Privacy and Surveillance

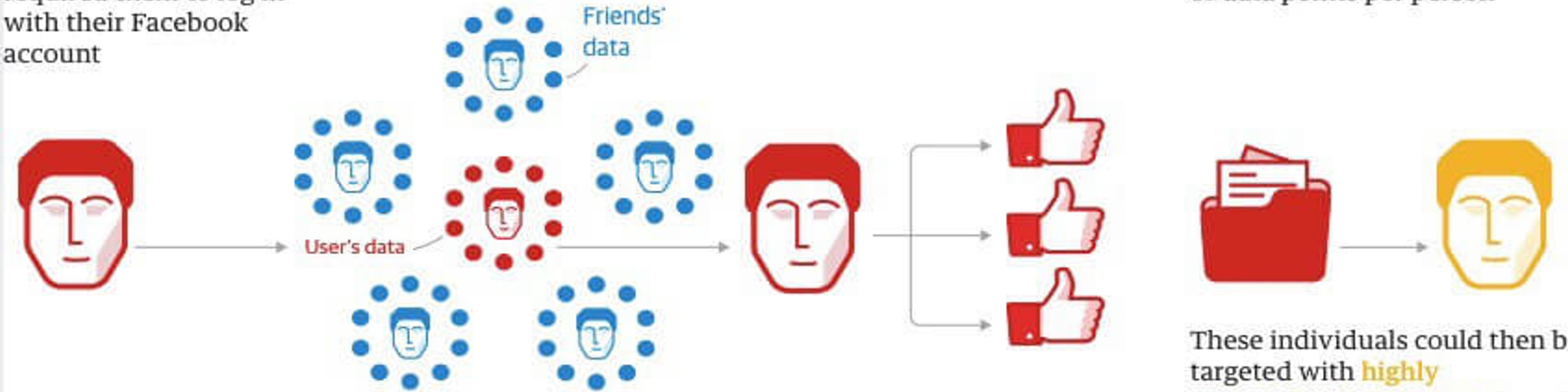
Cambridge Analytica: how 50m Facebook records were hijacked

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



... as well their **friends'** data, amounting to over 50m people's raw Facebook data

These individuals could then be targeted with **highly personalised advertising** based on their personality data

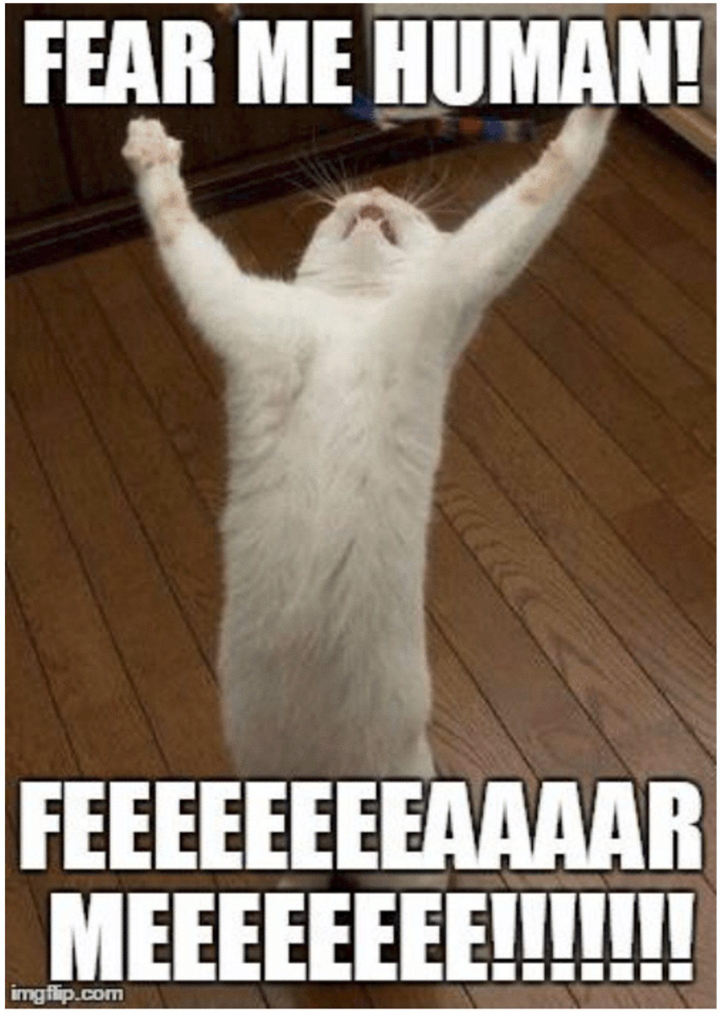
Guardian graphic. *Arkansas, Colorado, Florida, Iowa, Louisiana, Nevada, New Hampshire, North Carolina, Oregon, South Carolina, West Virginia

AI Surveillance

- Why we should worry about this now?

