CMPUT 626 - Fall 2024
Module 4: Legal Privacy

Thursdays 11am - 1:50pm

Prof: Bailey Kacsmar

UNIVERSITY OF ALBERTA

Data Exploitation

Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach

Whistleblower describes how firm linked to former Trump adviser Steve Bannon compiled user data to target American voters

- 'I made Steve Bannon's psychological warfare tool': meet the data war whistleblower
- Mark Zuckerberg breaks silence on Cambridge Analytica

▲ Cambridge Analytica whistleblower: 'We spent $1m harvesting millions of Facebook profiles' – video

The Guardian March 2018

The New York Times

AT&T Said to Expose iPad Users' Addresses

By Miguel Helft

June 9, 2010

A group of hackers said Wednesday that it had obtained the e-mail addresses of 114,000 owners of 3G Apple iPads, including those of military personnel, business executives and public figures, by exploiting a security hole on AT&T's Web site.

The New York Times June 2010

Technology to Manipulate People and Decisions

Facebook apologises for psychological experiments on users

The second most powerful executive at the company, Sheryl Sandberg, says experiments were 'poorly communicated'

▲ Facebook's Sheryl Sandberg apologises for poor communication over psychological experiments. Photograph: Money Sharma/EPA Photograph: MONEY SHARMA/EPA

Facebook's second most powerful executive, Sheryl Sandberg, has apologised for the conduct of secret psychological tests on nearly 700,000 users in 2012, which prompted outrage from users and experts alike.

Tech policy / AI Ethics

AI is sending people to jail —and getting it wrong

Using historical data to train risk assessment tools could mean that machines are copying the mistakes of the past.

by **Karen Hao** January 21, 2019

AI might not seem to have a huge personal impact if your most frequent brush with machine-learning algorithms is through Facebook's news feed or Google's search rankings. But at the Data for Black Lives conference last weekend, technologists, legal experts, and community activists snapped things into perspective with a discussion of America's criminal justice system. There, an algorithm can determine the trajectory of your life.

MIT Tech Review January 2019

Privacy and Surveillance

Your Roomba May Be Mapping Your Home, Collecting Data That Could Be Shared

The Roomba 980 from iRobot, which was released in 2015. Some of the company's robotic vacuums collect spatial data to map users' homes. iRobot, via Reuters

By Maggie Astor

July 25, 2017

Your Roomba may be vacuuming up more than you think.

High-end models of Roomba, iRobot's robotic vacuum, collect data as they clean, identifying the locations of your walls and furniture. This helps them avoid crashing into your couch, but it also creates a map of your home that iRobot could share with Amazon, Apple or Google.

The New York Times July 2017

Technology

Doorbell-camera firm Ring has partnered with 400 police forces, extending surveillance concerns

A Ring Pro video doorbell. (James Pace-Cornsilk)

By Drew Harwell

August 28, 2019 at 6:53 p.m. EDT

The Washington Post August 2019

Hackers can hijack Wi-Fi Hello Barbie to spy on your children

Security researcher warns hackers could steal personal information and turn the microphone of the doll into a surveillance device

▲ Hello Barbie listens to children and uses cloud-based voice recognition technology to understand them and talk back. Photograph: Mattel

Mattel's latest Wi-Fi enabled Barbie doll can easily be hacked to turn it into a surveillance device for spying on children and listening into conversations without the owner's knowledge.

The Guardian November 2015
(see Valerie Steeves work as well)

