or disclosed and the period during which the breach occurred
 - Contact information of person in public body who can answer questions or provide information
 - Steps taken to control or reduce harm
 - Future steps planned to prevent further privacy breaches

CLARK WILSON 18

Privacy Management Programs

- Section 36.2 of FIPPA states that the "head of a public body must develop a privacy management program for the public body and must do so in accordance with the Minister responsible for FIPPA



- Section 36.2 will come into force February 1, 2023

CLARK WILSON 19

Privacy Management Programs

- The Minister of Citizens' Services has issued the **Direction on Privacy Management Programs**
- Specifically, privacy management programs under Section 36.2 of FIPPA must at least include the following:
 - Designate an individual to be responsible for:
 - being a point of contact for privacy matters
 - supporting the development, implementation and maintenance of privacy policies
 - supporting compliance with FIPPA

CLARK WILSON 20

Privacy Management Programs

- Process for completing and documenting privacy impact assessments and information-sharing agreements
- Documented process for responding to privacy complaints and breaches
- Awareness and education for employees
- Privacy policies, processes and practices available to employees, and where applicable, to the public
- Methods to ensure service providers are aware of their privacy obligations
- Process for regularly monitoring and updating privacy management programs

CLARK WILSON 21

Privacy Management Programs

The BC government has also produced pursuant to Section 36.2 of FIPPA the **Privacy Management Program Guidance for BC Public Bodies** (December 2022).

- Similar requirements to the Direction on Privacy Management Program document but greater detail
- Also, identifies obligations with respect to privacy complaints and breaches

CLARK WILSON 22

Privacy Management Programs

Previous Guidance and Tools Published:

1. Guidance from The BC Privacy Commissioner has been published:
 - “Accountable Privacy Management in BC’s Public Sector”
2. BC government’s internal framework for privacy management programs:
 - “Privacy Management and Accountability Policy” (PMAP)

CLARK WILSON 23

Privacy Management Programs

Accountable Privacy Management in BC’s Public Sector

- Privacy Management Programs should include key “building blocks”:
 - Demonstrating senior management commitment and support
 - Designate and empower a Privacy Officer
 - Compliance reporting
 - Personal information inventory
 - Compliance policies
 - Risk assessment tools
 - Training
 - Breach and incident management protocols
 - Service provider management
 - External communication

CLARK WILSON 24

Privacy Management Programs

Privacy Management and Accountability (PMAP)

- Specifically intended to ensure BC government Ministries comply with FIPPA's requirements
- Similar to requirements found in BC Privacy Commissioner's "Accountable Privacy Management in BC's Public Sector"



CLARK WILSON 25

**PART II:
Data Residency Rules
Privacy Impact Assessments (PIA's)
Indigenous Cultural Protection**

Jeff Holowaychuk, Partner
604 643 3194
jholowaychuk@cwilson.com

CLARK WILSON 26

New Data Residency Rules

From Prohibition to Permission

- Recent FIPPA Amendment removed prohibition on access and storage outside of Canada and replaced it with an entirely new regime:
 - Access from outside of Canada
 - o No longer subject to previous strict data residency regime (e.g. installing, implementing, maintaining, repairing, troubleshooting or upgrading an electronic system)
 - o Public bodies still need to ensure that any access to personal information remains secure and subject to adequate controls

CLARK WILSON 27

Disclosure for Storage Regulation

Disclosure of personal information for Storage outside of Canada

- o Permitted only if the disclosure is in accordance with the new Disclosure for Storage Regulations.

The head of a public body must make an assessment in [a PIA] with respect to each of the public body's programs, projects and systems in which personal information that is sensitive is disclosed to be stored outside of Canada.

- o What about personal information that is not "sensitive"?

CLARK WILSON 28

Disclosure for Storage Regulation (cont.)

Assessment for Storage of Sensitive PI Outside of Canada

- Minister responsible for FIPPA has produced PIA templates for public bodies that include a section to assist with this assessment
- Public bodies must make a risk-based decision based on the assessment whether to proceed with disclosure for storage of personal information outside of Canada.
- Risk-based decision must be documented in the PIA (but non-Ministry public bodies may choose another format)

CLARK WILSON 29

Disclosure for Storage Regulation (cont.)

Steps for Assessment

1. Determine whether the program, project or system:
 - o involves sensitive personal information; and
 - o will result in that personal information being disclosed for storage outside of Canada.
2. Identify Privacy Risks and Risk Responses
3. Document risk-based decision setting out the public body's reasoning for accepting the risks and proceeding with disclosure for storage outside of Canada

CLARK WILSON 30

Privacy Impact Assessments (PIAs)

- **New Ministerial Directions now require both Ministries and Non-Ministry public bodies to conduct a PIA on:**
 - any new initiative when no PIA has previously been conducted; and
 - Before implementing a significant change to an existing initiative (includes a change to the location in which sensitive personal is stored when it is stored outside of Canada)
- **“Initiative” includes:**
 - Enactments
 - Systems
 - Projects
 - Programs and activities

CLARK WILSON

31

Privacy Impact Assessments (cont.)

- If a public body determines that a PIA is required:
 - **Ministries** – must use PIA templates created by the Minister responsible for FIPPA or other form/manner approved by the Minister
 - **Non-Ministry Public Bodies** – can use the template created by the responsible Minister, but may use another form as determined by the head of the public body
- Forms can be found on the BC Government [Privacy & Personal Information Resources](#) webpage

CLARK WILSON

32

Privacy Impact Assessments (cont.)