Big Data + Neural Networks + GPUs

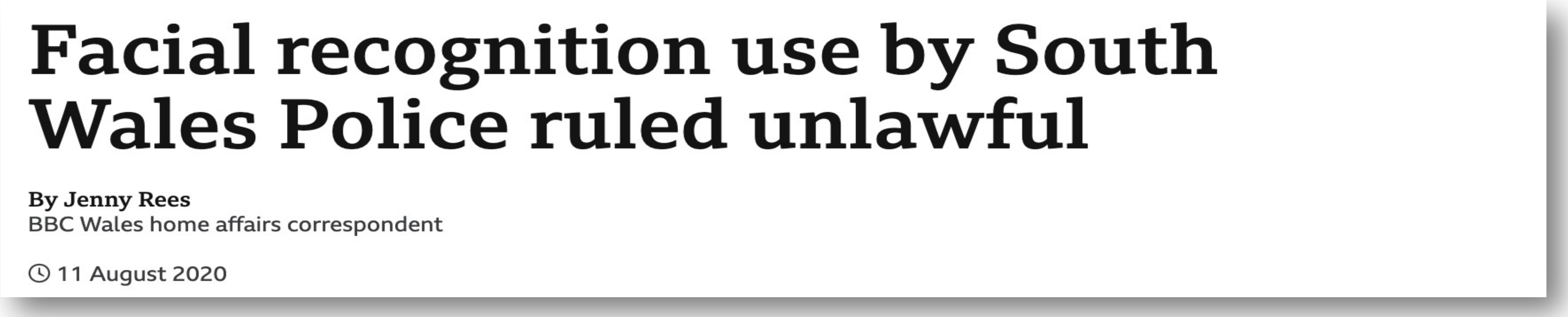
- Who is supplying this technology?
    - China: Major driver in AI surveillance e.g. Huawei serves at least fifty countries worldwide
    - The US: IBM, Palantir, Cisco



San Francisco Bans Facial Recognition Technology

Somerville Bans Government Use Of Facial Recognition Tech

June 28, 2019 | By Katie Lannan, State House News Service



Facial recognition use by South Wales Police ruled unlawful

By Jenny Rees
BBC Wales home affairs correspondent

🕓 11 August 2020

“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.”

https://www.bbc.co.uk/news/uk-wales-53734716

#disarmICE

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.

