The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are white with detailed capitals and fluted shafts. The entire slide is framed by a thin brown border.

Commercial vs. Broader Public Sector Privacy – Security Some Thoughts

Jan 22, 2018

The background of the slide features a faint, light blue image of classical architectural columns, possibly from a university building, which are partially visible behind the text boxes.

Our Presentation

Your personal information is treated differently in

- Commercial vs Broader Public Sector contexts
- What are the major differences?
- Data privacy / security at the University

TECHNOLOGY / INFORMATION

Think about all technological tools, platforms, apps, sites, service providers, companies, etc. that have information about you

What do YOU know about ...

- Who has what information about you?
- How, when, where, when it is being used?
- Are you being analyzed, commoditized?

The background of the slide features a light blue gradient. On the left side, there is a faint, semi-transparent image of classical architectural columns, likely from a government building, which adds a sense of formality and law to the theme.

PRIVACY

PRIVACY IS...GENERALLY

1. Privacy of the person
 - 'bodily privacy', blood samples, etc.
2. Privacy of personal behaviour
 - religion, politics, etc., including 'media privacy'
3. Privacy of personal communications
 - 'interception privacy', various media
4. Privacy of personal information // data
 - 'data/information privacy', control of data

The background of the slide features a low-angle, upward-looking perspective of several classical columns, likely from a government building. The columns are light-colored with detailed capitals. The image is faded and serves as a background for the text.

Snowden on Privacy, nov 10, 2016

The background of the slide features a light blue gradient. On the left side, there is a vertical strip showing a close-up of classical architectural columns with Corinthian capitals. The text is centered horizontally and partially overlaps the columns.

ORDERING PIZZA IN 2015

PRIVACY IS...

A SET OF CONCEPTS

**Philosophical, Social, Ethical,
About sanctity and inviolability of the person**

...AND A BUNDLE OF LEGAL RIGHTS

(WHICH VARY SOMEWHAT BY WITH JURISDICTION)

...and WHICH SUPPORT:

Your control of your personal information

The background of the slide features a faint, blue-tinted image of classical architectural columns, likely from a government building, which adds a sense of formality and legal authority to the presentation.

INFORMATION PRIVACY

Key principle of modern privacy laws

Control of your own personal information

...Usually by regulating collection, use, and disclosure of your personal information by govt., companies, etc.

PRIVACY LIMITS

Privacy is never absolute; lots of exceptions for:

- Law enforcement
- Public health
- Legal processes (generally supersede statutory privacy protections)
subpoenas, summonses, court orders, etc.
- Other legislation
emergency management, health protection, anti-terrorism etc.

...data protection laws are made by law-makers, who may discover new priorities, exceptions or other reasons to change or abrogate privacy.

The balance is found in the same way as other political/social balances. Public involvement, consultation and advocacy help to guide politicians...

National Security???

PERSONAL INFORMATION IS...

INFORMATION ABOUT AN **IDENTIFIABLE INDIVIDUAL**
EXCEPT IN A BUSINESS OR PROFESSIONAL CAPACITY

...FROM [FIPPA](#) S. 2, **including, but not limited to;**
ethnic origin, race, religion, age, sex, sexual orientation,
education, financial, employment, medical, psychiatric,
psychological or criminal information, identifying
numbers; S.I.N., home address, home phone number,
photos, videos, identifiable recordings of individual,
name appearing with / revealing other personal
information **etc.**

Does not include actions in business or professional capacity
eg. name, position, routine work information, actions at work

LAWS BASED ON **CONSENT**

FEDERAL

Personal Information Protection and Electronic Documents Act [PIPEDA](#)

Strongly consent-based; Incorporates CSA Code Principles;

Commercial Sector Privacy Law;

regulates commercial activity with personal information, inter-provincial data flows and federally-regulated endeavours like banking, insurance and telecommunications

(Some provincial laws in Que, Alta, BC.)

Most jurisdictions have broadly consent-based commercial privacy laws

Canadian Federal Privacy Laws

Parliament of Canada [page](#) on Federal Privacy Laws (including PIPEDA)

Introduction

Classically understood as the “right to be left alone,” privacy in today’s high-tech world has taken on a multitude of dimensions. To experts in this area, privacy is equated with the right to enjoy private space, to conduct private communications, to be free from surveillance and to have the sanctity of one’s body respected. **To most people, it is about control – what is known about them and by whom.**

Privacy protection in this country essentially focuses on safeguarding personal information. **Drawing upon generally accepted fair information practices, federal data protection laws seek to allow individuals to decide for themselves, to the greatest extent possible, with whom they will share their personal information, for what purposes and under what circumstances.** Thus, what is an unacceptable privacy intrusion to one person, may not be to another. ...

CSA PRIVACY CODE PRINCIPLES

1. Accountability

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

2. Identifying Purposes

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

3. Consent

The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate.

4. Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

5. Limiting Use, Disclosure and Retention

Personal information shall not be used or disclosed for purposes other than those for which it is collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of the stated purposes.

6. Accuracy

Personal information shall be as accurate, complete and up-to-date as is necessary for the purpose for which it is used.

7. Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

8. Openness

An organization shall make specific information about its policies and practices relating to the management of personal information readily available to individuals.

9. Individual Access

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information, and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.







10. Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

The background of the slide features a low-angle photograph of classical columns on the left side, which fades into a solid light blue gradient that covers the rest of the slide. The entire composition is framed by a thin brown border.

SURVEILLANCE

A FEW (CURRENT) TYPES

1. ONLINE; BROWSING/SURFING/BUYING
2. EMAIL, SOCIAL MEDIA
3. TELEPHONY AND VOICEMAIL
4. “SMART” DEVICES, INTERNET OF THINGS
5. ALWAYS ON APPS/DEVICES
6. VIDEO /PERSONAL / POLICE BODY - CAMERAS
7. FACIAL RECOGNITION 
8. MEDICAL RECORDS  
9. MEDICAL TELEMETRY 
10. EVENT DATA RECORDERS EDRs  
11. ETC.

COMMERCIAL PRIVACY STATEMENTS

They detail how your information is collected, used, and shared. They can be lengthy.

[Google Privacy Policy](#)

....They can be difficult to understand. You be the judge.

You often consent just by being on a website:

“By using this website, you agree to...”

“When you use this website, your information...”

“privacy statements” are very often notices of data harvesting/aggregation/use activities

ANALYTICS

Google Analytics is now the most widely used web analytics service on the internet

[Wikipedia article on Google Analytics](#)

With section on privacy issues

But, very good for business:

[9 Awesome Things Your Can Do With Google Analytics 5](#)

SOCIAL MEDIA

[Jennifer Golbeck Ted talk “Curly Fries” 2013](#) ...Social media information and its use to predict how you will behave...

“It’s sometimes said of Facebook that the users aren’t the customer; they’re the product.”

Behavioural patterns of large numbers looped back and applied to the individual –for advertising or ?

[Alessandro Acquisti Ted talk “What will a future without secrets look like?”](#)

Public/private blurring, including how to match a photo to an individual’s sensitive personal information

CRYSTAL KNOWS

An app that tells you how to communicate by email based on personality, using only publicly available information about you

<https://www.crystalknows.com>

[Guardian article on Crystal knows](#)

[Youtube Review of Crystal knows](#) by KW Labs

IT IS ALL ABOUT CONSENT

Commercial personal information exploitation is based on consent.

We consent [John Oliver Show on Net Neutrality](#)

Read privacy statements (if you have time) In 2012, a month or even 76 days, according to this [NPR article](#) , or this [Atlantic article](#).

...Check out and maybe [delete your Google history](#) back to 2005

It knows you better than you know yourself. It knows every smartphone you've thought about buying, every coworker you've tried to find dirt on, every embarrassing ailment you've suffered...

Or you could obfuscate, as this [Guardian article](#) details.

But really, we like convenience.

We have been “figured out” by business

IT IS ALL ABOUT ADVERTISING

We have consented to sharing of our information by businesses, service providers, sites, apps, etc. etc.

You're Soaking In It Documentary

Documentary on how all your online activity is tracked continually across platforms, websites and activities

- aggregated and shared by (many many) companies to develop a better profile of you than you could remember
- used to predict your behaviours and activities to know before you do what you might do or buy next
- auctioned in real time to serve you personalized adverts while you browse, email, etc.

TECHNOLOGY / INFORMATION

Think about all technological tools, platforms, apps, sites, service providers, companies, etc. that have information about you

What do YOU know about ...

- Who has what information about you?
- How, when, where, when it is being used?
- Are you being analyzed, commoditized?

The background of the slide features a light blue gradient. On the left side, there is a vertical strip showing a close-up, low-angle view of classical columns with Corinthian capitals, rendered in a semi-transparent blue style. The entire slide is framed by a thin white border, which is itself set within a larger brown border.

MINORITY REPORT ADVERTISING

OTHER PROBLEMS

If the information is out there, it (and maybe you) are vulnerable
Hacking, Data theft...happening (more) all the time

Keren Elazari on [hacking](#)

Including Ashley Madison, medical, cars, drones, target, ,etc,etc...

Yahoo Data [Breach](#) ... exposed Sept 2016

- state-sponsored actors
- 200 Million Yahoo accounts

Just Google biggest [data breaches](#)

Government hacking

[Stuxnet](#); software-based attack on Iranian nuclear program



The background of the slide features a light blue gradient. On the left side, there is a faint, semi-transparent image of classical architectural columns, likely from a government building, which adds a sense of formality and law to the presentation.

BROADER PUBLIC SECTOR PRIVACY LAWS

PUBLIC SECTOR PRIVACY LAWS ARE...

An approximated one-size solution for limiting the spread of our personal information, so that we don't lose control of it

Public sector privacy laws restrict data and protect confidentiality.

They limit collection, use and disclosure of personal information...
To information needed for official lawfully authorized activities.

Only this personal information can be collected, used or disclosed.

They differ in this critical way from commercial sector privacy laws.

