

# CMPUT 626 - A2

## Machine Learning and Practical Privacy

---

Law, Ethics, and Policy

# Admin Stuff

---

Main schedule is up on eClass

If you want to request to be able to do a third paper, let me know by Monday.

After add/drop day I will schedule any remaining slots with those interested in speaking more.

# Why this session?

---

- Course content includes attacks
- Attacks can have societal impact and individual impact
- Your future work, research, industry, start-up, software, security...



# 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 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'



**The Guardian June 2014**

▲ 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

Technology

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



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

**The Washington Post August 2019**

By Drew Harwell

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

**The New York Times July 2017**

**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



# What are the effects of your actions... your code?

---

- It's not just on the humanities..
- Tech ethics as a field is increasing because what you build matters.

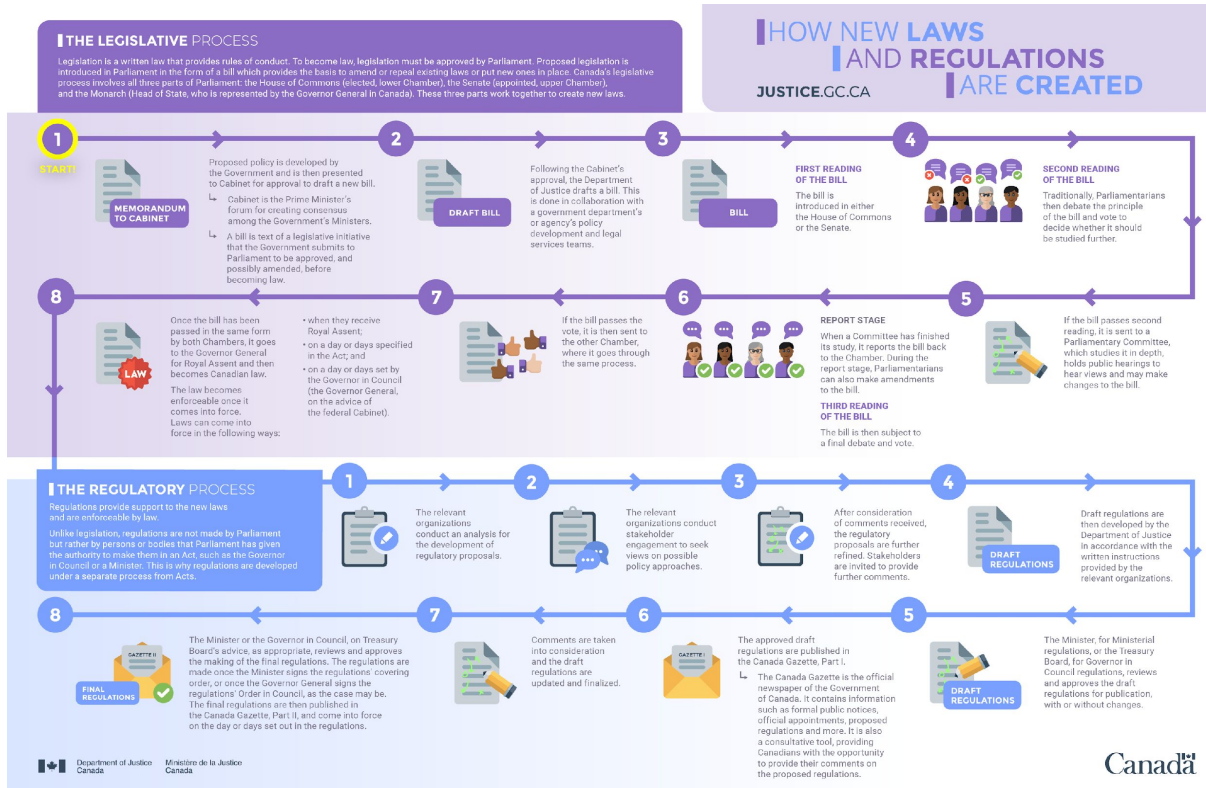




# False Equivalence: Ethics and Law



# 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.

# Learning Outcomes

---

- 1) Recognize ethical issues in computer science (and security/privacy specifically)
- 2) Assess technology for ethical implications with consideration to multiple perspectives and social consequences.

# The Remainder of this Session...

---

- Professional societies and codes of ethics
- What is ethics?
- What can ethics say about technology?
- Some practical advice and actions

# Ethics and Professional Societies


---

- As a computer (security) professional you will be expected to uphold certain ethical standards
- Association for Computing Machinery (ACM)
- Institute of Electrical and Electronics Engineers (IEEE)
- Canadian Information Processing Society (CIPS)



# Overview of CIPS' Code of Ethics:

---

- Protect Public Interest and Maintain Integrity
- Demonstrate Competence and Quality of Service
- Maintain Confidential Information and Privacy
- Avoid Conflicts of Interest
- Uphold Responsibility to the  CIPS profession

# WHAT IS ETHICS?

---

Using Ethical Theory Grid and Description: Steve Robinson, Brandon University



# What is Ethics?

---

Ethics != Law

Ethics != A subjective expression of what you think

---



# What is Ethics?

---

Ethics != Law

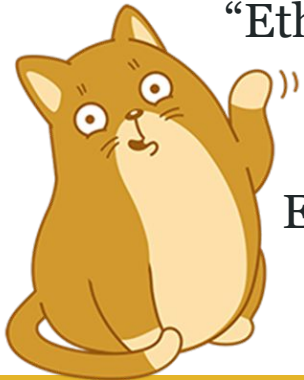
Ethics != A subjective expression of what you think

---



“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 Prescriptions

---

## Consequentialism

John  
Stuart  
Mill

“Be happy,  
and make  
others  
happy...”