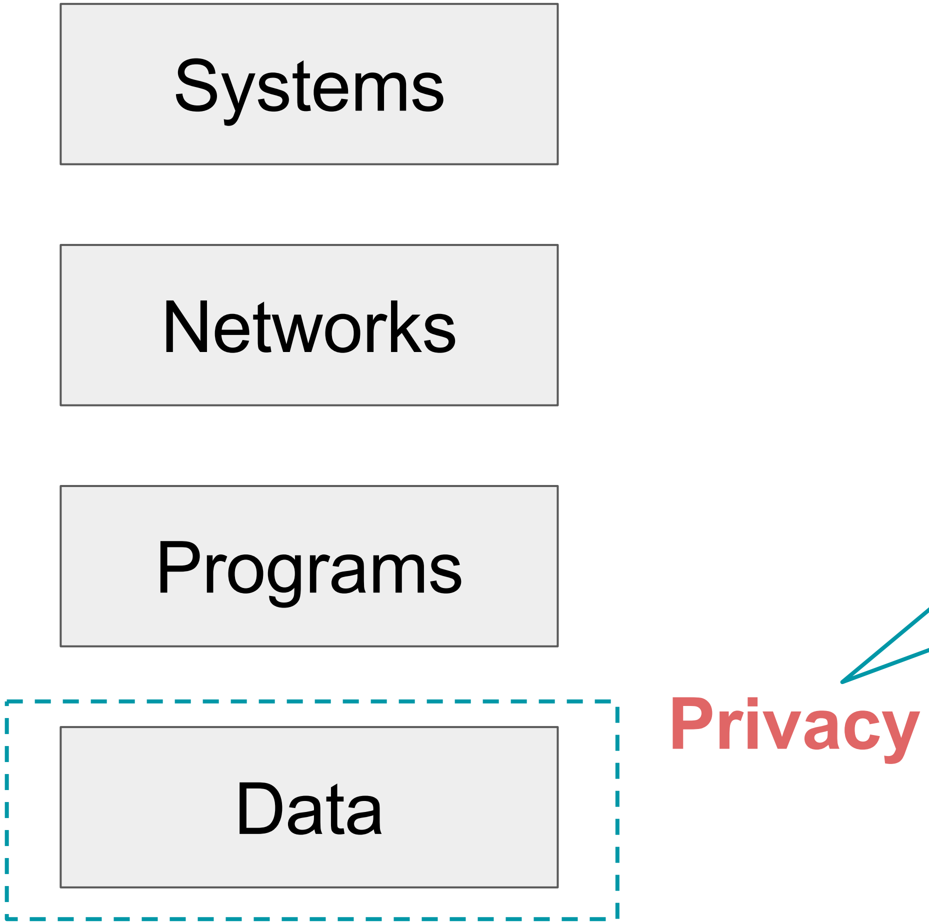
Ethical Issues: deporting migrants, refugees, and asylum seekers, separating families, keeping children in detention...

"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.

***ICE: Immigration and Customs Enforcement**

Cybersecurity



