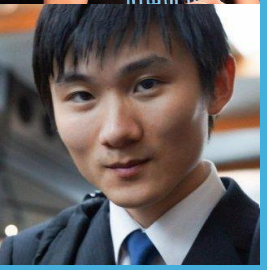
Data Privacy

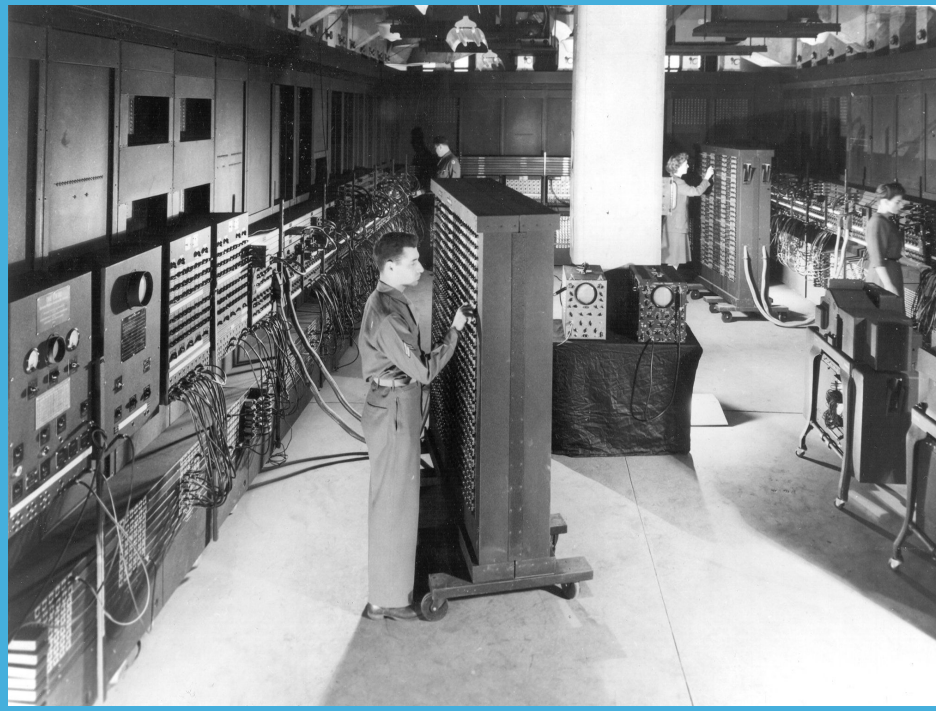
Science Policy Exchange
29 May 2018

Benjamin Tan
@ichthys101
Hardware Security

Ryan Kurte
@ryankurte
Internet-of-Things



Andrew Chen
@andrewtychen
Computer Vision



What is privacy?

A brief introduction

“When it comes to privacy and accountability, people always demand the former for themselves and the latter for everyone else.

- David Brin

Privacy

- Subjective:
  - Differing definitions and preferences
  - Non-binary: depends on use cases and contexts
  - “Ensuring that we *feel secure*”
  - Privacy is a response to imperfect trust
- Information Privacy vs Personal Privacy
- Our data, our thoughts, our feelings

By the way, data and information are not the same thing, but they are the same thing

New Zealand's Information Privacy Principles

- Only collect data
  - if it's necessary for a purpose
  - directly from the person
- When you're collecting data
  - Tell the person
  - Be lawful and fair

New Zealand's Information Privacy Principles

- When you're storing data
  - Keep data safe
  - Let people access data about them
  - Let people correct data about them
  - Delete data when you don't need it anymore

New Zealand's Information Privacy Principles

- When you're using data
  - Check data is accurate
  - Do not use data for secondary purposes
  - Do not release other people's data
  - Do not use unique identifiers (unless necessary)

New Zealand's Information Privacy Principles

- 12 information privacy principles... UNLESS
  - We need to prevent, detect, investigate, prosecute, or punish criminal offences
  - There's a threat to public health or safety
  - We need to protect "public revenue"
  - Data is anonymised for "statistical or research"
  - Information is already publicly available
  - A person waives their right / gives permission
  - ... and a bunch of other reasons in the Act

Privacy

- Privacy is not absolute
  - There are many reasons to step over privacy
- Often a secondary concern
  - Let’s do the thing, and protect privacy if we can
- Enforcement is relatively weak
  - If you breach someone’s privacy… so what?
  - NZ Law requires harm to be demonstrated
- Is it *actually* important?

Why does privacy matter?

- Public confidence to do things?
- Limit power imbalances?
- Maintaining social boundaries?
- Freedom of thought and speech?
- To allow for self-development?
- Society probably needs it to function

Threats to Privacy

Entering the digital age

What can threaten our privacy?

