

# SENG 460 / ECE 574

## Practice of Information Security and Privacy

Week 5:

Security Awareness, Privacy

Gary Perkins, MBA, CISSP

[garyperkins@uvic.ca](mailto:garyperkins@uvic.ca)



# Security Awareness

- employee onboarding
  - ensure employees know that security is everyone's responsibility
  - roles and responsibilities
  - work to prevent issues and if you see something, report it
- security awareness course for employees
  - example of a course: [https://bcgov.github.io/SecurityAwareness/ISAPublic/story\\_html5.html](https://bcgov.github.io/SecurityAwareness/ISAPublic/story_html5.html)
  - organizations may choose to make mandatory or optional
  - regular content reviews to ensure relevant
  - gamification if possible



# Security Awareness

- establish and maintain a security awareness, education, and training program
  - e.g. passwords, physical security, devices, social media
  - e.g. phishing, social engineering
- methods and techniques
  - e.g. clean desk checks, phishing campaigns
- content reviews
- program effectiveness evaluation



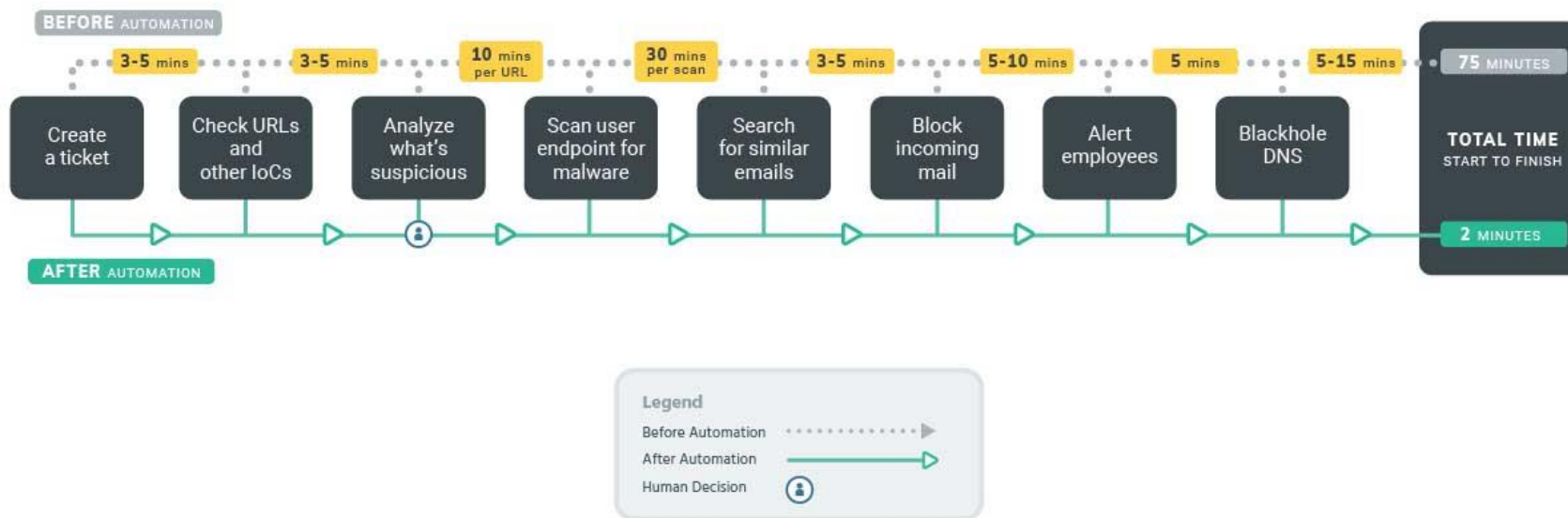
# Phishing Campaigns

- common for organizations to test the effectiveness of their security awareness program by sending phishing emails to their own employees
  - goal is to provide a safe environment for employees to practice making the right decisions – when an incident won't result
  - don't shame them but educate on what they could have looked for
- goal is not to come up with an email that is impossible to tell, want people to be looking for things
  - shouldn't focus on the click rate – better to 'catch someone doing something right' and focus on the report rate
- depends on organization – they may ask employees to report or simply to ignore/delete



# Phishing Campaigns

- other organizations will have a “Report Phishing” button or email address
  - this may route the email to the security team or hopefully submit into the SOAR (Security Orchestration and Automated Response) system to be automatically reviewed, possibly detonated, to determine if it is bad and take next steps
- example of process before and after SOAR:



# Security Awareness

- print/emails
  - Security News Digest (you can sign up too at <https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/security-news-digest>)
- multimedia/videos
  - many out there (e.g. <https://www.youtube.com/watch?v=EAtjO-fQJZw>)
- events
  - also many out there (e.g. B-Sides, DefCon, BlackHat)
  - e.g. [Security Day](#)
- anything to get the message out there...



# Security Awareness

- what messages would you share with employees?
  - e.g. stop and think before you click



TREAT YOUR **PASSWORD** LIKE YOUR **TOOTHBRUSH**

- 1 Choose a good password
- 2 Never share it with anyone
- 3 Change it every 3-6 months

[keepitsafe.auburn.edu](http://keepitsafe.auburn.edu)

