A Principled Approach:
Lessons on PIPA and the Privacy Principles

Privacy, Compliance & Training Branch
Corporate Information and Records Management Office
Ministry of Citizens’ Services
What we’ll talk about today …

• Who we are
• Oversight – the role of the OIPC
• What is Privacy? Personal Information?
• The 10 Privacy Principles
• Overview of PIPA
• Consent – how it works in practice
• Resources
Who are we?

Government’s central privacy office
The Office of the Information and Privacy Commissioner (OIPC):

- review actions and decisions of organizations under PIPA
- power to initiate audits and investigations
- issue binding orders
- can issue fines
- provide guidance resources (Privacy Right, PIA Template)

www.oipc.bc.ca
So...what is privacy?
THE RIGHT TO PRIVACY.

"It could be done only on principles of private justice, moral fitness, and public convenience, which, when applied to a new subject, make common law without a precedent; much more when received and approved by usage." — Willard, J., in Millar v. Taylor, 4 Barn. 1204, 1212.

That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society. Thus, in very early times, the law gave a remedy only for physical interference with life and property, for trespasses vi et armis. Then the "right to life" served only to protect the subject from battery in its various forms; liberty meant freedom from actual restraint; and the right to property secured to the individual his lands and his cattle. Later, there came a recognition of man's spiritual nature, of his feelings and his intellect. Gradually the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life,—the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term "property" has grown to comprise every form of possession — intangible, as well as tangible.

Thus, with the recognition of the legal value of sensations, the protection against actual bodily injury was extended to prohibit mere attempts to do such injury; that is, the putting another in
physical
spatial
informational
Personal Information means recorded information about an identifiable individual other than business contact information or work product information.
Mosaic Effect
Information is an asset.
Right information.
Right person.
Right purpose.
Right time.
Right way.
Ordering Pizza in the 21st Century

https://www.aclu.org/ordering-pizza
The 10 Privacy Principles

1. Identify Purpose. Must identify in writing: the purpose for which you are collecting personal information, the legal authority and contact information of someone who can answer questions about the collection, unless an exception applies. See link below for more.

2. Limit Collection. Do not collect personal information indiscriminately or without a legal authority. Information must be necessary to fulfill identified purposes, and be reasonable and appropriate. Find more information at the link below.

3. Get Consent. Secure consent as a means to use or disclose personal information for secondary purposes. Consent must be written and explicit. There are some specific circumstances where consent is not required. See the link below.

4. Limit Use, Disclosure. You may use or disclose personal information for the purposes identified when it was collected, or another reason authorized by FOIPPA. For new uses, get consent. More information provide at the link below.

5. Reasonable Security. Must make reasonable security arrangements to protect personal information. Measures should be appropriate and proportional to the sensitivity of the information. Consideration should be given to physical, technical and procedural measures. Find your MISO at the link below.

6. Be Accountable. Be responsible for all personal information under your control, including contractors’ records. Be aware of who your Ministry Privacy Officer is. Find your MPO at the link below.

7. Be Open and Transparent. Routinely release any records that can be regularly provided to the public. Proactively disclose any records that will be of interest to the public. Consult with Information Access Operations on these processes. Find the Open Information Open Data Policy provided at the link below.

8. Ensure Accuracy. You must make a reasonable effort to ensure personal information collected is accurate and complete if it will be used to make a decision affecting the individual it is about. Find out more about this requirement at the link below.

9. Right of Access and Correction. Individuals have a right to access their own personal information, or have that information corrected. Be aware of the FOI process, and direct any requests to Information Access Operations immediately. More information provided at link below.

10. Provide Recourse. If you receive a complaint about how an individual’s personal information has been handled, direct it to the Privacy, Compliance and Training Branch immediately, via the breach reporting line: 7-7000, option 3. Learn more from link provided below.