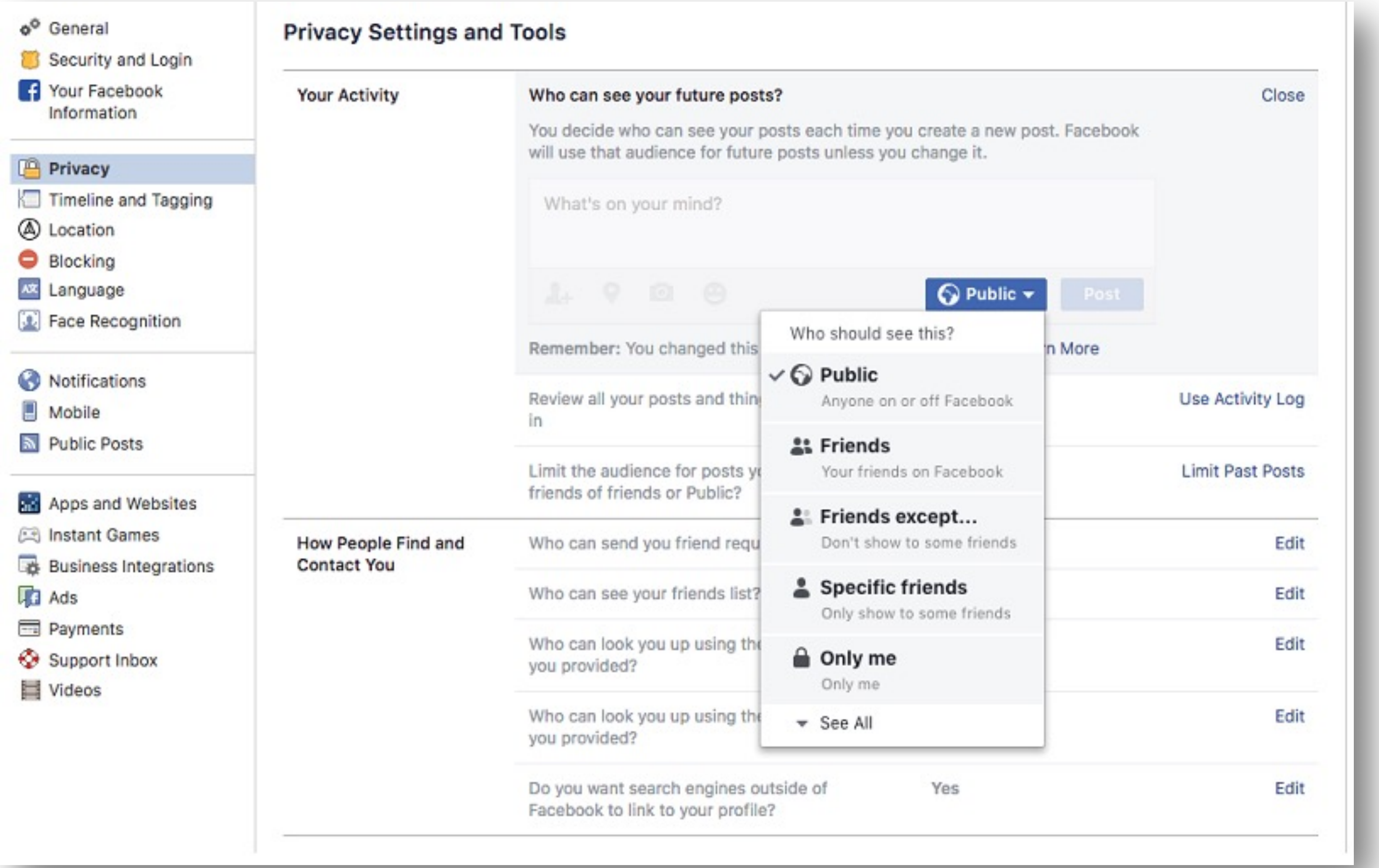
> “the claim of individuals, groups, or institutions to determine for themselves **when**, **how**, and to **what extent** information about them is communicated to others.” (...)
>
> - Alan Westin