Treat your passwords  
like your underwear

Change them regularly

Keep them off your desk



Never share them with anyone

# Privacy

<https://www.youtube.com/watch?v=rTIKWURvbQ4>

<https://www.youtube.com/watch?v=VbjC4uKXbvE>





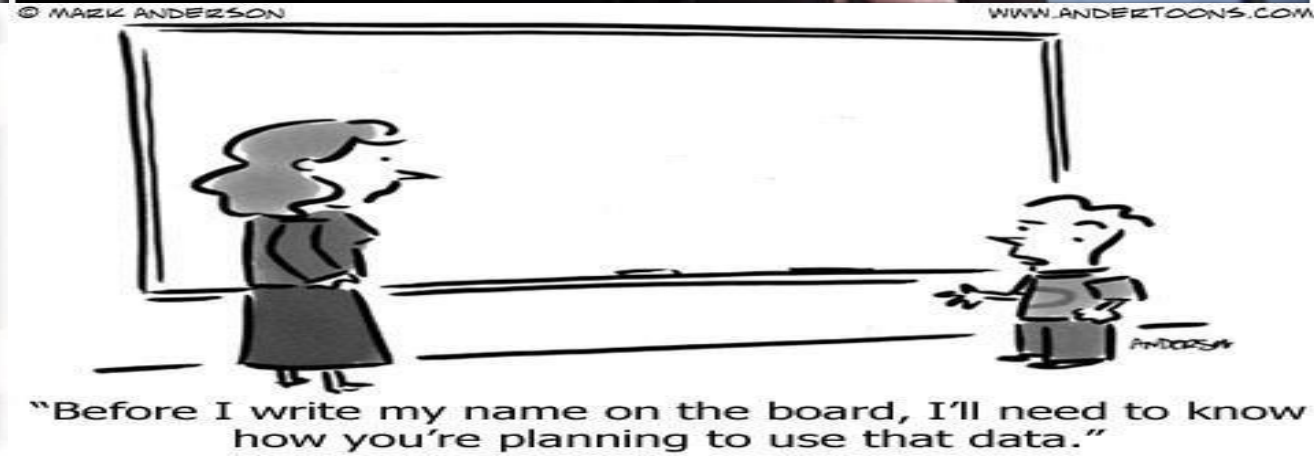
# Privacy

Combubody Sock Origin  
<https://www.youtube.com/watch?v=euQvtep54E8>



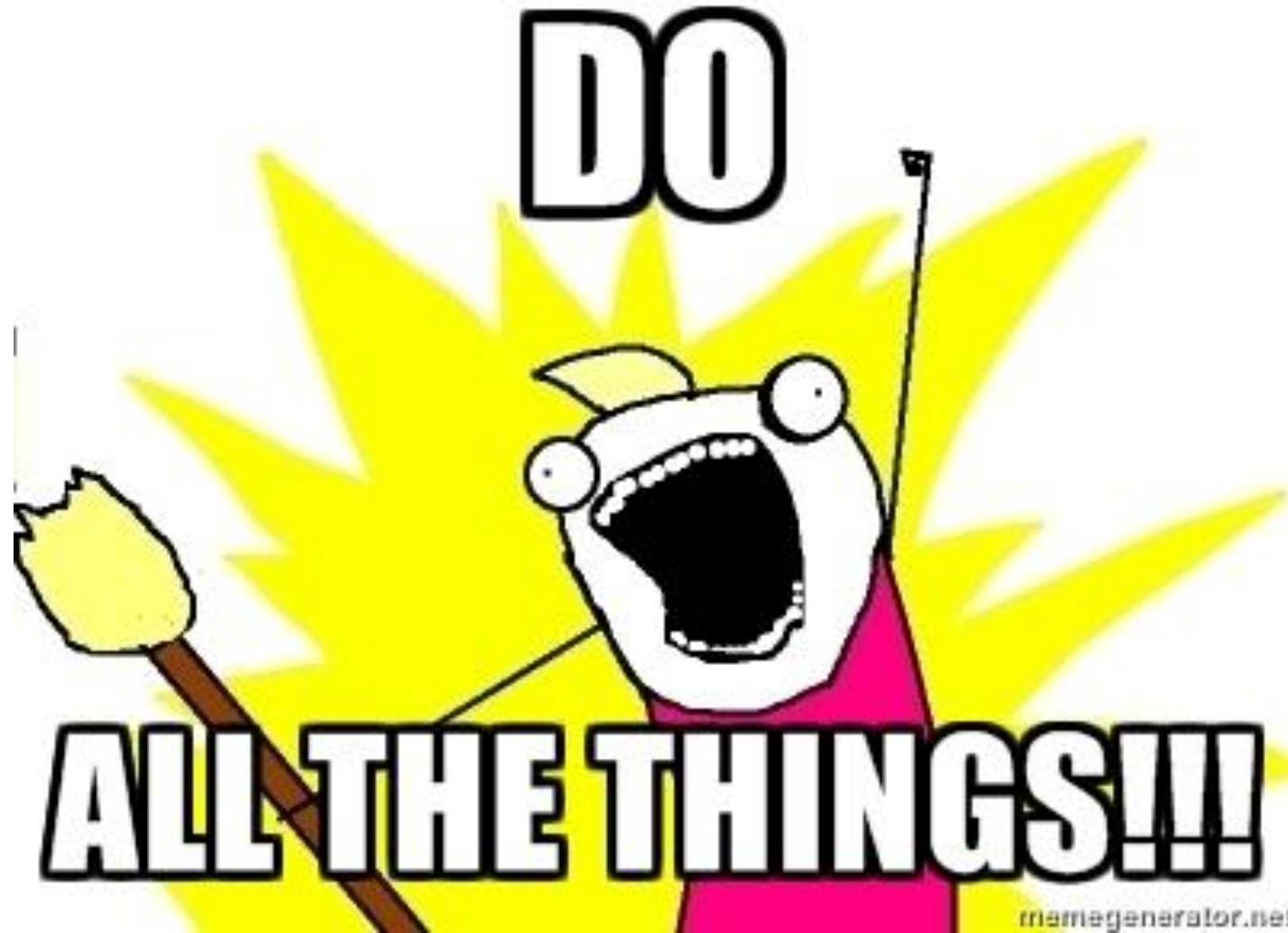
© MARK ANDERSON

WWW.ANDERTOONS.COM



# What the Privacy Team does:

- review initiatives
- respond to breaches
- advise on initiatives
- conduct audits
- develop policy
- provide training



# What they do not do:

- regulate
- oversee
- adjudicate

... they are not the  
privacy commissioner





# Definition of Privacy



**Privacy**

- formerly the right to be left alone

# Privacy

- privacy definition
  - we don't define it in law or policy
  - contextual, hard to pin down
  - **informational self determination**
- you get to choose what happens to your information
- who it goes to, in what capacity, what it is used for
- you are making choices with your information
- some people choose not to make it available

The term **informational self-determination** was first used in the context of a German constitutional ruling relating to [personal information](#) collected during the 1983 [census](#). The German term is **informationelle Selbstbestimmung**. It is formally defined as "the authority of the individual to decide himself, on the basis of the idea of self-determination, when and within what limits information about his private life should be communicated to others. ~ Wikipedia



# Privacy

- don't walk around with a definition
- privacy is:
  - subjective (different for me than someone else)
  - contextual (different across cultures, time, generations)
  - “negative” (often not aware of it until infringed on)
- it's different for different:
  - people, ages, demographics, cultures...



# Privacy

- 3 different kinds of privacy
  1. spatial                      your space and things around you  
eg. locker search, bag search
  2. physical                      privacy of body - eg. pat down
  3. informational              information about you  
eg. who you are, identity, what people say about you
- reasonable expectation of privacy
  - e.g. have very little expectation of privacy at a public event



# Privacy Considerations

- management
- notice
- choice and consent
- collection
- use/retention/disposal
- access
- disclosure to third parties





# Privacy

- data quality & reasonable steps to ensure information is accurate accurate/complete/relevant
- monitoring and enforcement
- limiting data collection
  - best way to ensure privacy, if you don't collect it you can't misuse or lose it
- should tell people what you're collecting and why
- obtain consent to get new information or use for other reasons



# People Are Willing to Give Away Their Personal Data for a Cinnamon Cookie



Share on Facebook



Share on Twitter



Would you give away your personal data for one of these cookies? Turns out a lot of people will.

IMAGE: TALISMAN BROLIN/COURTESY OF RISA PUNO

# Privacy Law



University  
of Victoria



# Expectation of Privacy

- R v. Cole
  - employees have a reasonable expectation of privacy even on an employer provided device
- reasonable use
- appropriate use policies
- network traffic inspection



## SUPREME COURT OF CANADA

**CITATION:** R. v. Cole, 2012 SCC 53

**DATE:** 20121019  
**DOCKET:** 34268

### BETWEEN:

**Her Majesty The Queen**  
Appellant  
and  
**Richard Cole**  
Respondent  
- and -

**Director of Public Prosecutions, Attorney General of Quebec,  
Criminal Lawyers' Association (Ontario), Canadian Civil Liberties Association**

**R v. Cole and unreasonable search and seizure**

Richard Cole was a high-school teacher who also supervised the use of the school's networked laptops by students. He was given a laptop, owned by the school board but for his exclusive use, to allow him to carry out this role.