For more information on the privacy principles and resources, visit: www.gov.bc.ca/privacyprinciples
B.C’s Privacy Legislation Landscape

- **FOIPPA**
  - Freedom of Information and Protection of Privacy Act
  - ✓ Public Bodies

- **PIPA**
  - Personal Information Protection Act
  - ✓ Private Sector
Which Privacy Laws Apply and When?

*for private sector

**Freedom of Information and Protection of Privacy Act (FOIPPA):**

- Applies in the instances when private sector organizations are contracted out by a public body

**Personal Information Protection Act (PIPA):**

- Applies in all other instances
Personal Information Protection Act

(PIPA)
• A public body (or info under FOIPPA)

• Personal, journalistic, artistic, and domestic uses

• The courts

• Information captured by PIPEDA
Does PIPA apply?

1. Roberta researching family history, gathers info about relatives, many of whom live in BC, from various sources.

2. You take a selfie with Duchess Meghan Markle while she’s going for a jog on Dallas Road.

3. Accounting firm handles payroll info for municipality.

4. The Greater Victoria Church of the Fonz collects congregant contact information for the upcoming fundraising campaign aimed at helping millennials learn about retro TV shows.
PIPA: law based on principles

1. Identify Purposes
2. Limit Collection
3. Get Consent
4. Limit Use, Disclosure & Retention
5. Reasonable Security
6. Be Accountable
7. Be Open & Transparent
8. Ensure Accuracy
9. Right of Access/Correction or Annotation
10. Provide Recourse
Identify Purpose

✓ Must be reasonable
✓ Must provide contact
Limit Collection

➢ Only what is necessary, reasonable and appropriate
➢ With notice
➢ Directly from the individual
GET ALL THE INFORMATION YOU CAN, WE'LL THINK OF A USE FOR IT LATER.
Is this collection of Personal Information “reasonable”?

- Would your doggie daycare company need your home phone number?
- Would a retailer taking your credit card’s imprint need your phone number? Your SIN?
- Would a mattress company need your level of income or education on a warranty card?
- Would a sports team need to collect detailed health information from its players?
Get Consent

✓ Collect personal information
✓ Collect from a 3rd party
✓ Use/Disclosure of PI
“Valid” Consent
Forms of consent

1. Explicit (Express)
2. Implicit (Deemed)
3. Opt Out
Which form of consent should be used?

**Consider:**

- Reasonable expectations
- Circumstance of the collection
- Sensitivity of the information
Collection *without consent.*

*limited circumstances*

*collection must still be reasonable and appropriate*
Considering Whether Consent is Needed

- The information is in a phone book available to the public. Can it be collected by an organization?

- Can a protest organizer collect personal information by observing individuals that attended a public awareness event?

- A client receiving counselling passes away and the police want personal information about their sessions. Is the counsellor able to provide the information?
Tips for obtaining consent

➢ Record it
➢ No deception
➢ Don’t make consent as a condition
➢ Do not prohibit withdrawal
You run a local childcare business called Later Tots. You request that parents of new children consent to completing a questionnaire about themselves, their children and provide any other necessary information.

1. What would be reasonable to ask as part of questionnaire?

2. What would be unreasonable to ask?

3. In caring for the children, which instances for handling personal information would allow for implicit or explicit consent and why?

4. In caring for the children, are there times where consent would not be required when handling personal information?
Employee Personal Information

- Not consent-based
- Must collect, use, disclose:
  - For a reasonable purpose
  - For employment relationship only
- Must notify (*limited exceptions may apply*)
Would the following be considered a reasonable collection of employee personal information?

- Asking prospective employees of a retail store whether they are smokers because of cigarette smoke odour concerns
- Video taping or monitoring employees where there is no known employment issue
- Use of credit checks in the employee hiring process
Limit Use, Disclosure, & Retention
Limit USE and DISCLOSURE to...

1. The **same purpose** for which it was obtained.
2. Other limited PIPA authorities

New Purpose?  Get **NEW** consent!
Need to know vs. nice to know

But I might need it later.
Would the following use or disclosure be okay?

