Ethan Plato, Legal Counsel

Office of the Information and Privacy Commissioner for British Columbia

Balancing Accessibility and Privacy in Records Management

2023 AABC & ARMA Vancouver Island Joint Conference

April 28, 2023

This presentation is not intended as or should be considered legal advice, not does it constitute a finding or an opinion of the Commissioner.

TODAY'S DISCUSSION

1. Intro to the OIPC
2. Legislative overview
3. FOI under FIPPA
4. FIPPA and privacy
5. Recent updates
6. Discussion and questions

ABOUT THE OIPC

- Established in 1993
- Independent Officer of the Legislature
- Enforces the *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Personal Information Protection Act* (PIPA)
- Regulator of **public bodies** and **private sector organizations**' compliance with provincial privacy legislation
- Power to investigate and issue orders and public reports

INDEPENDENT OFFICE OF THE LEGISLATURE

- One of nine statutory officers in BC
- Officers are independent, accountable to legislators (MLAs)
- Aim is more open, transparent and honest government

OIPC OVERSIGHT

Oversight of FIPPA and PIPA

- **Investigative:** Commissioner led investigations
- **Adjudicative:** Binding Orders
- **Consultative:** Advice in relation to FIPPA and PIAs, etc.*

*not legal advice and cannot bind the Commissioner

HIGHLIGHTS FROM 2022/2023

CBC | MENU

Business

Tim Hortons app tracked too much personal information without adequate consent, investigation finds

App's data tracking resulted in loss of users' privacy, says report by authorities

Nojoud Al Mallees · CBC News · Posted: Jun 01, 2022 8:37 AM PDT | Last Upda

CTV NEWS
VANCOUVER ISLAND

VANCOUVER ISLAND | News

Canadian Tire stores broke privacy laws on facial ID technology, B.C. privacy commissioner says

VANCOUVER SUN

News / Local News

Personal health information 'disturbingly' vulnerable: B.C. privacy commissioner

Michael McEvoy says that security gaps in the public health computer system put it at risk of abuse by bad actors, from cyber criminals to jilted lovers looking for information about an ex.

CANADIAN PRESS The Canadian Press

Published Dec 15, 2022 • 2 minute read

Join the conversation

HIGHLIGHTS FROM 2022/2023

PIPA

- Privacy legislation that regulates the **private sector** – replaces PIPEDA in most cases, and it is more broad
- Applies to any collection, use, or disclosure of personal information by an **organization**
- PIPEDA (Federal Law) only applies in BC to FWUBs (airlines, banks, etc.)

PIPA

- Twin concepts: consent and reasonableness
- Consent required in most cases, can be deemed [s.8] and some exceptions apply [s.12]
- Even if collection, use or disclosure is otherwise permitted, it must always be done for “purposes that a reasonable person would consider appropriate in the circumstances”

FIPPA: SOME HISTORY

- Born out of a 1990 scandal involving the use of government jets by ministers for personal use
- Flight logs were provided but incomplete
- FIPPA passed in 1992 as a result