The school board had a policy which allowed employees to use work computers for personal use, while stating that all data and messages generated on or handled by the school board's equipment would be considered the property of the school board. While conducting maintenance on Mr. Cole's board-issued laptop, a school board technician found photographs of a partially nude underage female student stored on the laptop. The principal was informed of the photographs and the photographs were copied onto a disc and provided to the police. A police officer, relying on the consent of the principal and the fact that the laptop's owner was the school board, then conducted a warrantless search of the laptop.

Justice Hsstein, Cromwell and

The main issue before the Supreme Court was whether Mr. Cole's Charter rights were violated by the warrantless search conducted by the police officer contrary to section 8 of the **Canadian Charter of Rights and Freedoms**. The Court found that while the principal had a statutory duty to maintain a safe school environment and the reasonable power to seize and search the school-issued laptop, the police officer did not. The police officer required judicial authorization to perform the search, either in the form of a warrant or with the consent of Mr. Cole. The consent of the principal was not enough for the purposes of a criminal investigation.

Justice Hsstein, Cromwell and



# Privacy Legislation (Canada)

- Privacy Act
  - applies to federal governments and agencies
- Personal Information Protection and Electronic Documents Act (PIPEDA)
  - applies to information-handling practices of many businesses
  - Manitoba, New Brunswick, Newfoundland/Labrador, NWT, Nova Scotia, Nunavut, Ontario, PEI, Saskatchewan, Yukon

Unless the personal information crosses provincial or national borders, PIPEDA does not apply to organizations that operate entirely within:

- Alberta
- British Columbia
- Quebec.

These three provinces have general private-sector laws that have been deemed substantially similar to

PIPEDA.



# Privacy Legislation (BC)

- Personal Information Protection Act (PIPA) applies to private sector
- Freedom of Information and Protection of Privacy Act (FIPPA) applies to public sector
- Other relevant laws:
  - impact of US Patriot Act
  - CLOUD Act (Clarifying Lawful Overseas Use of Data)
  - NAFTA/USMCA
  - GDPR (General Data Protection Regulation) and right to be forgotten
  - CASL (Canadian Anti-Spam Legislation)



# Privacy Legislation (BC)

## ■ Freedom of Information and Protection of Privacy Act (FIPPA)

### Storage and access must be in Canada

**30.1** A public body must ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada, unless one of the following applies:

(a) if the individual the information is about has identified the information and has consented, in the prescribed

### Disclosure inside or outside Canada

**33.1** (1) A public body may disclose personal information referred to in section 33 inside or outside Canada as follows:

- (a) in accordance with Part 2;
- (a.1) if the information or disclosure is of a type described in section 22 (4) (e), (f), (h), (i) or (j);
- (b) if the individual the information is about has identified the information and consented, in the prescribed manner, to its disclosure inside or outside Canada, as applicable;
- (c) in accordance with an enactment of British Columbia, other than this Act, or Canada that authorizes or requires its disclosure;
- (c.1) if it is made available to the public in British Columbia under an enactment, other than this Act, that authorizes or requires the information to be made public;
- (d) in accordance with a provision of a treaty, arrangement or written agreement that
  - (i) authorizes or requires its disclosure, and
  - (ii) is made under an enactment of British Columbia, other than this Act, or Canada;
- (e) to an individual who is a minister, an officer of the public body or an employee of the public body other than a service provider, if
  - (i) the information is necessary for the performance of the duties of the minister, officer or employee, and
  - (ii) in relation to disclosure outside Canada, the outside disclosure is necessary because the individual is temporarily travelling outside Canada;
- (e.1) to an individual who is a service provider of the public body, or an employee or associate of such a service provider, if
  - (i) the information is necessary for the performance of the duties of the individual in relation to the public body, and
  - (ii) in relation to disclosure outside Canada,
    - (A) the individual normally receives such disclosure only inside Canada for the purpose of performing those duties, and
    - (B) the outside disclosure is necessary because the individual is temporarily travelling outside Canada;
- (f) to an officer or employee of the public body or to a minister, if the information is immediately necessary for the protection of the health or safety of the officer, employee or minister;
- (g) to the Attorney General or legal counsel for the public body, for the purpose of preparing or obtaining legal advice for the government or public body or for use in civil proceedings involving the government or public body;
- (h) to the minister responsible for the [Coroners Act](#) or a person referred to in section 31 (1) of that Act, for the purposes of that Act;



# Mandatory Breach Notification

- As of November 1, 2018, organizations subject to The Personal Information Protection and Electronic Documents Act (PIPEDA) will be required to:
  - report to the Privacy Commissioner of Canada breaches of security safeguards involving personal information that pose a real risk of significant harm to individuals
  - notify affected individuals about those breaches, and
  - keep records of all breaches

## What is a breach of security safeguards?

A breach of security safeguards is defined in PIPEDA as: the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards that are referred to in clause 4.7 of Schedule 1 of PIPEDA, or from a failure to establish those safeguards.

## Does this apply to small businesses?

Yes. Large and small business will be subject to PIPEDA requirements to report and notify breaches of security safeguards that pose a real risk of significant harm, and to keep records of all breaches of security safeguards.

## Are there financial penalties?

Yes. Under PIPEDA it is an offence to **knowingly contravene** PIPEDA's reporting, notification and record-keeping requirements relating to breaches of security safeguards, and doing so could lead to fines.

The OPC does not prosecute offences under PIPEDA or issue fines. What the OPC can do is refer information relating to the possible commission of an offence to the Attorney General of Canada, who would be responsible for any ultimate prosecution.

For additional information you can [read what the law says](#).



## FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT

### Protection of personal information

**30** A public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

### Storage and access must be in Canada

**30.1** A public body must ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada, unless one of the following applies:

- (a) if the individual the information is about has identified the information and has consented, in the prescribed manner, to it being stored in or accessed from, as applicable, another jurisdiction;
- (b) if it is stored in or accessed from another jurisdiction for the purpose of disclosure allowed under this Act;
- (c) if it was disclosed under section 33.1 (1) (i.1).



# FOIPPA – There are exceptions!

## Disclosure inside or outside Canada

**33.1** (1) A public body may disclose personal information referred to in section 33 inside or outside Canada as follows:

:

(e) to an individual who is a minister, an officer of the public body or an employee of the public body other than a service provider, if

(i) the information is necessary for the performance of the duties of the minister, officer or employee, and

(ii) in relation to disclosure outside Canada, the outside disclosure is necessary because the individual is temporarily travelling outside Canada;

(e.1) to an individual who is a service provider of the public body, or an employee or associate of such a service provider, if

(i) the information is necessary for the performance of the duties of the individual in relation to the public body, and

(ii) in relation to disclosure outside Canada,

:



:

(h) to the minister responsible for the [Coroners Act](#) or a person referred to in section 31 (1) of that Act, for the purposes of that Act;

(i) if

(i) the disclosure is for the purposes of collecting amounts owing to the government of British Columbia or a public body by

(A) an individual, or

(B) a corporation of which the individual the information is about is or was a director or officer, and

(ii) in relation to disclosure outside Canada, there are reasonable grounds for believing that

(A) the individual the information is about is in, resides in or has assets in the other jurisdiction, or

(B) if applicable, the corporation was incorporated in, is doing business in or has assets in the other jurisdiction;

:



NEW!