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”

Cambridge Dictionary

Controlling Personal Information Disclosure



- General
- Security and Login
- Your Facebook Information
- **Privacy**
- Timeline and Tagging
- Location
- Blocking
- Language
- Face Recognition
- Notifications
- Mobile
- Public Posts
- Apps and Websites
- Instant Games
- Business Integrations
- Ads
- Payments
- Support Inbox
- Videos

Privacy Settings and Tools

Your Activity

Who can see your future posts? Close

You decide who can see your posts each time you create a new post. Facebook will use that audience for future posts unless you change it.

What's on your mind?

Public ▾ Post

Who should see this?

- ✓ **Public** Anyone on or off Facebook
- **Friends** Your friends on Facebook
- **Friends except...** Don't show to some friends
- **Specific friends** Only show to some friends
- **Only me** Only me
- ▾ See All

Remember: You changed this … n More

Review all your posts and thin… in — Use Activity Log

Limit the audience for posts y… friends of friends or Public? — Limit Past Posts

How People Find and Contact You

Who can send you friend requ… — Edit

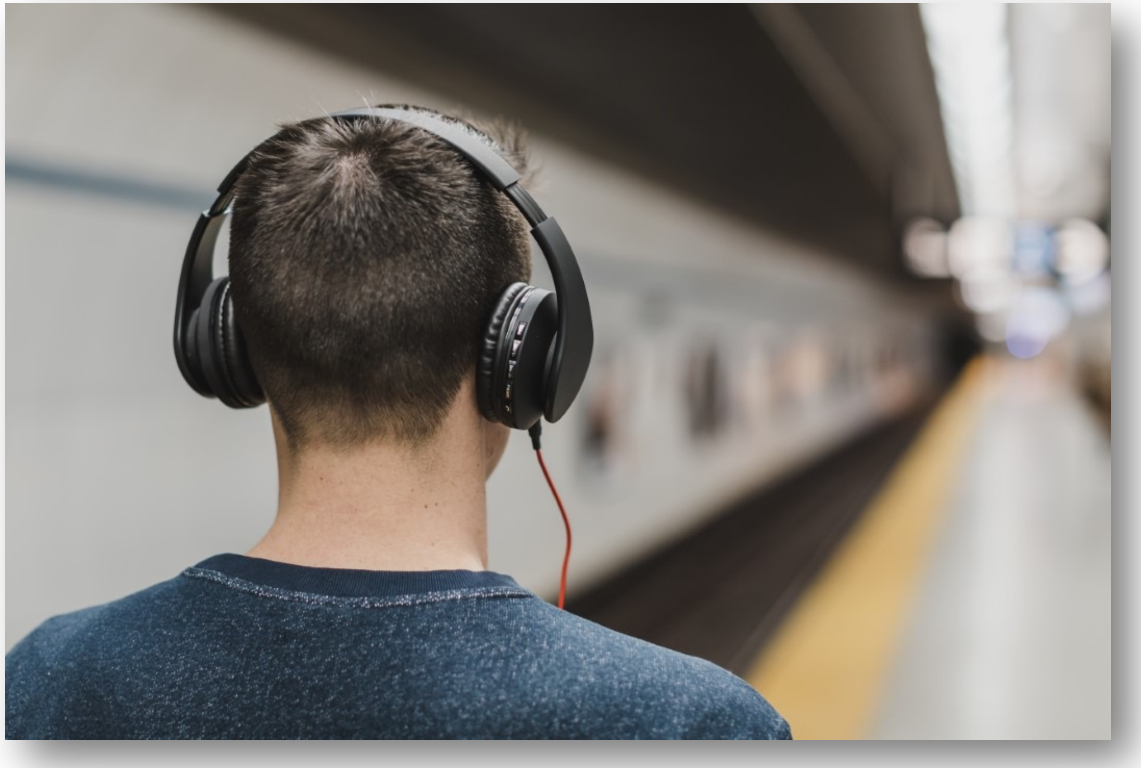
Who can see your friends list? — Edit

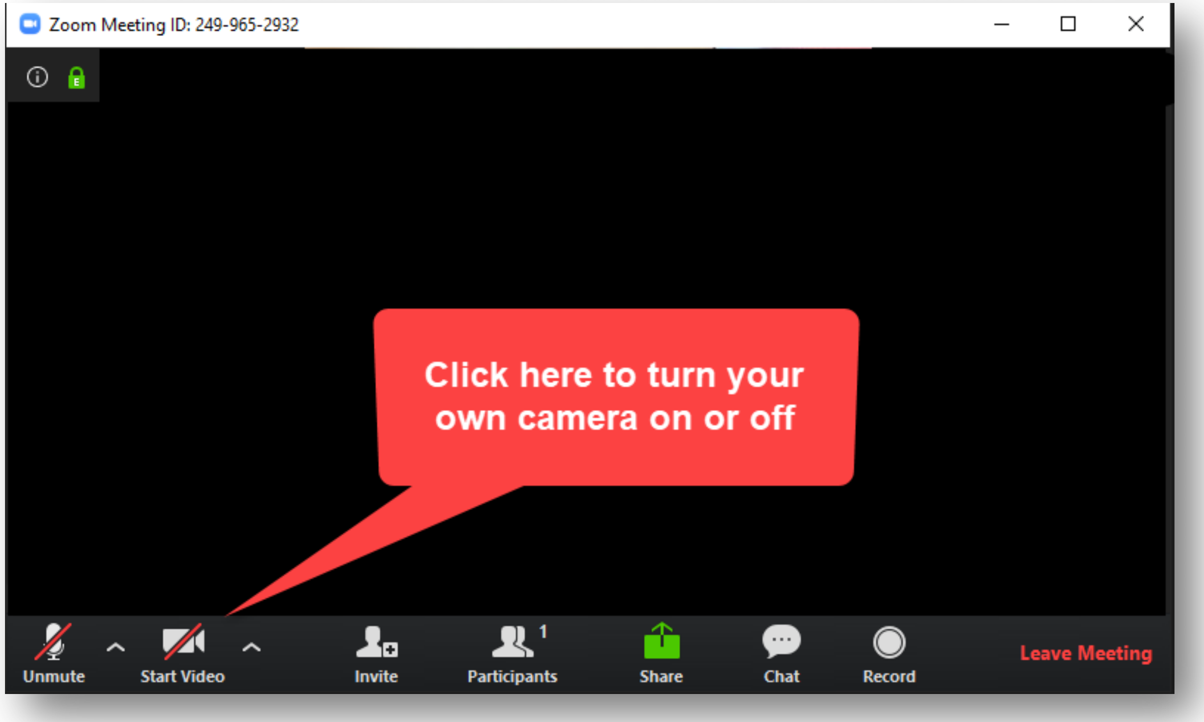
Who can look you up using th… you provided? — Edit

Who can look you up using th… you provided? — Edit

Do you want search engines outside of Facebook to link to your profile? — Yes — Edit