FIPPA

Part 2: Freedom of Information

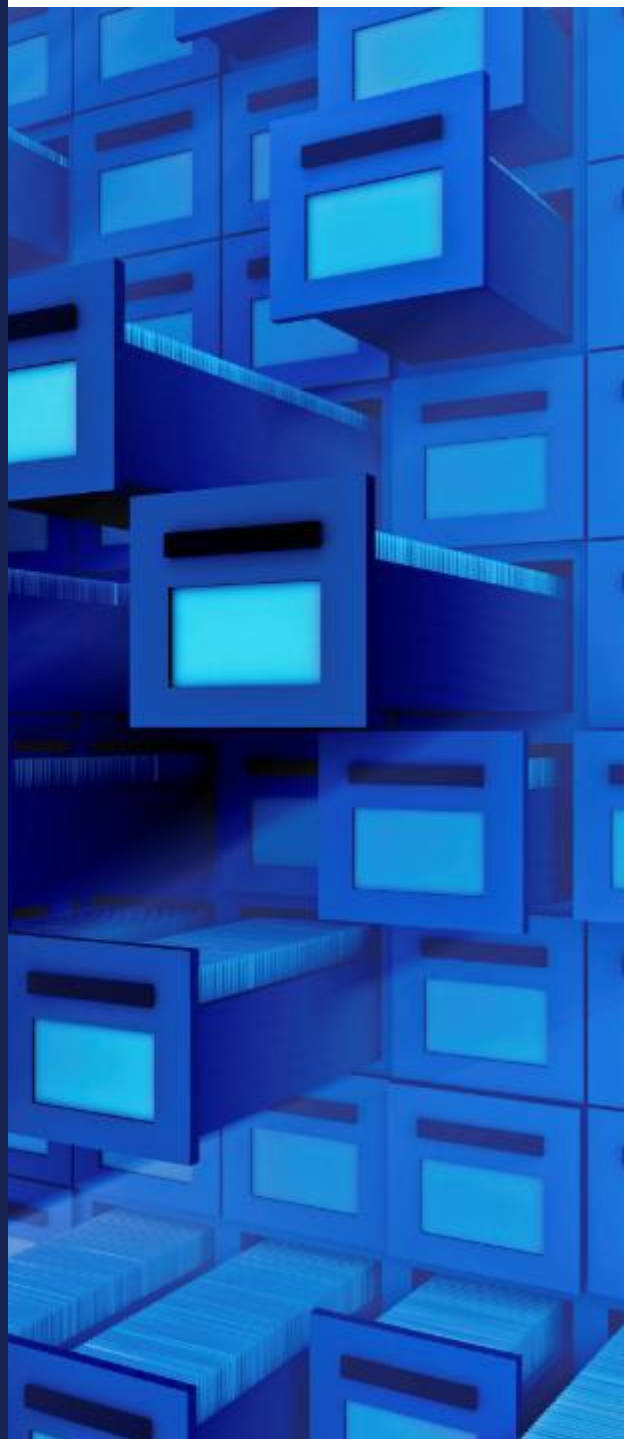
- “to make public bodies more accountable to the public”
- Establishes “Heads” of public bodies responsible for administration of FOI requests
- Oversight by OIPC and ultimately the courts

Part 3: Protection of Privacy

- “to protect personal privacy”
- Collection, use and disclosure of personal information by public bodies

FOI UNDER FIPPA

- Applies to all records in the custody or under the control of a public body
- Default is disclosure unless an exemption applies
- Exemptions (sections 12-22)



RECORDS, CUSTODY AND CONTROL

- Issues with people not understanding what is subject to FIPPA
- Possession is not the end of the road
- Gets complicated if work accounts/devices are used for personal purposes

"Record"

- books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records"

Indicators of control

- Possession
- Rights and responsibilities, incl use disclosure and destruction
- Integrated with other records

LIFECYCLE OF AN ACCESS REQUEST UNDER FIPPA

1. Initial request to public body
2. Review by OIPC (mediation)
3. Inquiry by OIPC (arbitration)

CHALLENGES WITH ACCESS REQUESTS

1. Timeliness
2. Assisting applicants
3. Frivolous or vexatious applicants
4. Institutional buy-in
5. Volume of requests

10 TIPS FOR PUBLIC BODIES

MANAGING REQUESTS FOR RECORDS

The *Freedom of Information and Protection of Privacy Act* (FIPPA) regulates the information and privacy practices of public bodies including BC government, local governments, crown corporations, and local police forces, etc.

FIPPA gives individuals the right to request access to records held by public bodies. Here are our top 10 tips to help public bodies meet the timelines and requirements for responding to requests for records under FIPPA.

1. Designate an FOI Manager
2. Assist applicants
3. Adopt early resolution tactics
4. Pay attention to timelines
5. Keep adequate documentation
6. Maintain policies and training
7. Stay up-to-date on OIPC guidelines
8. Adopt routine release
9. Make information easy to access
10. If in doubt, contact us!

SEARCHING FOR RESPONSIVE RECORDS

- What records are covered by FIPPA?
- How does age of records factor in?
- Small organizations, big responsibility: building systems to standardize handling of requests

SEARCHING FOR RESPONSIVE RECORDS

- Small organizations, big responsibility: develop procedures/policies for FOI requests
- Staff training crucial
- Review and update policies

FIPPA AND PRIVACY

- Protects “personal information”
- Not consent based, public bodies can only collect, use, or disclose personal information when authorized by FIPPA
- Deceased individuals have privacy rights!

