COMP20008
Elements of Data Processing

Semester 2 2019

Big Data and Analytics - Cool! But .. do the humans really understand where they are headed?

Dr Suelette Dreyfus
School of Computing and Information Systems

Introduction to your lecturer

Who is Dr Suelette Dreyfus – and why does she know about digital privacy?

State of the Art in Consumer Data Tracking and Its Impact on Consumers in Australia

Report written by Dana McKay, with contributions by Yung Ju Chua, Shanton Chang, Suelette Dreyfus, Monica Whitty, Jeannie Marie Paterson, Pan Zhan, Garreth Hanley and Andrew Clausen

September 2019

Funded by Consumer Policy Research Centre

Embargoed until Friday Nov 8

Analytics is being used to track and analyse individuals

Former US National Security Agency executive Thomas Drake referencing George Orwell's famous book about state surveillance '1984':

> "I don't want to be Winston cowering in a corner because its only place the cameras couldn't reach"

Support The Guardian
Available for everyone, funded by readers
Contribute → Subscribe →
Sign in The Guardian

News Opinion Sport Culture Lifestyle

Australia World AU politics Environment Football Indigenous Australia Immigration More

Technology

US whistleblower blames Australian government for 'Orwellian' axing of conference speech

Thomas Drake and academic Suelette Dreyfus were dropped from the line-up at a Melbourne cyber conference at the last minute

▲ US whistleblower Thomas Drake says Australia is the only country where he has had a speech cancelled.
Photograph: Larry Busacca/Getty Images

Source:
https://www.theguardian.com/technology/2019/oct/08/us-whistleblower-thomas-drake-says-speech-was-cancelled-due-to-government-pressure

Old vs New Surveillance

Old surveillance:

- 'What you say': Transaction-based
- Conversations
  - Postal Mail
  - Wire taps on phones
  - Chat logs

New surveillance:

'Who you are'

- movement tracking of consumers in private-public spaces
- facial recognition
- mood analysis