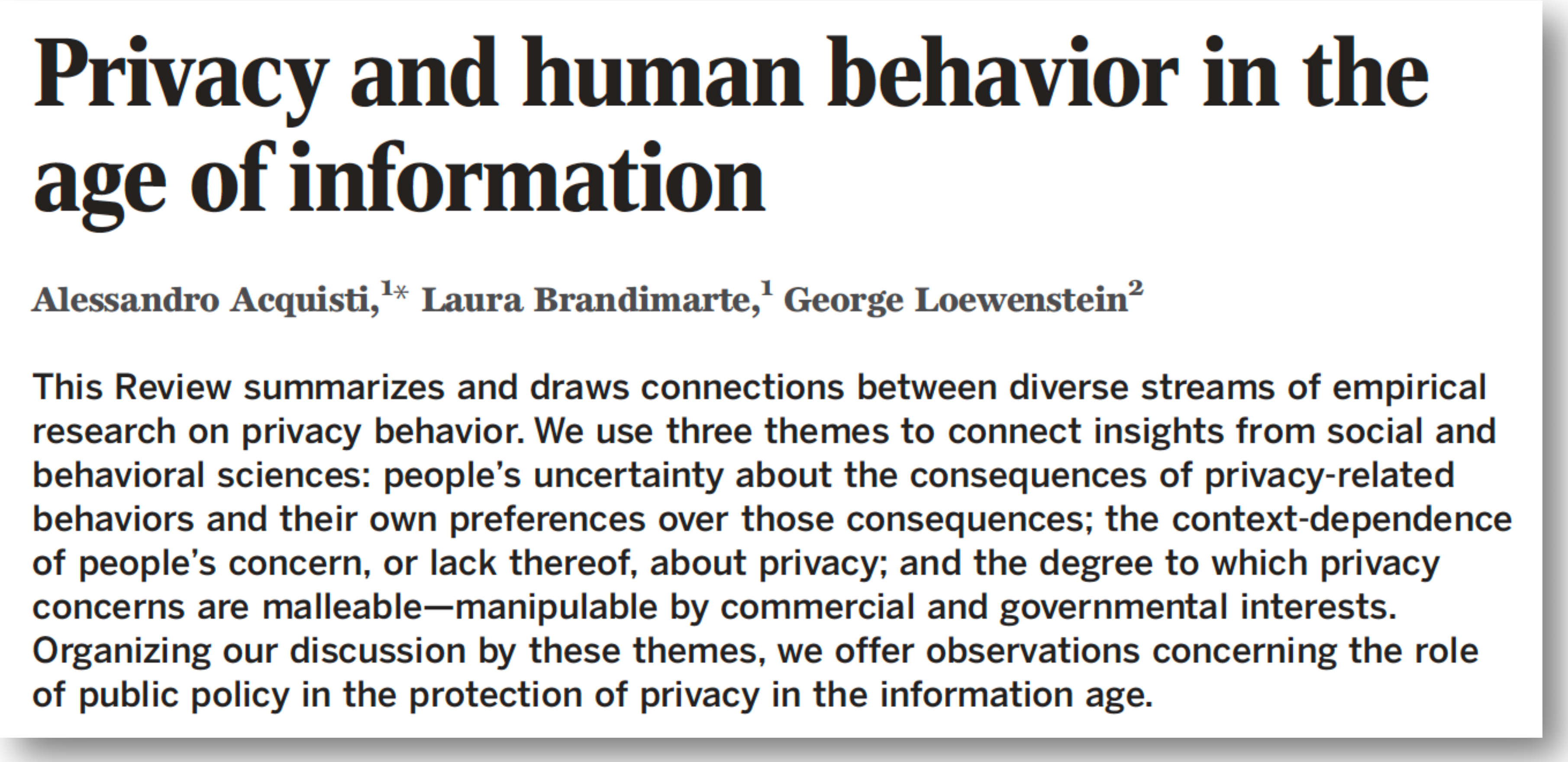
Controlling Access to Self





Zoom Meeting ID: 249-965-2932

Click here to turn your own camera on or off



Privacy and human behavior in the age of information

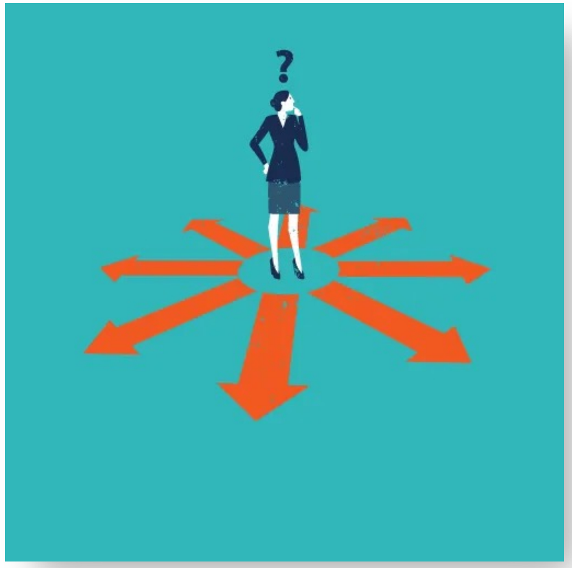
Alessandro Acquisti,[1*] Laura Brandimarte,[1] George Loewenstein[2]

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.

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509-514.