PERSONAL INFORMATION

- Information about an identifiable individual, other than contact information (business contact info)
- Examples:
  - name, age, sex, weight, height
  - address, email phone number
  - Health care history
  - Unique number associated with an individual
  - Biometric info
  - Personal views or opinions
- “Mosaic effect” – non-identifying data can become “personal information” when combined with other data or when placed in a particular context

DISCLOSURE – ARCHIVAL OR HISTORICAL PURPOSES

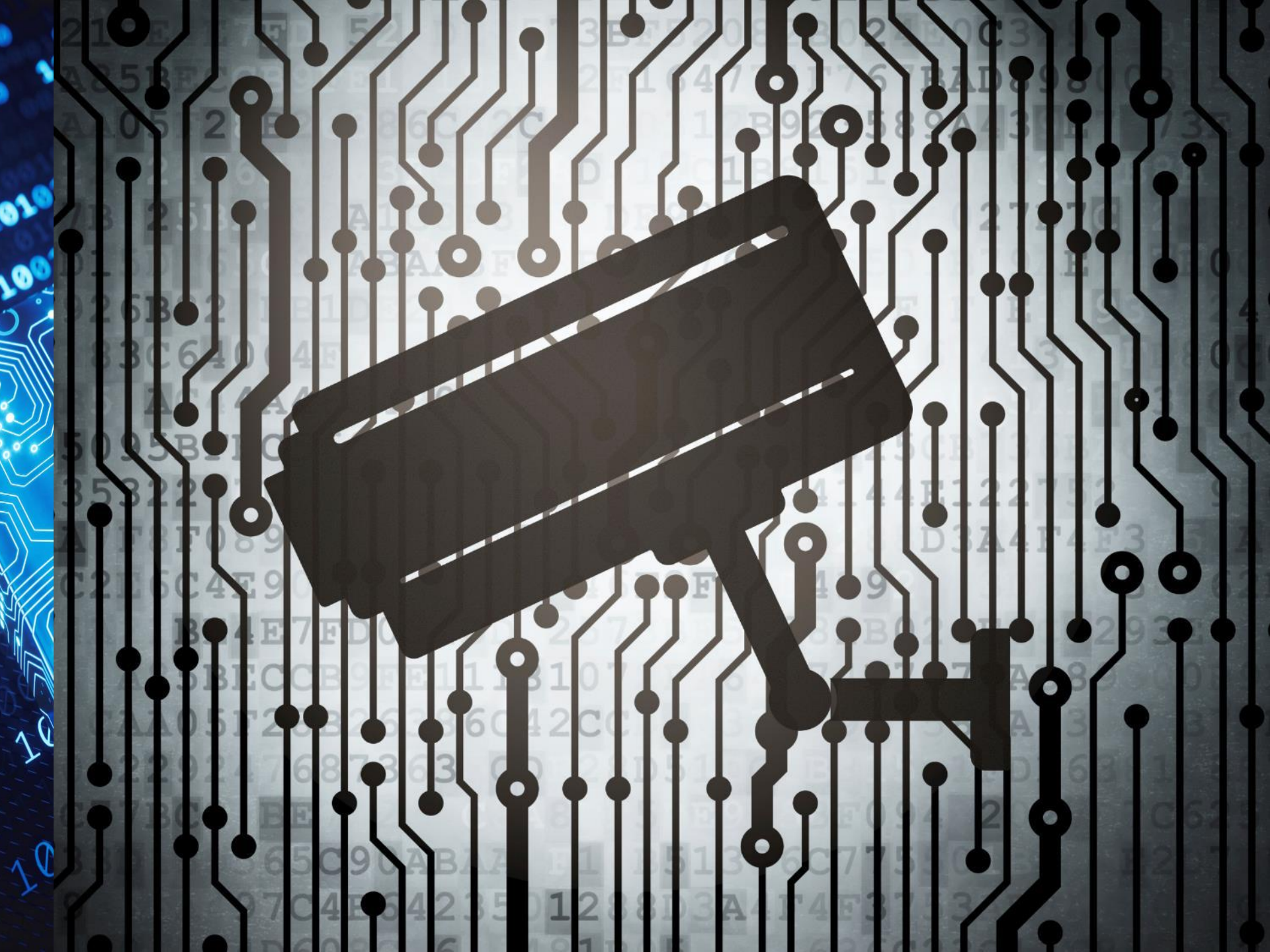
(4) In addition to the authority under any other provision of this section, the digital archives or museum archives of government or archives of a public body may disclose personal information in its custody or under its control for archival or historical purposes if

(a) the disclosure would not be an unreasonable invasion of personal privacy under section 22,

(b) the information is about an individual who has been deceased for 20 or more years, or

(c) the information is in a record that has been in existence for 100 or more years.