Data / Information can be in four states:

Collection

Collecting unnecessary data

Collecting false/wrong data

Storage

Insecure storage of data

Access by unauthorised individuals

Transmission

Interception of communication

Accidental disclosure of data

Use

Improper and secondary uses of data

Decisions based on false/wrong data

Combination of multiple data sources

Information Security

- Technologies are built with boundless optimism
- Opportunities for misuse by design are often overlooked
- Let alone opportunities if compromised

Information Security

- **Everything** is under attack
  - The internet is a hostile environment
  - If it's valuable, it's worth stealing or subverting
- *Every* service will fail
  - See Google, Facebook, Microsoft, Boeing, ...
  - If they can't do it, no-one else can
- How do we think about these risks

Information Security

Threat models

- Risks depend on personal situation
  - Threats might be opportunistic or targetted
- Difficult to conceptualise
  - Can individuals be expected to do this?
- Difficult to effect
  - Opt-out is naive and often not reasonable

Information Security

Trust Relationships

- Interpersonal trust is:
  - Multidimensional (trust with X, not with Y)
  - Temporal (changes over time)
  - Freely given and revoked
  - Based on person-to-person experience

We trust technologies like people

Information Security

- Information security is difficult
- The way we conceptualise risks and trust doesn’t work for most people
- And probably shouldn’t be required of most people
- Sometimes security vs. privacy tradeoffs

Hardware Security

- Research
  - Security *of* Hardware
  - Security *in* Hardware
- Context:
  - Distributed design teams
  - Globalised supply chains
- Physical attacks, probing, side-channels
- Software-based solutions?

Design Challenges

- Privacy is often not a primary concern
- Trade-offs, especially time-to-market
- Do something quickly, then worry about the potential that things go wrong later
- Research: design flows, methods, formalisation
  - Literature exists on research about things like access control, audit trails from the 80s...

Algorithmic Security

- Big Data + Machine Learning / AI
  - Speed: faster processing
  - Scale: more data can be processed
  - Scale: multiple sources can be combined
  - Transparency: developers call them ‘black boxes’
  - Vulnerabilities: exploitable by bad actors
- AI can exceed human performance, but can also fail in ways a human wouldn’t

Algorithmic Security

- AI enables new ways to extract data
  - Surveillance cameras can track people 24/7

The Internet of Things

- More data, all the time, everywhere
- Implications of data are not understood
  - Temperature and humidity
- All sorts of different devices and services
  - Different requirements, expectations, social contexts
- Consent is impossible

The Internet of Things

- What expectation of privacy do you have?
  - Does it include being observed all the time, wherever you are?
  - Do you understand this data is “anonymous” and thus not protected in any way?
  - And that the use / combination / analysis of this data is completely outside your control?
  - And also maybe outside the collectors control?

Everyone is bad at computers

So what can we do about it?

Protecting Privacy

How science and technology can help

Protecting Privacy

Two Pathways: The Good

By Regulation

Governments must pass laws that protect our privacy, and enforce them by punishing those that infringe upon the privacy rights of individuals

By Design

Technology developers must build privacy into their systems and products, so that it is impossible for privacy rights to be infringed

Protecting Privacy

Two Pathways: The Bad

By Regulation

Governments are slow. Very slow. Extremely slow.

Also, legislators often are not expert enough.

By Design

“Privacy-by-design is incompatible with capitalism”

There is little incentive for powerful system owners to pay for privacy protection

Protecting Privacy

- Can we encourage these two pathways to develop side-by-side?
- The literature says... maybe?!
  - A lot of theory has been written
    - Privacy-by-design (Cavoukian, Europe)
  - A lot of practical systems have been rekt
    - Facebook, Google, Equifax, Governments
- Can the two pathways be intertwined?

Protecting Privacy

- How can people inform these processes?
  - Influence regulation through democracy?
  - Influence design through... markets?
- Ultimately, who “controls” privacy?
  - The Surveillers vs The Surveilled
  - Who has the power to change protections?
- What role does science play?

Protecting Privacy

- Science influences:
  - Technological development of what is possible
  - Sociological study of populations and perception
  - Intersection of science and ethics
- Value-based judgements are hard to assess scientifically - hard to run an experiment
- The knowledge gap between technology and values is widening - different paces

Public Perceptions

- What drives perceptions of privacy?
- Global survey on surveillance cameras
- Based on 10 scenarios
  - Public vs Private owners
  - Recorded vs Non-recorded
  - Human-in-the-loop vs AI
  - Public safety vs Commercial data collection
  - Benefit to the surveilled vs to the system owners

Public Perceptions

- Demographics don’t matter
- Scenario context overrides principles
- Underlying factors:
  - Access
  - Human Influence
  - Anonymity
  - Data Use
  - Trust

Privacy Policy

The current situation

Privacy in New Zealand

- Privacy Act 1993
  - Is very old and outdated
- Privacy Bill in Parliament now
  - Select Committee submissions closed last week
  - Is slightly less old but still outdated [opinion]
- Office of the Privacy Commissioner
  - Is not that old and not outdated
  - But can only go as far as the legislation allows

Privacy Globally

- General Data Protection Regulation
  - The European Union Strikes Back - In Force May 25
  - Applies to European companies...
    and companies with European customers!
  - Day 1: Lawsuits against Google and Facebook filed
- Contagious Legislation
  - Policy experiments are risky
  - Once a jurisdiction has done it, others may copy
  - Privacy Commissioners share information

Challenges of Protecting Privacy

- Who even reads privacy statements?
- Does the “average person” understand privacy and the implications of privacy loss?
- Power imbalances - corporations and governments write the rules
- Where are the incentives to protect privacy?
- Can we deal with scale before it is too late?

Concluding Remarks

- Privacy is **subjective**, dependent on the application and context
- Yet we need common privacy rights for our **society** to be functional
- Our **expectations** of privacy change over time

- **Science** and technology *threatens* privacy, but can also *empower* privacy
- Privacy is **not easily quantitative**, so *evidence* is hard to gather
- **Studying Privacy** needs a combination of ethics and social sciences
- It is difficult - and irresponsible - to draw definitive conclusions from scientific experiments about privacy

Panel Discussion