(p.1)if the disclosure

(i)is necessary for the processing of information and if that processing does not

(A)involve the intentional access of the information by an individual, or

(B)result in the storage of personal information, other than personal information that is metadata, outside Canada, and

(ii)in the case of disclosure outside Canada, results in temporary access that is limited to the minimum period of time necessary to complete the processing;

(p.2)if the information is metadata that

(i)is generated by an electronic system, and

(ii)describes an individual's interaction with the electronic system, and if,

(iii)if practicable, personal information in individually identifiable form has been removed from the metadata or destroyed, and

(iv)in the case of disclosure to a service provider, the public body has prohibited any subsequent use or disclosure of personal information in individually identifiable form without the express authorization of the public body;



NEWER!

## **Disclosure outside of Canada**

**33.1** A public body may disclose personal information outside of Canada only if the disclosure is in accordance with the regulations, if any, made by the minister responsible for this Act.

## **Repealed**

**33.2** [Repealed 2021-39-21.]

## **Disclosure of personal information in records available to public without request**

**33.3** (1) A public body may disclose to the public a record that is within a category of records established under section 71 (1).

(2) A ministry may disclose to the public a record that is within a category of records established under section 71.1 (1).



# Privacy Teams

- can respond when things don't go well
- investigate breaches
- advise on important files
- recommend others check in with privacy team early and often on projects
- perform audits, develop policy, provide training



# Privacy

- **trust people with information and to make the right decisions once they have the training**
- continually question whether you are applying the rules or others are on your behalf
- up to the privacy commissioner to regulate, oversee, adjudicate
- PII: personally identifiable information – info that can directly identify or can be combined with other identifiers
- PHI: personal health information



# Privacy

- each of a pair of twins could feel differently
- examples of young people, older people
- example of crossing the border
- self determination changes moment by moment
- privacy is something you negotiate all day
- example of being asked for postal code





# Privacy Exercise



**Kate Klonick**  
@Klonick

Thread for those who teach or study information privacy: So I gave my information privacy students (2Ls and 3Ls) a project for spring break, after we learned about anonymous speech, reasonable expectation of privacy, third party doctrine, and privacy by obscurity. 1/6

8:34 AM · Mar 5, 2019 · [Twitter Web Client](#)

1.3K Retweets 2.4K Likes



**Kate Klonick** @Klonick · Mar 5, 2019  
Replying to @Klonick

The assignment was this: At some point over break, when you're in a public place, using only Google see if you can de-anonymize someone based on things they say loudly enough for lots of others to hear and/or things that are displayed on their clothing or bags 2/6

22

337

709



**Kate Klonick** @Klonick · Mar 5, 2019

At first they were like "Professor Klonick this is so creepy," but I said "we're not doing anything with this information, this is an exercise in whether or not public places are private and whether we expect them to be." 3/6

3

37

302



**Kate Klonick** @Klonick · Mar 5, 2019

The project has had the best results. They have been writing to me all break being like, "this is crazy. I found the guy in the front of me on the plane in 3 minutes" or "this person just gave out their entire credit card number on full train over the phone" etc. 4/6

6

55

382



**Kate Klonick** @Klonick · Mar 5, 2019

Most significantly, a number who had clung to the idea of "I don't care if anyone's watching, I have nothing to hide" were shocked into seeing the privacy issues. Including a future district attorney. 5/6

3

71

524



**Kate Klonick** @Klonick · Mar 5, 2019

I'm pretty thrilled with this, as a teaching tool, but also as a really interesting lesson in how to check our own expectations about being private in public and how clearly we're not. And it's a reminder that norms, not laws, govern a lot of our day to day personal privacy. 6/6

19

96

733



# Privacy Exercise



Bill  
Fitzgerald

## Privacy and Security Exercise

2 min read

Do this exercise with your phone, tablet, and/or any computer you use regularly.

Imagine that someone has accessed your device and can log in and access all information on the device.

- If they were a thief, what information could they access about you?
- If they were a blackmailer, what information could they access about you?
- What information could they access about your friends, family, or professional contacts?
- If you work as a teacher, counselor, consultant, or other type of advisor: what information could someone glean about the people you work with?

As you do this exercise, be sure to look at all apps (on a phone or tablet), online accounts accessible via a web browser, address books, and ways that any of this information could be cross referenced or combined. For example, what information could be accessed about people you "know" via social media accounts?

- What steps can you take to protect this information?
- Assuming that someone you know has comparable information about you, what steps would you want them to take?

Are there differences between the steps you could take, and the steps you would want someone else to take? What accounts for those differences?

When it comes to protecting information, we are connected. At some level, we are as private and secure as our least private and secure friend.

# Privacy

- example of Smart Meters
- personal expectation of privacy does not always translate to the law
- context not always dictated by you
  - eg. border crossing
- people don't always make good choices



# Privacy

- what is personal information?
- anything BUT your contact information - name and phone and address if you are at a business





# Privacy

## What is personal information?

[https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/information-privacy/privacy-impact-assessments/pia\\_guidelines.pdf](https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/information-privacy/privacy-impact-assessments/pia_guidelines.pdf)

FOIPPA provides a simple but broad definition of personal information:

**“Recorded information about an identifiable individual other than contact information.”**

Note: contact information is information used to contact someone at a place of business.

The following is a non-exhaustive list of personal information examples:

- **name, address, email address, or telephone number;**
- **age, sex, religious beliefs, sexual orientation, marital or family status, blood type;**
- **an identifying number, symbol or other particular assigned to an individual;**
- **information about an individual’s health care history, including a physical or mental disability;**
- **information about an individual’s educational, financial, criminal or employment history; and**
- **personal views or opinions.**

# Privacy

- includes when you combine things – the mosaic effect
  - gender, age, car you drive, city you drive in may not be personal information
  - but if it identifies an individual would be
- context is important - think about it for yourself
  - your opinions, things you think
  - **unless they are about someone else**

**and then it is their information**



# Privacy

- some places do not control the information
- law tries to give you a choice to control
  - people ask “can I have the information so I can share it” and you say yes...
- sometimes you don’t have to ask
  - eg. description of fleeing robber
  - lost right to privacy – supporting an investigation
- privacy law applies to inmates same as citizens



# Privacy

## The 10 Privacy Principles

- 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.
- 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.
- 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.
- 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.
- 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.



- 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.  
**Limit Retention.** Personal information used to make a decision about an individual must be retained for at least one year. Information must be destroyed in accordance with any applicable records retention schedules. Find your Records Officer 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.