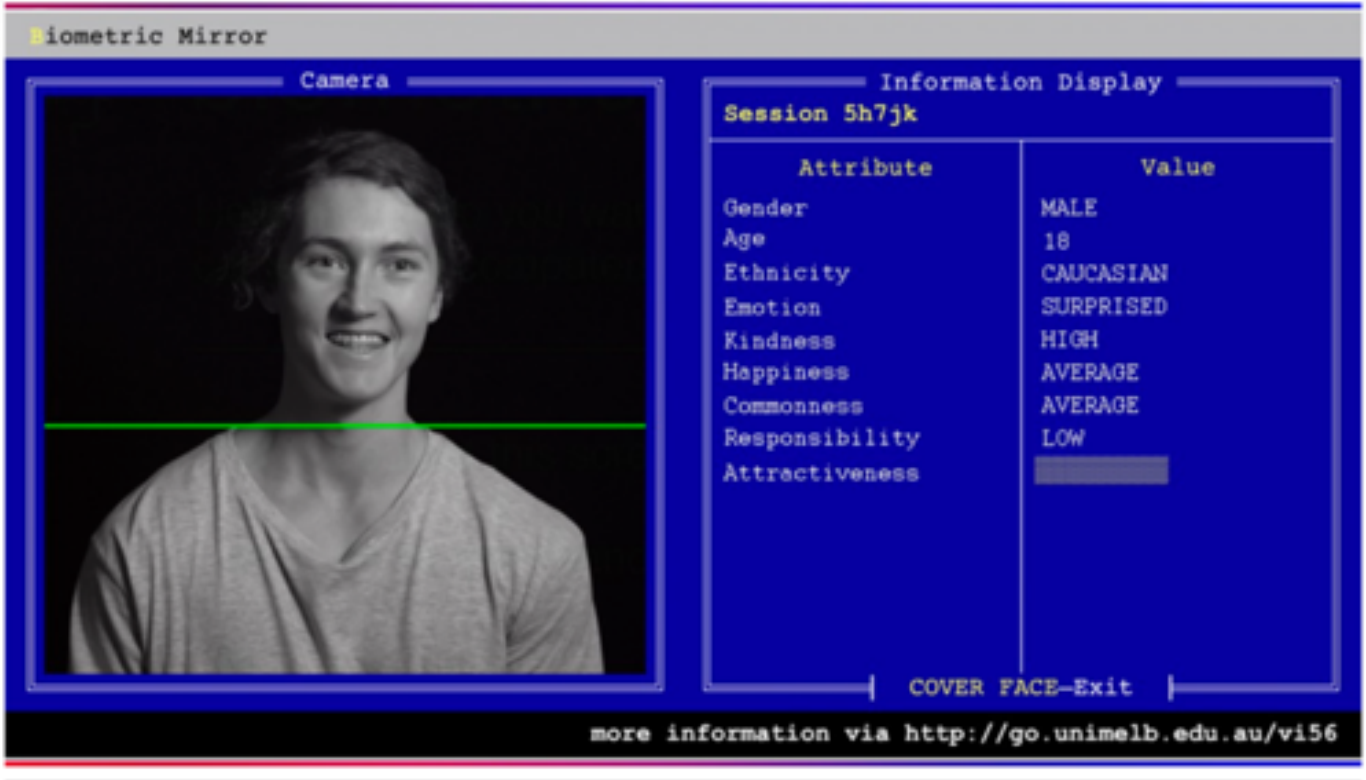
AND .. *New* New Surveillance

'Who **we say** you are'

1. Interpretations of a consumer's capabilities and self
2. Based on untested, non-transparent 'science'
3. **Potentially used in a discriminatory manner**

Biometric Mirror

Biometric Mirror



Biometric Mirror uses an open dataset of thousands of facial images and crowd-sourced evaluations. Picture: Sarah Fisher/University of Melbourne

Analytics being used to track and analyse individuals

Ex: Capable. Not Active?

Airplanes:

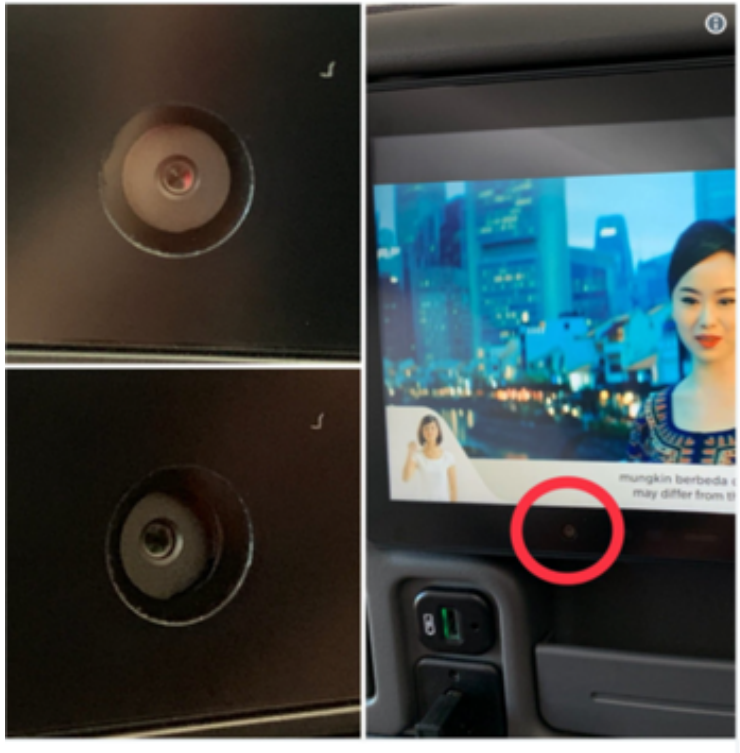
Carriers w/ installed Panasonic IFE systems:

SQ, AA, EK, QF

- Singapore stated they are ‘disabled’.
- AA: ‘Never been activated’
- UA: ‘Possible future use’

Cameras have become the norm, not the exception, for most hardware

Hacking risk to privacy?



Analytics being used to track and analyse individuals

Capable. And Active?

Emporium shopping centre
(Melbourne)

Analytics being used to track and analyse individuals

Capable. And Active?

Doncaster shopping centre
(Melbourne)