Commercial sector privacy laws are based on consent - you can agree to "anything"

BPS PRIVACY LAW (over)SIMPLIFIED

NOTICE > COLLECTION > USE/DISCLOSURE

Give **Notice** when collecting personal information

Specify the information, purposes, contact person

Collect only personal information **needed to do the job**

(this is much, much narrower than just consent)

Use or Disclose personal information for the purposes for which it was collected – according to the notice

M/FIPPA works this way, regulates Ontario BPS

HOW (NOT) TO COLLECT PERSONAL INFORMATION



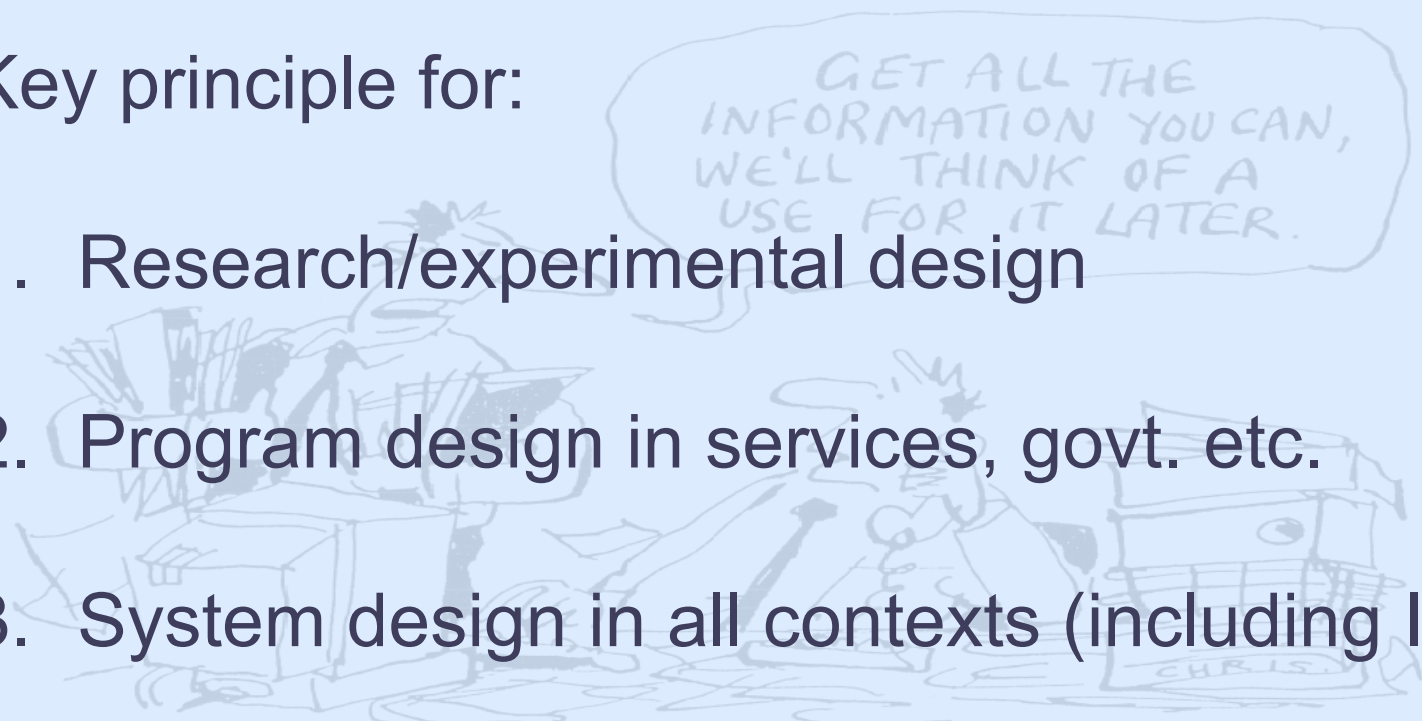
HOW (NOT) TO DO ANYTHING



MORE THAN A PRIVACY PRINCIPLE

Key principle for:

1. Research/experimental design
2. Program design in services, govt. etc.
3. System design in all contexts (including IT)
4. All planned activities / work tasks



GET ALL THE
INFORMATION YOU CAN,
WE'LL THINK OF A
USE FOR IT LATER.

U of T NOTICE of COLLECTION

The University of Toronto respects your privacy. Personal information that you provide to the University is collected pursuant to section 2(14) of the University of Toronto Act, 1971.

It is collected for the purpose of administering admissions, registration, academic programs, university-related student activities, activities of student societies, financial assistance and awards, graduation and university advancement, and reporting to government.

At all times it will be protected in accordance with the *Freedom of Information and Protection of Privacy Act*. If you have questions, please refer to www.utoronto.ca/privacy or contact the University Freedom of Information and Protection of Privacy Coordinator at 416-946-7303, McMurich Building, room 201, 12 Queen's Park Crescent West, Toronto, ON, M5S 1A8.

FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY OFFICE

Rafael Eskenazi – FIPP Director

Tel: (416) 946-5835

E-Mail: rafael.eskenazi@utoronto.ca

University of Toronto FIPP Office

McMurrich Building, Room 104

12 Queen's Park Crescent West

Toronto, ON M5S 1A8

Fax: (416) 978-6657