For more information on the privacy principles and resources, visit: [www.gov.bc.ca/privacyprinciples](http://www.gov.bc.ca/privacyprinciples)



# Privacy

- not making good choices if don't know why someone is asking
- privacy is about limiting the use, disclosure, retention based on what you told someone you want to do with the information
- surprises are never a good thing
- force people to not surprise you
- ensuring accuracy of information is important



# Privacy

- how do you know what they have if you can't get access to it?
  - anyone who has your info should give it to you
  - you shouldn't have to be in the dark with your information
- as individuals not bound to same laws though can't set up a camera in your front yard pointed at neighbours' bedroom



# Privacy

- individual to individual need to ask do I trust this person enough to do the right thing?
- organizations have a requirement – they have to listen if the information is wrong
  - example with “the information you used to assess me was wrong”
  - you have the right to ask people to correct the information



# Privacy

- in some cases the information will not be corrected – eg. gender at birth – if it was correct on that day
- recourse: when you have been wronged there is someone to help you with it (eg. OIPC)



# Quote

*“The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; **but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.**”*

~ “The Right To Privacy” – Harvard Law Review



# Correlation

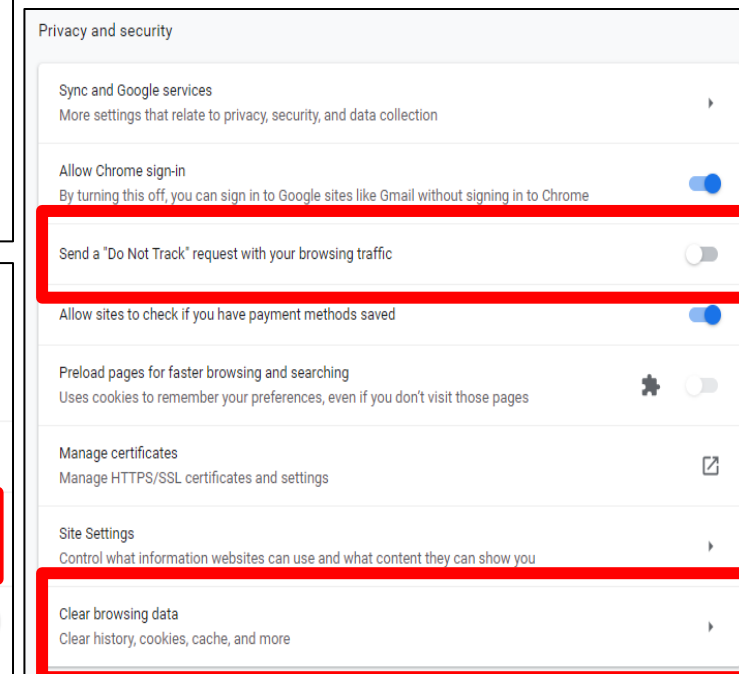
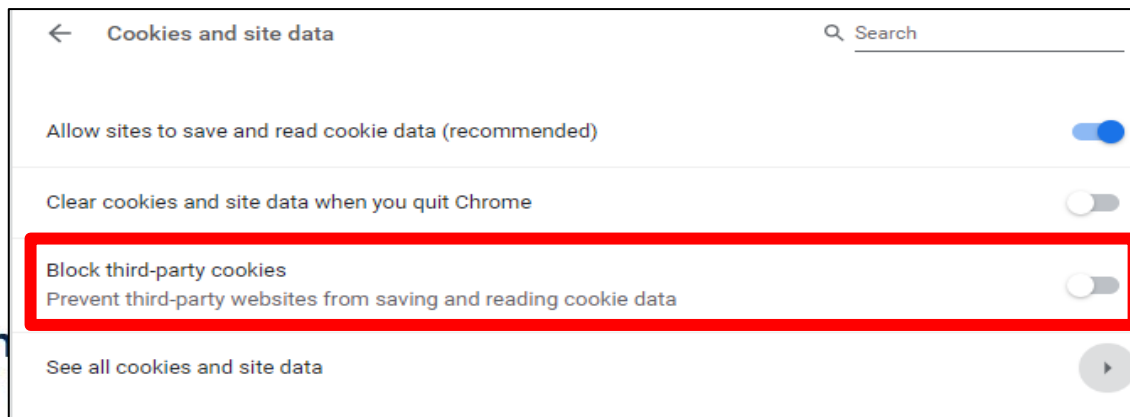
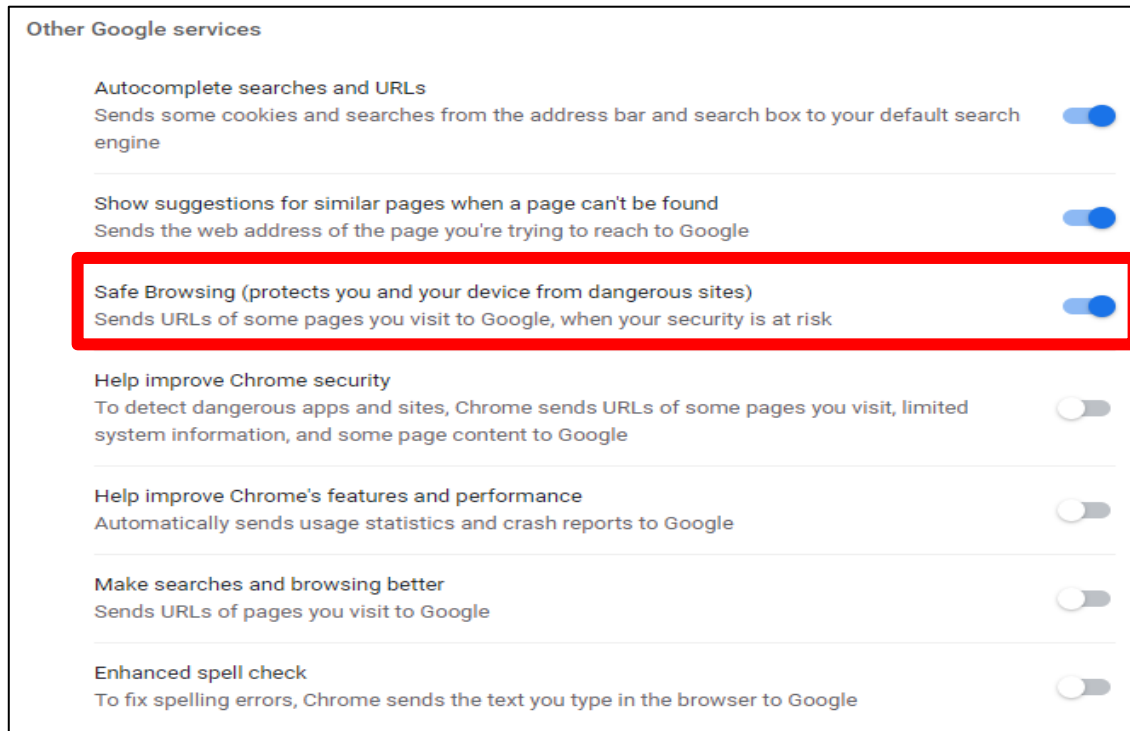
French- & English-speaking women between the ages of 31 and 56  
located in a 10-mile radius of **Victoria, BC**,  
who work either from home or from a small office in the retail  
production industry,  
who are “fit moms” and “green moms” of grade school kids,  
who have friends with an anniversary within 30 days or  
friends with upcoming birthdays,  
who have university degrees from either UVic or UBC  
who are active in politics and either liberal or very liberal and self-  
proclaimed New Democrats,  
who live in a **condo or apartment built after 2011, between 1,000 and  
1,500 square feet**,  
who enjoy attending ballet, theatre and musical theatre movies,  
who frequently travel internationally, plan to travel to Spain,  
and **used a travel app within the last month**,  
who are categorized as “foodies” and “green living” buyers,  
who tend to spend above average in **high-end retail online stores**,