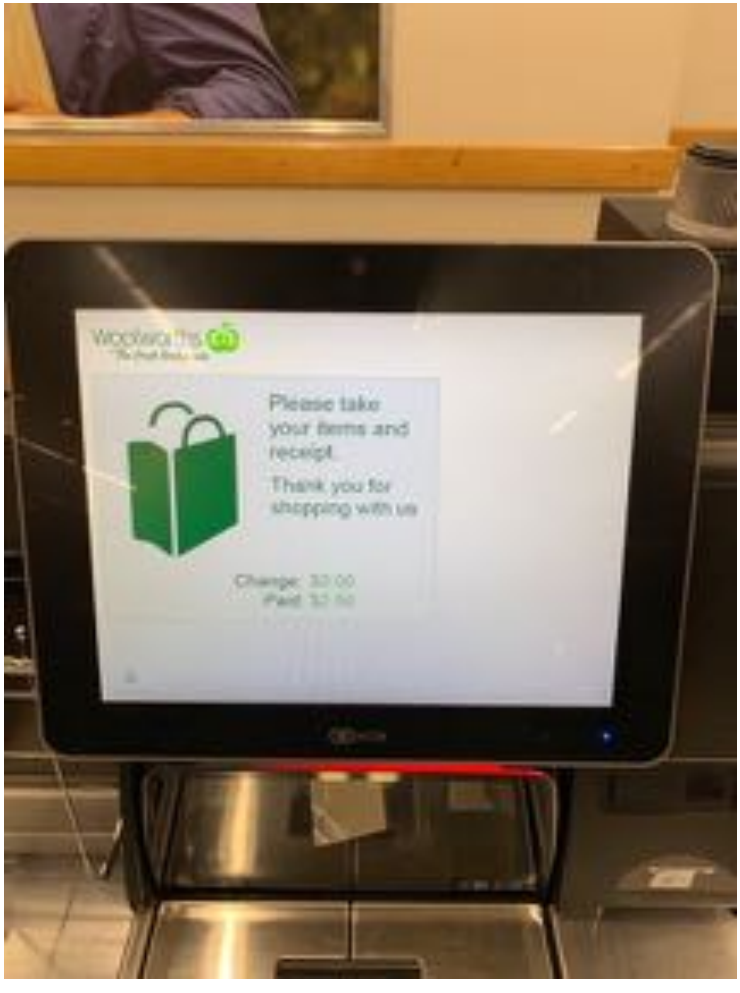
Analytics being used to track and analyse individuals

Capable.
And Active.

7-11 Petrol Station

Analytics being used to track and analyse individuals

Spot the Camera at top of Point of Sale



DART
Digital-outdoor Audience in Real Time

- Collection of data combined with responsive advertising
- Real time responsiveness
- “The most intelligent out of home audience measurement system”
- “So advanced its like having a digital analyst assessing audience while they view your outdoor content in real time.
- “A DA anonymously tracking over 2 m Australians weekly
- “Measures those viewing your content based on Age, Gender, when they viewed, how many viewed across entire length of campaign”

Analytics being used to track and analyse consumers

(Continued)

- Reads audience characteristics with precision
- Identifying 18 demographic profiles
- It even highlights **facial features**
- “Know viewing habits”
- “Know **moods**” (eg sentiment analysis)
- “Have your content triggered when the **relevant** target audience is watching”
- Its not called campaigning but rather:
- “It’s your campaign intelligence” (eg facial slurping and analysis)

Tracking and analysing citizens too..

(Continued)

- Not only the commercial sector
- Governments are putting forward more related laws
- Parliamentary Joint Committee on Intelligence and Security review of Identity-matching Services Bill 2019 and the Australian Passports Amendment (Identity-matching Services) Bill 2019
- October 2017, the Prime Minister and state and territory leaders agreed to establish a National Facial Biometric Matching Capability & signed Intergovernmental Agreement on Identity Matching Services.
- Easier for law enforcement agencies to identify people
- all jurisdictions will be able to use the new face matching services to access passport, visa, citizenship, and driver licence images.

Sources:https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Identity-Matching2019

And https://www.efa.org.au/2019/10/11/scheduled-facial-recognition-public-inquiry-cancelled-by-australian-government/

Models of consent in data gathering from consumers

1. **Forced consent**: A clickwrap ‘take it or leave it’ approach
2. **Unforced consent**: Fully informed, and where consumers have some control over their own data
3. **No consent**: No information or opportunity to opt out is provided to users of a space or service.

To have any control over their data, consumers must be able to give unforced or genuine informed consent.

But with facial ‘slurping’, #3 becomes the norm.

Deeper Issues

1. Do you ‘own’ the exterior manifestation of yourself?
   - Can we talk about ‘digital citizenship’ if you have no enforceable claim of rights?

Summary Issues

2. Do we have the **right to know** how others 'read' us in 'forced consent' or 'no consent'?

- Govt institutions
- Commercial service providers
- Other people (consumers) who use these services (eg dating, housemate finding services)
- Privacy is contextual: one Insta post versus the entire Twitter feed

Summary Issues

2. Do we have the **right to correct** how others 'read' us in 'forced consent' or 'no consent'?

- Govt institutions
- Commercial service providers
- Other people (consumers) who use these services (eg dating, housemate finding services)

Summary:
3 big emerging areas of concern

- Movement tracking of consumers and citizens in private-public spaces
- Facial recognition
- Mood / sentiment analysis

Ethical implications for Individuals: Some factors to consider

Data Control	The extent to which an individual is empowered to audit the access to, storage, exploitation and modification of data about the individual.
Awareness	The extent to which an individual is mindful in consenting as to what data is collected about them and how it is used.
Trust	The extent to which an individual can have confidence that the parties who have access to their data respect the individual's rights.
Privacy	The extent to which an individual is able to restrict the disclosure of their personal information. *"If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place" ?*
Choice	The extent to which an individual is able to make choices without being unfairly discriminated against or constrained by the use of big data and analytics.
Anxiety	The extent of psychological discomfort engendered by the collection and use of personal information for big data analytics purposes.