- PIA Topic Areas
 1. General Information about the Initiative
 2. Collection, Use, Disclosure of Personal Information
 3. Storing Personal Information
 4. Assessment of Disclosures outside of Canada
 5. Security of Personal Information
 6. Accuracy, Correction and Retention
 7. Personal Information Banks
 8. Additional Risks
- See Privacy Impact Assessment Guidance on the [Privacy & Personal Information Resources](#) webpage

CLARK WILSON

33

Indigenous Cultural Protection

- New FIPPA Section 18.1 requires public bodies to refuse to disclose information if the disclosure could reasonably be expected to harm the rights of an indigenous people to maintain, control, protect or develop their:
 - Cultural heritage
 - Traditional knowledge
 - Traditional cultural expressions
 - Manifestations of sciences, technologies or cultures
- Subject to Third Party Notice Procedures in sections 23 and 24 of FIPPA

CLARK WILSON 34

**PART III:
FOI Requests
Penalties and Fines**

Lauren Zeleschuk, Associate
604 643 3915
lzeleschuk@cwilson.com

CLARK WILSON 35

Freedom of Information Requests

Background

- Section 4 states that the purpose of FIPPA is to make public bodies more accountable to the public and to protect personal privacy by
 - a) giving the public a right of access to records,
 - b) giving individuals a right of access to, and a right to request correction of, personal information about themselves,
 - c) specifying limited exceptions to the right of access,
 - d) preventing the unauthorized collection, use or disclosure of personal information by public bodies, and
 - e) providing for an independent review of decisions made under this Act.

CLARK WILSON 36

Freedom of Information Requests

- **Who:** Persons (including corporations)
- **What:** Records in the custody or under the control of a public body, including records containing personal information about the applicant, subject to various exceptions such as the protection of a third party's personal information
- **How:** By making a written request to a public body with enough detail to enable the public body to identify the record(s) sought
- **When:** The Public Body is required to respond to the FOI request within 30 days of receiving it, unless the time limit is extended

CLARK WILSON 37

Freedom of Information Requests

- **FIPPA applies to more than 2,900 public bodies, including**
 - provincial government ministries
 - provincial agencies, boards and commissions, and provincial Crown corporations, as listed in Schedule 2 of FIPPA
 - municipalities, regional districts, and improvement districts
 - universities, colleges, school boards,
 - municipal police forces,
 - hospitals, and
 - self-governing professional bodies (such as the College of Physicians and Surgeons and the Law Society of BC)

CLARK WILSON 38

Freedom of Information Requests

Fees

- Processing an FOI Requests costs an average of \$3,000 and an annual cost of \$31 million



CLARK WILSON 39

Freedom of Information Requests

Fees

- Section 75 allows public bodies to charge a fee for some of the work to respond to requests (locating, preparing, shipping and providing records where processing the request takes more than 3 hours)
- Amended section 75 allows public bodies to charge a \$10 fee per request, unless the request is for an individuals own information
- Applies to each request, so applicants must pay each public body included in the request
- Each public body has discretion and does not have to charge the fee

CLARK WILSON 40

Freedom of Information Requests

New Exceptions to What can be Requested

- Section 3(3)(h) was amended to clarify that FIPPA does not apply to either questions or answers used on an examination or test; prior to the amendment the exception was only carved out for questions.
- New section 3(5) creates an exception for:
 - Records that do not relate to the business of the public body;
 - Metadata generated by an electronic system and describing an individuals interaction with it; and
 - electronic records that have been lawfully deleted by the employee of a public body and can no longer be accessed.

CLARK WILSON 41

Freedom of Information Requests

Power to Disregard of Refuse FOI Request

- Section 43 allows FOI requests to be disregarded where the request is frivolous, vexatious, or the information is already disclosed to the applicant or accessible from another source
- Section 43 now allows requests to be disregarded where responding would unreasonably interfere with the operations of the public body because it is excessively broad or repetitious or systematic.
- New section 18.1 requires requests to be refused if the disclosure could reasonably be expected to harm the rights of indigenous people in relation to cultural heritage, traditional knowledge, traditional cultural expressions, and manifestations of sciences, technologies or cultures.

CLARK WILSON 42

New Part 5.1 - Offences

- 65.1 → Offence Act does not apply
- 65.2 → Offence to wilfully mislead, obstruct or fail to comply with commissioner
- 65.3 → Offence to wilfully evade access provisions
- 65.4 → Offence to wilfully collect, use, disclose, and/or fail to notify head of public body of privacy breach
- 65.5 → Corporate liability for authorizing, permitting or acquiescing to an offence
- 65.6 → Penalties

CLARK WILSON 43


New 65.6 Penalties

- \$50,000 for wilfully misleading, obstructing or failing to comply with commissioner (65.2)
- Wilfully evading access provision or committing a privacy offence:
 - \$50,000 for an individual
 - \$50,000 for a service provider, including individuals
 - \$500,000 for a corporation




CLARK WILSON 44


Questions?



Scott Lamb
Partner
604 643 3103
slamb@cwilson.com



Jeff Holowaychuk
Partner
604 643 3194
jholowaychuk@cwilson.com



Lauren Zeleschuk
Associate
604 643 3915
lzeleschuk@cwilson.com

These materials are necessary of a general nature and do not take into consideration any specific matter, client or fact pattern.

CLARK WILSON