- Could an organization notify the police about a client that they have seen in a wanted poster?
- Could an organization use photos of people relaxing at the beach in their promotional material?
- Could an organization use personal information to do a reference check from job applicants on references provided?
- Could an organization use an employee’s SIN as a password for daily timekeeping?
Limit Retention
Making a decision that directly affects an individual?
Reasonable Security
Privacy and Security

Reasonable security is ... proportional to the sensitivity of the personal information
Security Tips

➢ Ensure staff awareness

➢ Ensure sufficient monitoring

➢ Ensure access to a contact for questions

➢ Ensure plan for reporting incidents
Group Activity

In terms of securing personal information, please share what you have done within your own organization.

OR

If you are unable to share about your own organization, provide hypothetical tips that can be used by Later Tots as it relates to the questionnaire they ask parent’s complete.
Incidents happen
An information incident is an unwanted or unexpected event that threatens the privacy or security of confidential information.

Includes privacy breaches.
What is a Privacy breach?
Information Incident

Is personal information involved?

Yes
- Privacy Breach
- Privacy Complaint

No
- Information Incident
<table>
<thead>
<tr>
<th>Administrative Errors</th>
<th>Deliberate Employee Actions</th>
<th>Loss/Theft of Mobile Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail, email, fax</td>
<td>Snooping</td>
<td>Laptops, hard drives, USB keys, mobile phones</td>
</tr>
<tr>
<td>Account errors</td>
<td>Leaks/unauthorized disclosure</td>
<td></td>
</tr>
<tr>
<td>Human error/accidental</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The majority of breaches are due to human error.
Information Incident Management Process

Step 1 - Report
Step 2 - Recover
Step 3 - Remediate
Step 4 - Prevent
Report all actual or suspected incidents immediately.

What is your process ...???

Does your staff know it ...???
Step 2: Recover

**Containment Measures**

- Recovering physical documents
- Shredding documents
- Correcting system errors
- Double deletion of emails
- Restricting system access
When personal or sensitive information has been breached, notification to the affected individuals needs to be assessed.
Notification is determined through a **harms assessment**.
Prevention

Step 4

ONLY YOU
Prevention is key!
Be Accountable

✓ Based on “reasonable person test”
Appoint a Privacy Officer
Be Open & Transparent
❖ Write Policies
❖ Collection Notices (for PI)
❖ Develop Material (e.g. brochures)
Ensure Accuracy

➢ Proactive duty of “Reasonable Effort”
Right of Access / Correction or Annotation
Right of Access

1. **Access** to their personal information.

2. Explain how their personal information is being/has been **used**.

3. Identify who their personal information has been **disclosed** to.
An individual has the right to request correction of their personal information.

➢ If denied => right to annotation
I'M HERE TO CORRECT AN ERROR IN MY FILE.
Provide Recourse
Organizations must develop process for responding to complaints.
The Soggiest Survivor, an outdoor survival reality show, is being filmed off the rugged coasts of Vancouver Island. You’ve been asked to work as a Privacy Officer for the development of this television show. How would you apply the principles found in the privacy wheel to enhance contestant’s privacy?
Resources!

PCT’s webpage providing information on your PIPA obligations
https://www2.gov.bc.ca/gov/content/employment-business/business/managing-a-business/protect-personal-information

PrivacyRight: Information from the OIPC helping small businesses and organizations understand their PIPA obligations
https://www.oipc.bc.ca/privacyright/

A helpful guide from the OIPC relating to PIPA
https://www.oipc.bc.ca/guidance-documents/1438

Privacy Impact Assessment Guidelines for the Private Sector
https://www.oipc.bc.ca/guidance-documents/2382
BC Privacy and Access Helpline

250-356-1851
(Service BC 1-800-663-7867)

privacy.helpline@gov.bc.ca

www.gov.bc.ca/protectprivacy