- Different than an FOI request – discretionary (by the Head)
- Analysis under s.22 factors – lots of caselaw and guidance



2021 FIPPA AMENDMENTS

- Regulations came into force February 1
- Mandatory privacy breach notification requirement
- Public bodies must have privacy management programs
- Requirements for PIAs
- Stronger penalties

MANDATORY BREACH NOTIFICATION

- Public bodies must report breaches that could result in ‘significant harm’
- Gives individuals time to protect themselves following breach
- Gives public body best chance to minimize damage from a breach

PRIVACY MANAGEMENT PROGRAM ESSENTIALS

1. Appoint privacy officer
2. Process for PIAs and ISAs
3. Process to respond to privacy breaches and complaints
4. Privacy awareness and education for staff
5. Make privacy policies and processes available
6. Service provider management
7. Monitoring/updating

PRIVACY IMPACT ASSESSMENTS (PIAS)

- Help identify personal information and assess risks/privacy impacts and mitigate risks
- Required for new initiatives for which no PIA previously completed
- Required before significant change to existing initiative

DATA RESIDENCY

- February 2021 FIPPA amendments removed residency requirements
- PIA requirements now in law
- Supplementary assessments for sensitive personal information stored outside of Canada

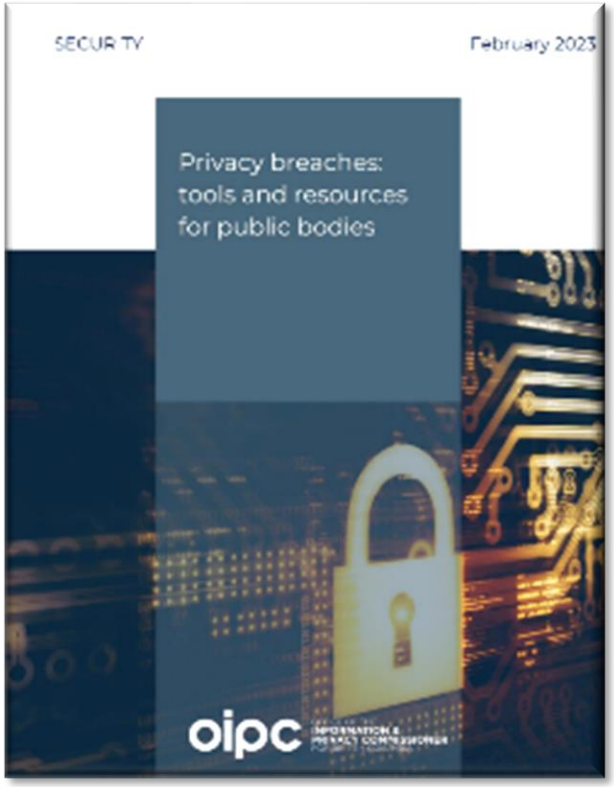
WHAT ARE REASONABLE SECURITY MEASURES UNDER FIPPA?

- “A public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized collection, use, disclosure or disposal.” (FIPPA S. 30)

HOW THE OIPC CAN HELP

- Our office is here to help, email us at info@oipc.bc.ca (or me at eplato@oipc.bc.ca) and your question will be forwarded to the appropriate person
- Policy team has very in-depth experience
- It's free!
- As you will see in our signatures, we do only provide guidance and not binding advice

RESOURCES: OIPC.BC.CA



oipc

March 17, 2020

Tips for public bodies and organizations setting up remote workspaces

VICTORIA—Many public bodies and organizations are now setting up employees to work remotely in the wake of the COVID-19 outbreak. Care must be taken when doing this because it often means personal information leaves the worksite. Below are some tips for how to keep personal information safe when working away from the office.

Mobile devices

- Password protect your device
- Lock your device when not in use
- Ensure portable storage devices (such as USBs and portable hard drives) are encrypted and password protected
- Keep your software up-to-date

Emails

- Use work email accounts rather than personal ones for work-related emails involving personal data.
- Before sending an email, ensure you're sending it to the correct recipient, particularly for emails involving large amounts of personal data or sensitive personal data

Paper copies and files

- Only remove personal information from the office if it is necessary to carry out your job duties
- Take the least amount of personal information you need and leave the rest behind
- Securely store any paper files when not in use. This means locking files away and not leaving any files in your vehicle

General rules of thumb

- Avoid viewing personal information collected and used for work in public. If you must, take precautions to make sure no one else can view the personal information.

Resources for public bodies considering remote work options:
Protecting personal information away from the office
Mobile devices: tips for security and privacy

Resources for organizations considering remote work options:
Protecting personal information away from the office
Is a Bring Your Own Device (BYOD) program the right choice for your organization?
Mobile devices: tips for security and privacy

PRIVACYRIGHT
fundamentals for business

ADDITIONAL RESOURCES

- LGMA FOI Toolkit
- OIPC Guidance
- CanLII (to search previous decisions and court decisions)
- OIPC sectional index
- BC Government FOIPAA Policy and Procedures Manual

HAVE A PRIVACY QUESTION? WE CAN HELP!

(250) 387-5629

info@oipc.bc.ca