## Deontology

Immanuel  
Kant

“Respect others’  
rights and  
legitimate  
demands...”

## Virtue Ethics

Aristotle

“Be the most  
fully human  
person  
you can be...”

# Ethical Theory Grounds

---

**Naturalistic**



“...because it’s human nature to behave that way.”

**Rationalistic**



“...because common sense demands it.”

**Pragmatic**



“...because that’s how we do things ’round here.”

# Ethical Theories

	Consequentialism	Deontology	Virtue Ethics
Naturalistic	John Stuart Mill		Aristotle
Rationalistic		Immanuel Kant	
Pragmatic			

# What can theories say about tech actions? Pick A.

## Consequentialism

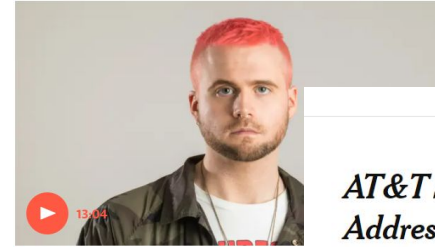
The culture we share commits us all to the promotion of individual desire satisfaction: all of our institutions push us in this direction; it's the only way to make sense of our actual lives. (Other cultures may differ.)

Pragmatic

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 I

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.

# What can theories say about tech actions? Pick B.

## Consequentialism

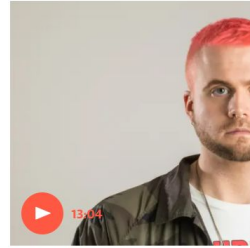
You are most fully and completely human when you are working to maximize the happiness of all people.

Naturalistic

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 m

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.

# What can theories say about tech actions? Pick C.

## Deontologism

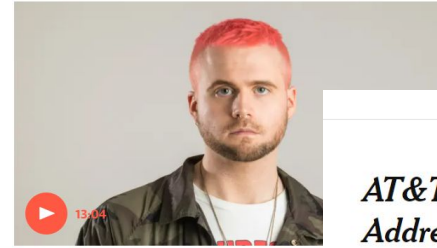
If what I seek is my own fulfillment in life, then it is necessarily the case that I will succeed better by working with others rather than against them; respecting human rights and human dignity will always make me better off than I would otherwise be.

Rationalistic

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 Faceb

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.



# 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 poker"*

# 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 Fiorida](#) Investigative Journalist  
[@francescafiorida](#) | [Contact](#)

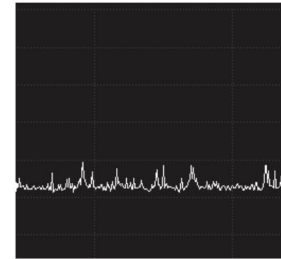
Published Monday, September 9, 2019 6:00AM EDT



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 Fiorida / Attention Control podcast)

SHARE: [Twitter](#) [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.

# Trying to Build Ethically – 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)



# Trying to Build Ethically – Question

---

**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?

# 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.**

## 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

# 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.



▲ 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.**

# 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.

# 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 offers to chat on and even 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.





# Trying to Build Ethically – Refusal

---

- You do not have to contribute your labor to work which serves to oppress
- You may face pressure for your job security/promotion or financial stability
- There are no cookies for making the right ethical decision
- Labor or work is not disassociated from the effects it has and harms it creates
- It is still not easy

# Making Ethical Decisions is Hard

## Technology

### Google hired Timnit Gebru to be an outspoken critic of unethical AI. Then she was fired for it.

Gebru is one of the most high-profile Black women in her field and a powerful voice in the new field of ethical AI, which seeks to identify issues around bias, fairness, and responsibility.



Google AI research scientist Timnit Gebru speaks on Sept. 7, 2018, at TechCrunch Disrupt SF 2018 at the Moscone Center in San Francisco. (Kimberly White/Getty Images/TechCrunch)

### Hootsuite Drops ICE Contract After Employee Backlash



Rachel Sandier Forbes Staff  
Business  
I cover breaking news.

Updated Sep 24, 2020, 04:44pm EDT

**TOPLINE** Social media company Hootsuite said Thursday it will no longer do business with U.S. immigration authorities after an employee tweeted that the Vancouver-based firm signed a contract with U.S. Immigrations and Customs Enforcement this week, despite internal protests.



### The controversy behind a star Google AI researcher's departure

Timnit Gebru says she was pushed out of the company; now some are worried it will have a chilling effect on academics in tech.

By Shirin Ghaffary | Updated Dec 9, 2020, 6:30pm EST

## TECHNOLOGY

### Employees of Microsoft's GitHub demand company cancel its contract with ICE



People protest migrant detention at the Otay Mesa Detention Center in San Diego in July 2018. (Etienne Laurent / EPA/Shutterstock)

By JOHANA BHUIYAN | STAFF WRITER  
OCT. 9, 2019 3:31 PM PT



# 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