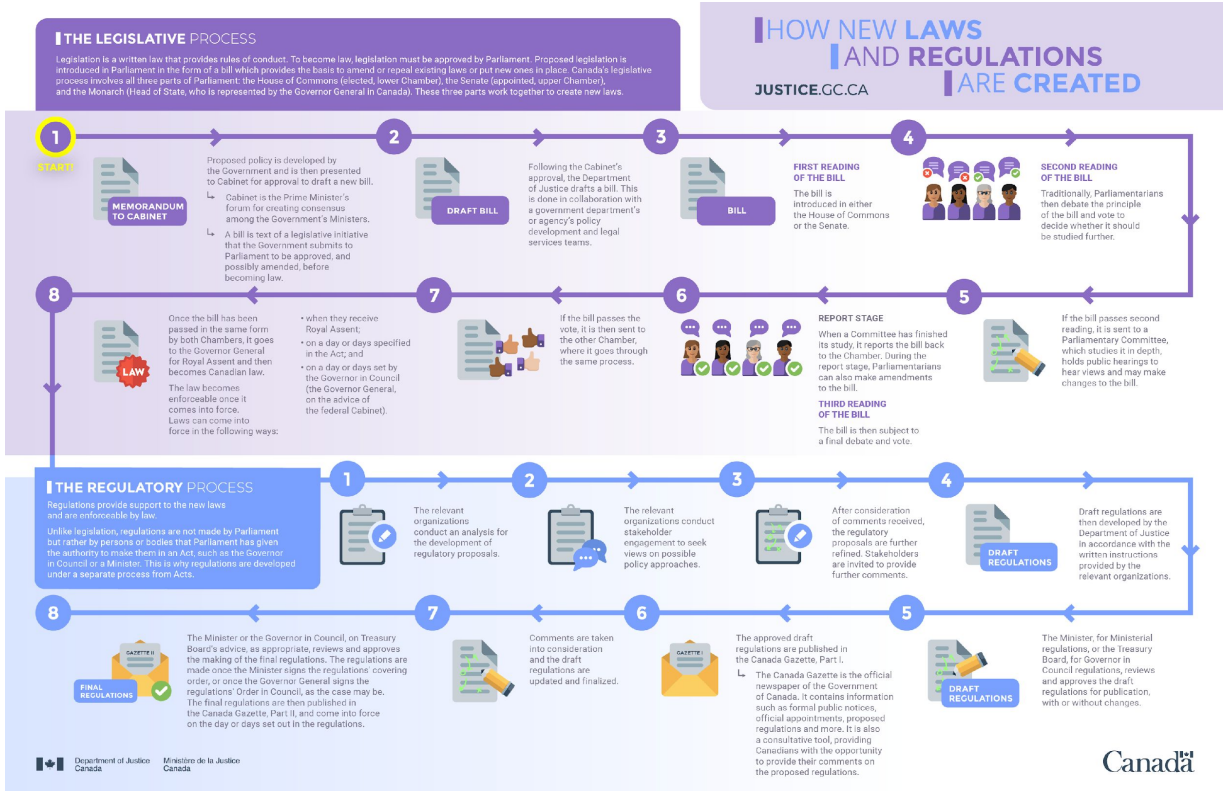
The Jurassic Problem

False Equivalence: Ethics and Law

PIPEDA

HIPAA
Health Insurance Portability and Accountability Act

A Practical Problem of Technology Law



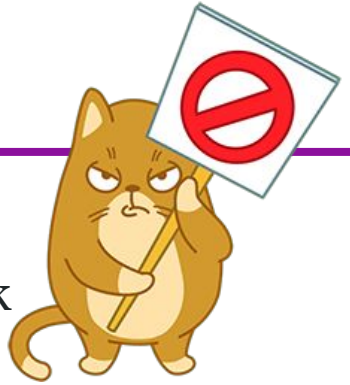
Newer (?) Laws

- California Consumer Protection Act 2018
- California Privacy Rights Act
  - 2020 approval, 2023 into effect
- Canada: Bill C-27, the Digital Charter Implementation Act
  - Recall, PIPEDA, implemented in 2001, 2002, 2004
  - As of 2018, several provinces have similar privacy laws
  - Parliament, 1st session November 22, 2021,
  - Passed second round April 24, 2023
  - Passed first round in June 16, 2022
  - Includes Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act, and the Artificial Intelligence and Data Act.

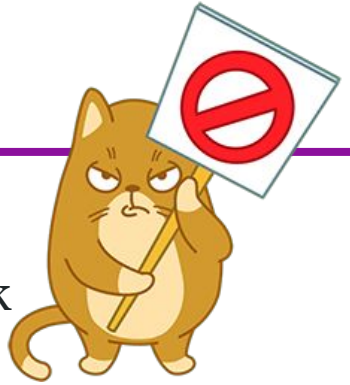
What about Ethics?