# Browser Settings

- clear browsing data including cookies on occasion
- browser privacy & security settings



# Summary

- privacy is only dead if you give up your choices and decision making
- privacy is only dead if you allow it to be



# Privacy Impact Assessments

- process to make sure personal information collected and used by organizations is protected
- personal information belongs to the person it's about
- 5 steps:
  - 1) download template
  - 2) fill out template
  - 3) submit for review
  - 4) get signatures
  - 5) start project



# Privacy Impact Assessments

- template
- identify person filling out and the initiative

	<b>Privacy Impact Assessment for</b> [organization] PIA# [will be assigned by privacy team]
---	---

## Why do I need to do a PIA?

Section 69 (5) of the *Freedom of Information and Protection of Privacy Act* (FOIPPA) requires the head of a ministry to conduct a privacy impact assessment (PIA) in accordance with the [directions](#) of the minister responsible for FOIPPA. Section 69 (5.1) requires the head to submit the PIA to the minister responsible for FOIPPA for review, [during the development](#) of any new system, project, program or activity, or proposed enactment, or when making changes to an existing one.

## What if my initiative does not include personal information?

Ministries still need to complete Part 1 of the PIA and submit it, along with the signatures pages, to privacy team even if it is thought that no personal information is involved. This ensures that the initiative has been accurately assessed.

## Part 1 – General

Name of Org:			
PIA Drafter:			
Email:		Phone:	
Program Manager:			
Email:		Phone:	

*In the following questions, delete the descriptive text and replace it with your own.*

### 1. Description of the Initiative


*This section should provide a general description of the initiative and the context in which it functions. This could include the purpose of the initiative, its benefits, the larger process (if any) that it is part of, how it functions, the parties involved, etc.*

### 2. Scope of this PIA

*This section should explain, where applicable, exactly what part or phase of the initiative the PIA covers and, where necessary for clarity, what it does not cover. For example, if a organization is overhauling its engagement process to better align with a new initiative and is launching new website. This section may also describe what phase of the initiative this PIA covers.*

### 3. Related Privacy Impact Assessments

*This section should identify, where applicable, PIAs for other parts of the initiative or any PIAs that were previously completed for this initiative. To follow on from the above example, this section may cite a PIA that has already been completed on the organization's website.*

	<b>Privacy Impact Assessment for</b> [organization] PIA# [will be assigned by privacy team]
---	---

## Elements of Information or Data

*Please list the elements of information or data involved in the initiative. This could include client's name, age, address, work/home email, work/home phone number, educational history, employment history, work status, health information, financial information, photos, comments on a blog, or information specific to your subject area, like stumpage totals, fish license numbers, visitor centre stats, or hiring data.*

If personal information is involved in your initiative, please continue to the next page to complete your PIA.

If no personal information is involved, please submit Parts 1, 6, and 7 unsigned to the privacy team. A privacy advisor will be assigned to your file and will guide you through the completion of your PIA.

# Privacy Impact Assessments

- is data outside Canada? \*\*
- is data linked between databases or orgs?



## Privacy Impact Assessment for [organization] PIA# [will be assigned by privacy team]

### Part 2 – Protection of Personal Information

In the following questions, delete the descriptive text and replace it with your own.

#### 4. Storage or Access outside Canada

Please provide a brief description of whether your information can be accessed from outside Canada, for example, by a service provider that is repairing a system, or if your information is being stored outside Canada, for example, in the “cloud”. If your data is stored within Canada and accessible only within Canada, please indicate this.

#### 5. Data-linking Initiative\*

In FOIPPA, “data linking” and “data-linking initiative” are strictly defined. Answer the following questions to determine whether your initiative qualifies as a “data-linking initiative” under the Act. If you answer “yes” to all 3 questions, your initiative may be a data linking initiative. If so, you will need to comply with specific requirements under the Act related to data-linking initiatives.

1. Personal information from one database is linked or combined with personal information from another <u>database</u> .	yes/no
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	yes/no
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	yes/no
If you have answered “yes” to all three questions, please contact a PCT Privacy Advisor to discuss the requirements of a data-linking initiative.	



## Privacy Impact Assessment for [organization] PIA# [will be assigned by privacy team]

#### 6. Common or Integrated Program or Activity\*

In FOIPPA, “common or integrated program or activity” is strictly defined. Answer the following questions to determine whether your initiative qualifies as “a common or integrated program or activity” under the Act. If you answer “yes” to all 3 of these questions, you must comply with requirements under the Act for common or integrated programs and activities.

1. This initiative involves a program or activity that provides a service (or services);	yes/no
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	yes/no
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	yes/no
Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.	

\* Please note: If your initiative involves a “data-linking initiative” or a “common or integrated program or activity”, consultation on this PIA must take place with the Office of the Information and Privacy Commissioner (OIPC). PCT will facilitate the consultation with the OIPC.

For future reference, ministries are required to notify the OIPC of a “data-linking initiative” or a “common or integrated program or activity” in the early stages of developing the initiative, program or activity. PCT will help facilitate this notification.

#### 7. Personal Information Flow Diagram and/or Personal Information Flow Table

Please provide a diagram and/or table that shows how your initiative will collect, use, and/or disclose personal information (see examples below). Your diagram and/or table must also include the authorities for the collection, use, and disclosure of personal information, as laid out in FOIPPA. It should also outline the flows of personal information wherever it is transmitted or exchanged.

Both a flow diagram and a table must be included if the PIA is related to a common or integrated program or activity or a data-linking initiative.



# Privacy Impact Assessments

- personal information flow diagram
- risks
- do you notify that personal information will be collected?

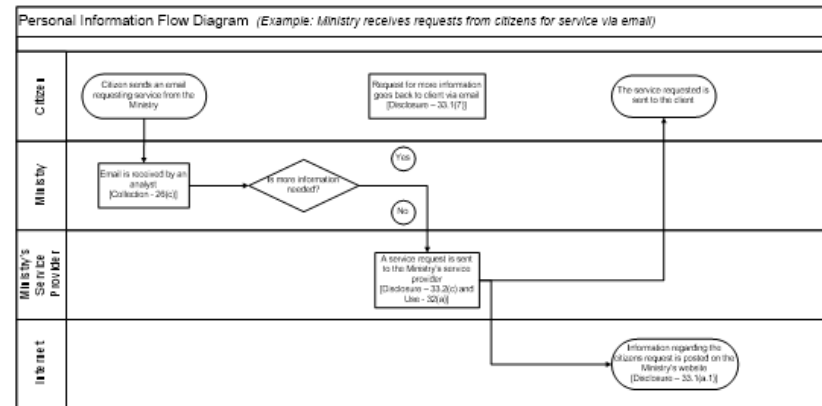


## Privacy Impact Assessment for [organization] PIA#[will be assigned by privacy team]

For ease of reference, the collection, use, and disclosure authorities in FOIPPA can be found in the [appendices](#). If you do not know what the relevant authorities are, please contact a PCT privacy advisor.