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.



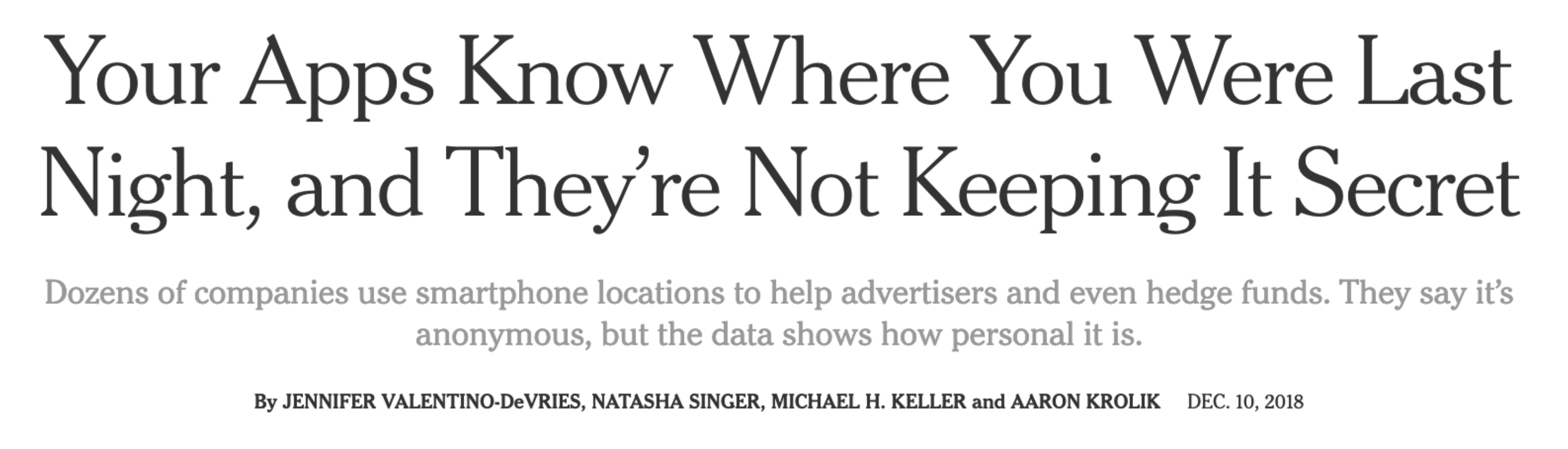
Context-dependence

- 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.”

Malleability and Influence



Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret

Dozens of companies use smartphone locations to help advertisers and even hedge funds. They say it's anonymous, but the data shows how personal it is.