Ethics != Law

Ethics != A subjective expression of what you think

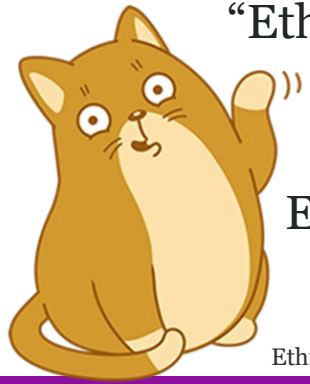


What about Ethics?



Ethics != Law

Ethics != A subjective expression of what you think



"Ethics" is about solving shared practical problems by building consensus through rigorous, logical argument.

Ethical theories aim to make a range of prescriptions, justified on certain grounds.

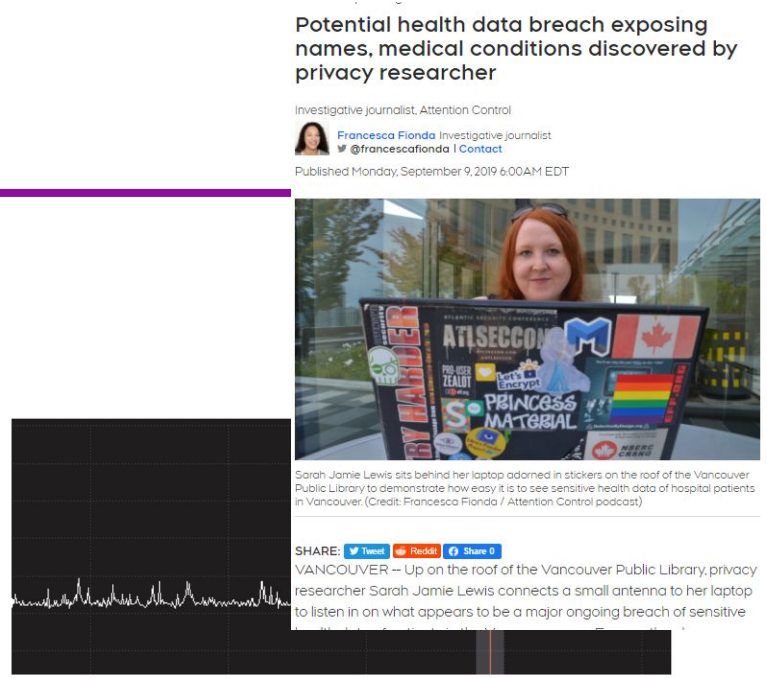
Ethical Theory Grid and Description: Steve Robinson, Brandon University

APPLYING ETHICS

When Wittgenstein challenged Popper to state an example of a moral rule, Popper claimed to have replied "Not to threaten visiting lecturers with hot pokers”

Responsible Disclosure

- When finding a vulnerability, what should you do?
- The idea of responsible disclosure is you inform those responsible so they have an opportunity to fix it first.



Potential health data breach exposing names, medical conditions discovered by privacy researcher

Investigative journalist, Attention Control

Francesca Fionda Investigative journalist
@francescafionda | Contact

Published Monday, September 9, 2019 6:00AM EDT

Sarah Jamie Lewis sits behind her laptop adorned in stickers on the roof of the Vancouver Public Library to demonstrate how easy it is to see sensitive health data of hospital patients in Vancouver. (Credit: Francesca Fionda / Attention Control podcast)

SHARE: Tweet Reddit Share 0

VANCOUVER -- Up on the roof of the Vancouver Public Library, privacy researcher Sarah Jamie Lewis connects a small antenna to her laptop to listen in on what appears to be a major ongoing breach of sensitive

Press Release: Open Privacy discovers unencrypted patient medical information broadcast across Vancouver

09 Sep 2019

Vancouver, BC - The Open Privacy Research Society has discovered that the sensitive medical information of patients being admitted to certain hospitals across the Greater Vancouver Area is being broadcast, unencrypted, by hospital paging systems, and that these broadcasts are trivially interceptable by anyone in the Greater Vancouver Area.

https://openprivacy.ca/blog/2019/09/09/open-privacy-discovers-vancouver-patient-medical-data-breach/

Trying to Build – Perspectives

- Get as many dissenting voices as possible.
- Explain how something works, what is possible to go wrong, and how bad actors can take advantage to a non-expert.
- The privacy and data protection norms and cultural values vary by region and country.
- Consult other types of experts
  (e.g. ethics, regions, advocates, activists)

@worldwise001, @ussjoin,@dinodaizovi, @wbm312, @limufar

Trying to Build – Questions

Not as intended…

As intended…

- Failure modes?
- Abuse cases?
- Who does this effect?
- Who could it effect?
- Did this need to be collected?
- Edge cases?