Depending on the complexity of your initiative, you may choose to provide one general diagram for the initiative, and more specific diagrams for particular components. If multiple organizations will collect, use, or disclose personal information, the diagram should identify how each organization is involved in the initiative.

Example:



Examples can be removed and additional lines added as needed.

Personal Information Flow Table			
	Description/Purpose	Type	FOIPPA Authority
1.	Email received from client requesting service	Collection	26(c)
2.	Email client back requesting more information	Disclosure	33.1(7)
3.	Service request transferred to service provider contracted by Ministry	Disclosure & Use	33.2(c) and 32(a)



## Privacy Impact Assessment for [organization] PIA#[will be assigned by privacy team]

### 8. Risk Mitigation Table

Please identify any privacy risks associated with the initiative and the mitigation strategies that will be implemented. Please provide details of all such strategies. Also, please identify the likelihood (low, medium, or high) of this risk happening and the degree of impact it would have on individuals if it occurred.

Examples can be removed and additional lines added as needed.

Risk Mitigation Table				
	Risk	Mitigation Strategy	Likelihood	Impact
1.	Employees could access personal information and use or disclose it for personal purposes	Role-based access	Low	High
2.	Request may not actually be from client (i.e. their email address may be being used by someone else)	Implementation of identification verification procedures	Low	High
3.	Client's personal information is compromised when transferred to the service provider	Transmission is encrypted and over a secure line	Low	High
4.	Inherent risks in sending personal information to a client via email	Policy developed to inform clients of risk and ask if they would like the information via a different medium, such as through the mail	Medium	Medium

### 9. Collection Notice

If your initiative is collecting personal information directly from individuals you must ensure that all individuals involved are told the following:

- The purpose for which the information is being collected
- The legal authority for collecting it, and
- The title, business address and business telephone number of an officer or employee who can answer questions about the collection.

Please include your proposed wording for a collection notice and where it will be located for individuals to read before collection takes place. You can also attach a screen shot or a copy of your form where the collection notice would be located. For further help with collection notices please see the "Collection Notice Tip Sheet" located on the [CIO's website](#).



# Privacy Impact Assessments

- security controls in place
- corrections to data
- disclosure of information



## Privacy Impact Assessment for [organization] PIA#[will be assigned by privacy team]

### Part 3 – Security of Personal Information

*If this PIA involves an information system, or if it is otherwise deemed necessary to do so, please consult with your Ministry Information Security Officer (MISO) when filling out this section. Your MISO will also be able to tell you whether you will need to complete a separate assessment called a Security Threat and Risk Assessment (STRA) for this initiative.*

10. Please describe the physical security measures related to the initiative (if applicable).

*For example: locked cabinets, securely stored laptops, or key card access to the building.*

11. Please describe the technical security measures related to the initiative (if applicable).

*For example: use of government firewalls, document encryption, or user access profiles assigned on a need-to-know basis.*

12. Does your branch rely on security policies other than the Information Security Policy?

*Please describe any specific policies and procedures and provide contact details for someone who could answer further questions regarding these policies and procedures.*

13. Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

*For example: role-based access.*

14. Please describe how you track who has access to the personal information.

*For example: audit trails or physical sign-in and sign-out of files.*

### Part 4 – Accuracy/Correction/Retention of Personal Information

15. How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If personal information will be disclosed to others, how will the ministry notify them of the update, correction or annotation?

*For example: users have access to update their own information or, notes will be made on a government case file.*

16. Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.



## Privacy Impact Assessment for [organization] PIA#[will be assigned by privacy team]

17. If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.

*For example: check to see that the information was obtained from a reputable source such as another government agency.*

18. If you answered "yes" to question 17, do you have approved records retention and disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?

*If you do not have a schedule, please document how these records will be kept until a schedule is in place. Please describe retention schedules that apply where retention exceeds the one year requirement of the FOIPPA. Please contact your [Ministry Records Officer](#) if you need assistance.*

### Part 5 – Further Information

19. Does the initiative involve systematic disclosures of personal information? If yes, please explain.

*For example: your ministry has a regular exchange of personal information (both collection and disclosure) with the federal government in order to provide services to your ministry's clients. Under section 69 (2), this information is required to be published in the Personal Information Directory (PID), which is maintained and published by PCT.*

**Please check this box if the related Information Sharing Agreement (ISA) has been prepared. If you have general questions about preparing an ISA, please contact the Privacy and Access Helpline.**

If an ISA has been prepared as part of your initiative, please complete the fields in the table below by deleting the descriptive text in the right-hand column and replacing it with your own.

Information Sharing Agreement – Required Information	
Description	A regular exchange of personal information between the Ministry of Administration (MADMIN) and the University of Life in order to provide scholarships to eligible residents of BC.
Primary ministry/government agency involved	MADMIN
All other ministries/government agencies and public bodies involved	University of Life

# Privacy Impact Assessments

- more contact info
- research
- personal info bank
- signatures



## Privacy Impact Assessment for [organization] PIA#[will be assigned by privacy team]

Business contact title	Manager, Administration Services
Business contact telephone number	250-555-5555
Indication of whether or not personal information is involved	Yes
Start date	26-Apr-14
End date (if applicable)	28-Apr-15

20. Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.

For example: you will be disclosing information to PhD students so they can conduct research.

Please check this box if the related Research Agreement (RA) is attached. If you require assistance completing an RA please contact a PCT advisor.

21. Will a personal information bank (PIB) result from this initiative?

A personal information bank means a collection of personal information that is organized or retrievable by the name of an individual or by an identifying number, symbol, or other particular assigned to an individual. Under section 69 (2) of FOIPPA, this information is required to be published in the PID, which is maintained and published by PCT.

If yes, please complete the fields in the table below by deleting the descriptive text in the right-hand column and replacing it with your own.

Personal Information Bank – Required Information	
Description	Personal contact information of branch staff in case of emergency
Primary ministry/government agency involved	MADMIN
All other ministries/government agencies and public bodies involved	None
Business contact title	Office Manager, Administration Services
Business contact telephone number	250-555-5555



## Privacy Impact Assessment for [organization] PIA#[will be assigned by privacy team]

Please ensure Parts 6 and 7 are attached unsigned to your submitted PIA.

### Part 6 – PCT Comments and Signatures

This PIA is based on a review of the material provided to PCT as of the date below. If, in future any substantive changes are made to the scope of this PIA, the ministry will have to complete a PIA Update and submit it to PCT.

Privacy Advisor Privacy, Compliance and Training Branch Ministry of Finance	Signature	Date
Director or Manager Privacy, Compliance and Training Branch Corporate Information and Records Management Office Ministry of Finance (if Personal Information is involved in this initiative)	Signature	Date

# Privacy Impact Assessments



## Privacy Impact Assessment for [organization] PIA#[will be assigned by privacy team]

- more signatures

### Part 7 – Program Area Comments and Signatures

Program Manager	Signature	Date
Ministry Contact Responsible for Security (Signature not required unless MISO has been involved.)	Signature	Date
Assistant Deputy Minister or Designate (if Personal Information is involved in this initiative)	Signature	Date
Executive Director or equivalent (if no Personal Information is involved in this initiative)	Signature	Date

A final copy of this PIA (with all applicable signatures and attachments) must be provided to PCT for its records to complete the process. PCT is the designated office of primary responsibility for PIAs under ARCS 293-60.