By JENNIFER VALENTINO-DeVRIES, NATASHA SINGER, MICHAEL H. KELLER and AARON KROLIK DEC. 10, 2018

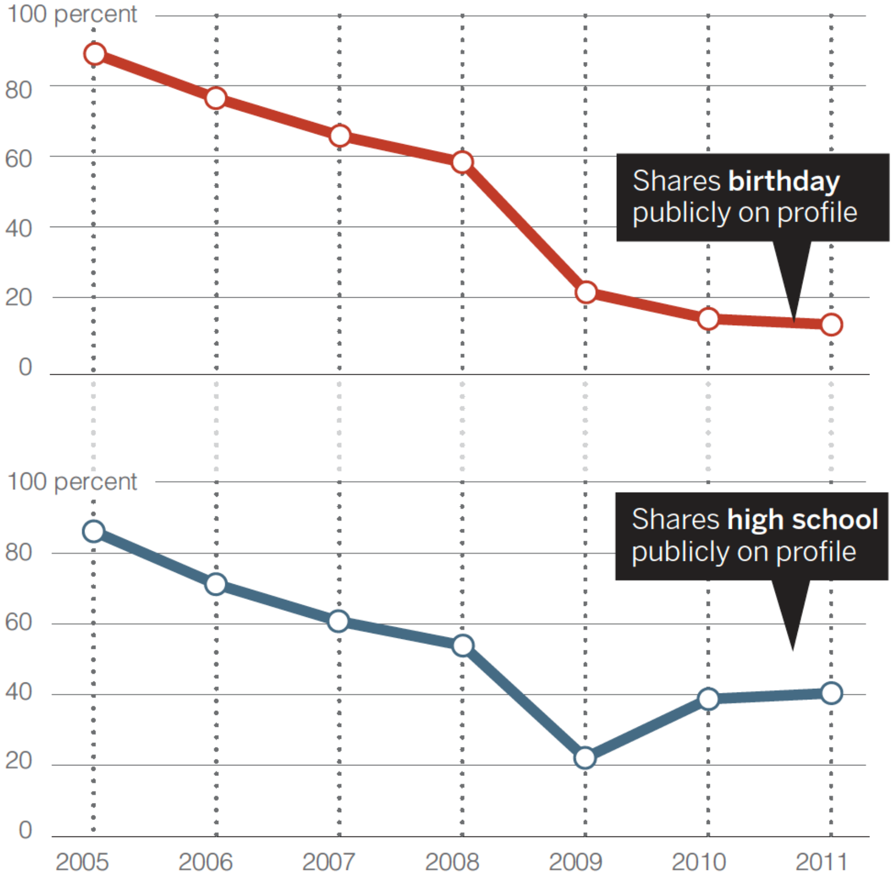
"An app may tell users that granting access to their location will help them get traffic information, but not mention that the data will be shared and sold. That disclosure is often buried in a vague privacy policy."

The Weather Channel

https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

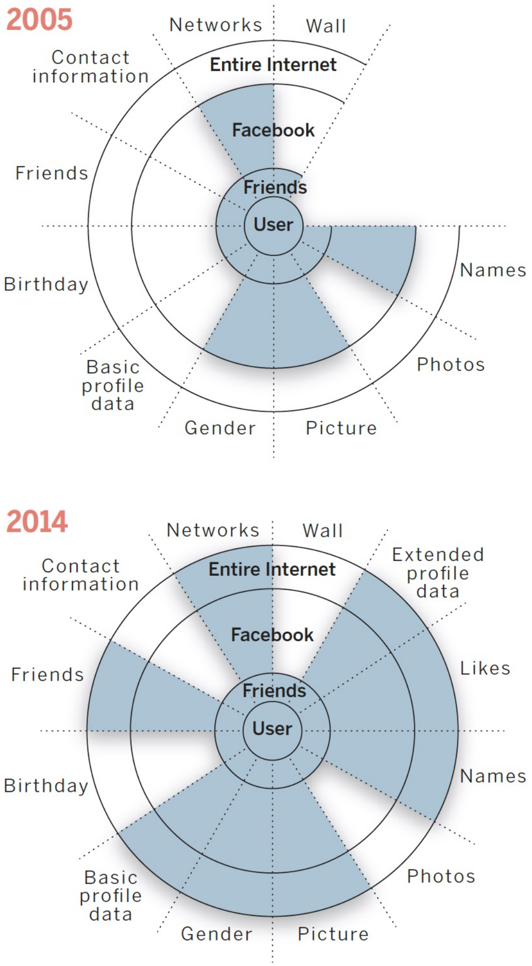
Disclosure behavior in online social media

Percentage of profiles publicly revealing information over time (2005-2011)



Default visibility settings in social media over time

▨ Visible (default setting) □ Not visible



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.