- Who does this effect?
- Who could it effect?
- Did this need to be collected?
- Edge cases?

@worldwise001, @ussjoin,@dinodaizovi, @wbm312, @limufar

Questioning Hello Barbie

Hackers can hijack Wi-Fi Hello Barbie to spy on your children

Security researcher warns hackers could steal personal information and turn the microphone of the doll into a surveillance device

▲ Hello Barbie listens to children and uses cloud-based voice recognition technology to understand them and talk back. Photograph: Mattel

Mattel's latest Wi-Fi enabled Barbie doll can easily be hacked to turn it into a surveillance device for spying on children and listening into conversations without the owner's knowledge.

The doll uses voice recognition software to 'listen' to the child and 'talk back'.

Children's voices are then recorded and sent to the cloud where they are analyzed

It also connects to Wi-Fi.

For more on this and things like it see Valerie Steeves work

Questioning Hello Barbie

1. Consider the effects of this toy when working correctly?
2. Incorrectly

Write out some questions you would want answered before this toy was built.

Hackers can hijack Wi-Fi Hello Barbie to spy on your children

Security researcher warns hackers could steal personal information and turn the microphone of the doll into a surveillance device

▲ Hello Barbie listens to children and uses cloud-based voice recognition technology to understand them and talk back. Photograph: Mattel

Mattel's latest Wi-Fi enabled Barbie doll can easily be hacked to turn it into a surveillance device for spying on children and listening into conversations without the owner's knowledge.

The doll uses voice recognition software to 'listen' to the child and 'talk back'.

Children's voices are then recorded and sent to the cloud where they are analyzed

It also connects to Wi-Fi.

For more on this and things like it see Valerie Steeves work

Questioning Hello Barbie – When it works

- Non-transparent to parents (and children)
- Children are the intended ‘users’
- Can it reproduce discriminatory patterns?
- Does this incorporate stereotypical performance?
- Is recording the children’s voices necessary?
- What are the risks of the Wi-Fi connection?
- Can parents access Barbie’s responses for their own review?

Hackers can hijack Wi-Fi Hello Barbie to spy on your children

Security researcher warns hackers could steal personal information and turn the microphone of the doll into a surveillance device

Hello Barbie listens to children and uses cloud-based voice recognition technology to understand them and talk back. Photograph: Mattel

Mattel's latest Wi-Fi enabled Barbie doll can easily be hacked to turn it into a surveillance device for spying on children and listening into conversations without the owner's knowledge.

For more on this and things like it see Valerie Steeves work

Questioning Hello Barbie – When it goes wrong

- Can recordings of children's voices be accessed on the server?
- Can recordings be connected to children or real locations?
- What security measures are in place to prevent malicious access to the toys sensors (microphone, speaker)?


Hackers can hijack Wi-Fi Hello Barbie to spy on your children

Security researcher warns hackers could steal personal information and turn the microphone of the doll into a surveillance device

▲ Hello Barbie listens to children and uses cloud-based voice recognition technology to understand them and talk back. Photograph: Mattel

Mattel's latest Wi-Fi enabled Barbie doll can easily be hacked to turn it into a surveillance device for spying on children and listening into conversations without the owner's knowledge.

For more on this and things like it see Valerie Steeves work

Task: The Law and Hello Barbie

For *Hello Barbie* (or other kids technology/toy), identify :

- At least one country/jurisdiction where you think the technology/toy **is compliant** with the regulations/law
- At least one country/jurisdiction where you think the technology/toy **is not compliant** with the regulations/law
- A list (subset) of attributes that correspond to whether or not any technology (wherther for kids or not) is likely to be compliant (or not)
-

Takeaways

- You need differing perspectives. Different expertise, but also different cultures, backgrounds, and experiences
- The intricacies and pressures of an ethical dilemma is hard when it is not theoretical anymore
- We should always consider whether we “should”, regardless of our field