Privacy and Surveillance
Cambridge Analytica: how 50m Facebook records were hijacked

1. Approx. 320,000 US voters (‘seeders’) were paid $2-5 to take a detailed personality/political test that required them to log in with their Facebook account...

2. The app also collected data such as likes and personal information from the test-taker’s Facebook account...

3. The personality quiz results were paired with their Facebook data - such as likes - to seek out psychological patterns.

4. Algorithms combined the data with other sources such as voter records to create a superior set of records (initially 2m people in 11 key states*), with hundreds of data points per person.

AI Surveillance

- Why we should worry about this now?
  - Big Data + Neural Networks + GPUs

- Who is supplying this technology?
  - China: Major driver in AI surveillance
    - e.g. Huawei serves at least fifty countries worldwide
  - The US: IBM, Palantir, Cisco
San Francisco Bans Facial Recognition Technology

Somerville Bans Government Use Of Facial Recognition Tech

June 28, 2019 By Katie Lannan, State House News Service
“For three years now, South Wales Police has been using it against hundreds of thousands of us, without our consent and often without our knowledge.”

“We should all be able to use our public spaces without being subjected to oppressive surveillance.”
"The question isn't whether you're undocumented — but rather whether a flawed algorithm thinks you look like someone who's undocumented."

Alvaro Bedoya, the founding director of Georgetown Law's Center on Privacy & Technology.

In 2017, Palantir software allowed ICE to launch an operation that targeted and arrested family members of children who crossed the border, leading to 443 arrests.

Ethical Issues: deporting migrants, refugees, and asylum seekers, separating families, keeping children in detention...

*ICE: Immigration and Customs Enforcement
“the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.”

- Alan Westin
Privacy Definitions

- someone's right to **keep** their personal matters and relationships secret
  - Controlling personal information disclosure and processing
  - e.g., laws to protect people’s privacy

- the state of **being alone**
  - Controlling access to self
  - “Right to be let alone”
Controlling Personal Information Disclosure
Controlling Access to Self

Click here to turn your own camera on or off
Privacy and human behavior in the age of information

Alessandro Acquisti, Laura Brandimarte, George Loewenstein

This Review summarizes and draws connections between diverse streams of empirical research on privacy behavior. We use three themes to connect insights from social and behavioral sciences: people's uncertainty about the consequences of privacy-related behaviors and their own preferences over those consequences; the context-dependence of people's concern, or lack thereof, about privacy; and the degree to which privacy concerns are malleable—manipulable by commercial and governmental interests. Organizing our discussion by these themes, we offer observations concerning the role of public policy in the protection of privacy in the information age.
Uncertainty

- Privacy uncertainty arises from **incomplete** and **asymmetric** information.
  - Data collection and data processing is often invisible.
  - People are uncertain about how much information to share.

- People are uncertain about their **privacy preferences**.
  - This leads to **privacy paradox**.
Context-dependence

- Depending on **time** and **place**, Westin categorizes people into three groups: pragmatists, fundamentalists, or unconcerned.
- Difficult to decide on **boundaries**.
- We are **influenced** by our culture and the behaviour of other people.
- Privacy concerns are also a function of **past experiences** (e.g., intrusive tech).
Malleability and Influence

- Some entities exploit behavioral and psychological processes to promote disclosure.
- Default settings in applications are interpreted as implicit recommendations.
- Malicious interface designs confuse users into disclosing personal information (e.g., cookies).
- “62% of respondents to a survey believed (incorrectly) that the existence of a privacy policy implied that a site could not share their personal information without permission.”
An app may tell users that granting access to their location will help them get traffic information, but not mention that the data will be shared and sold. That disclosure is often buried in a vague privacy policy.
Disclosure behavior in online social media
Percentage of profiles publicly revealing information over time (2005-2011)

Default visibility settings in social media over time

- Shares birthday publicly on profile
- Shares high school publicly on profile
What we know so far?

- **Uncertainty and context-dependence**
  - People are unaware of the information they are sharing, unaware of how it can be used, uncertain about their privacy preferences.
- **Malleability** implies that people are influenced in what and how much they disclose.
- Social and behavioural empirical research suggests that people are vulnerable, and they behaviour may be altered by the ones holding the data (power imbalance).
- Privacy policies should protect real people (naïve, uncertain, vulnerable) who need assistance and protection.