*PCT will publish the ministry name, business contact details and a brief summary of the PIA to the Personal Information Directory (PID) as required by section 69(2) of FOIPPA. If you have any questions, please contact your privacy advisor at PCT or call the Privacy and Access Helpline at 250 356-1851.*

# Summary

- privacy is a constantly negotiated battleground
- the circumstances today are different
- we produce a lot more information than we did
- ... and it seems we can't live without that information

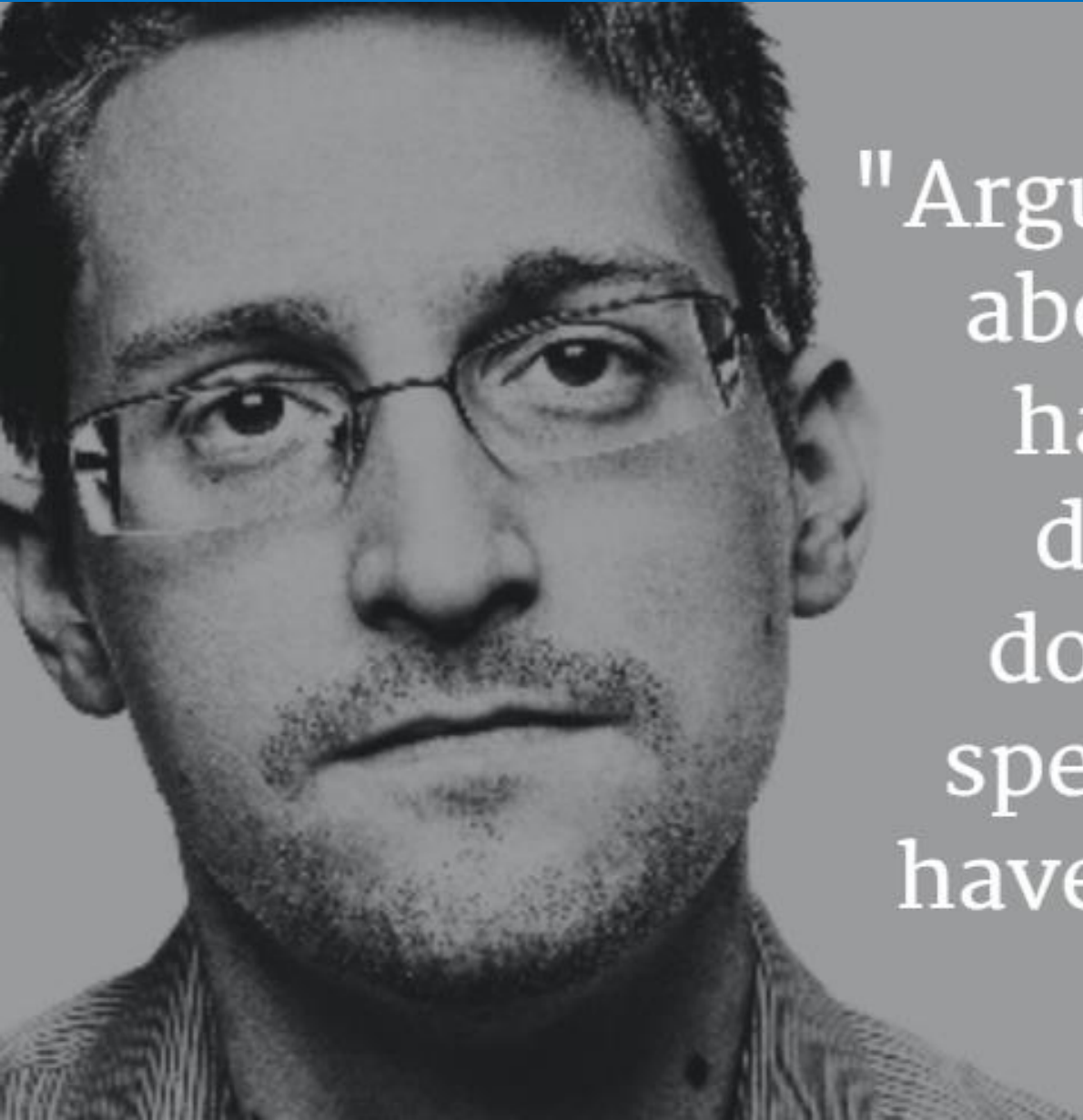


# Myths

- MYTH: privacy doesn't matter because I'm not doing anything wrong
  - this is usually said by people who are about to take your privacy away
  - the point is you get to hide it
  - it's what we choose to share with whom



# Quote



"Arguing that you don't care about privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say."



# Myths

- MYTH: you need an individuals' consent to do anything with their information
  - this is not the law
  - you get to choose to the greatest degree possible is the principle
- information about you that has your name pulled off – eg. hospital visit and how long your stay was – researchers may use the information
- privacy legislation has provisions where consent is not required



# Summary

- often hear people “wielding” consent
  - eg. “I never consented to that!”
- it is important to push on the rights
  - won’t always win
  - sometimes don’t have choice



# Myths

- MYTH: if information is publicly available anyone can do anything they want with it
  - eg. employer shouldn't look at Facebook to decide if you get a job
  - just because they "can't" doesn't mean they "won't"
  - are digital assistants infringing? Yes!
  - don't want someone/something listening when doesn't need to be
  - don't put yourself in a place to be victimized



# Facts

- public body needs authority to collect under FOIPPA
  - authorized under an Act
  - for law enforcement
  - related directly to and necessary for an operating program or activity
  - necessary for planning or evaluating a program or activity of the public body
  - the information is collected by observation at a public and voluntarily attended presentation, ceremony, performance, sports meet or similar event
- how PI collected:
  - directly from the individual
  - must notify the individual of the purpose
  - legal authority
  - should provide who to contact if there are questions



# Myths

- MYTH: the laws alone will protect me
  - treat it as a dialog, have the conversation
  - very awkward when someone asks you for something and you say no
  - you can say “I don’t think you can ask me that”
  - push the to the point so they have to prove it
  - force them to demonstrate
  - if they are entitled they should be able to prove it
- examples with Home Depot, other retailers

and returns



# Summary

- to be inquisitive is a positive thing
- be critical, analytical and do so as much as you can
- people often rely on laws but incidents do happen
- administrative errors by far are the most common issue
  - eg. sent to wrong address,  
wrong name,  
double-stuffed envelopes





# Summary

- because incidents happen doesn't mean ramifications of incidents are not very serious
- privacy as an industry is not going away
  - get involved in drones, AI, genomics, biometrics, etc.
  - everyone should have someone responsible for privacy
  - free resource to call: BC Privacy and Access Helpline



# Assigned Reading

- read Chapters 24, 27, 28, 31, 33 and Foreign Threats to the Democratic Process for next time
- complete the lab



University  
of Victoria