Ethical implications for Organisations

Data Quality	The extent to which organisations ensure the accuracy, currency, completeness and validity of big data.
Data Sourcing	The extent to which organisations collect, buy, and aggregate data from multiple sources in a manner that respects the rights of individuals.
Data Sharing	The extent to which organisations share, sell or otherwise disclose data in a manner that respects the rights of individuals.
Decision Making	The extent to which big data analytics and resulting organisational decisions respect the rights of individuals.
Ethical Culture	The extent to which organisations have values, norms and shared beliefs that promote ethical big data analytics practices through education, training and other means.
Ethical Data Governance	The extent to which organisations articulate ethical standards, decision rights and responsibilities for sourcing, analysing and sharing big data.
Behaviour	The extent to which organisational actors behave consistently with their organisation's ethical culture and standards.
Reputation	The extent to which relevant stakeholders (e.g. customers) believe an organisation will manage and utilise data about them ethically.
Competitive Pressure	The extent to which organisations are subject to pressure to compete using big data analytics unethically.

Ethical implications for Society

Power Imbalance	The extent to which power in society is imbalanced by the use of big data analytics by a dominant group, organisation or government.
Coercion	The extent to which participation and functioning in society is dependent on contributing one's own data to a collection for analysis.
Social Awareness	The extent to which members of a society are aware of the role of big data analytics in directing and regulating behaviour in the society.
Surveillance	The extent to which the lives of individuals in a society are observed, monitored, measured and profiled.
Principles and Guidelines	The extent to which effective principles and guidelines exist to protect the rights of individuals impacted by big data analytics.
Authority	The extent to which an entity (e.g., government, professional association) acts to enforce, through sanctions or other means, the rights embodied in the established principles and guidelines for big data analytics.
Social Mindset	The extent to which society collectively feels anxious and oppressed (or opposingly assured and empowered) about the use of big data analytics.

Societal actors need to provide oversight and regulate

EU General Data Protection Regulation (enforced since May 2018)

Aims to regulate and protect data privacy for all EU citizens.
- Penalty 4% of annual global turnover of the organizations.

The consent
- should be clear, concise, not too long and intelligibly written—should attach the reasons of data collection and analyses.
- individuals have the right to withdraw the consent with the same easiness that they have previously agreed with.

Accessing individual's data
- Individuals have the right to ask for a copy of their personal data together with information regarding the processing and purpose of data collection and analyses from a controller
- Individuals have the right of data portability, which means that they can transfer their data from one controller to another.

http://www.eugdpr.org/eugdpr.org.html

Summary: What can we do?

We need to empower individuals

- Educate individuals, raise social awareness
- Provide data access and control (e.g. Google activity)
  - http://www.abc.net.au/4corners/stories/2017/04/10/4649443.htm

Define and develop a culture of acceptable data use

- Organizations should internalize the costs
- Genuine consent from individuals
- Be transparent and clearly communicate intent of data collection and analytics/AI
- Adopt rules for responsible big data research
- Provide data control to individuals

Acknowledgements

The Research Project Team

Assoc. Prof. Shanton Chang – CIS, University of Melbourne
Prof. Jeannie Marie Paterson – Law, University of Melbourne
Prof. Monica Whitty – Arts, University of Melbourne
Dr Andrew Clausen – Economics, University of Edinburgh
Dr Dana McKay - CIS, University of Melbourne
Yung Ju Chua - CIS, University of Melbourne
Pan Zhan- ENG, University of Melbourne
Garreth Hanley - Journalist
Dr Suelette Dreyfus - CIS, University of Melbourne

And

The Consumer Policy Research Centre in Melbourne, Victoria

References

Anscombe, L. (2017). Westfield is using facial detection software to watch how you shop. Retrieved from https://www.news.com.au/finance/business/retail/westfield-isusing-facial-detection-software-to-watch-how-you-shop/newsstory/7d0653eb21fe1b07be51d508bfe46262

Culnane, C., Rubinstein, B. I. P., & Teague, V. (2017). Health Data in an Open World. arXiv eprints. https://ui.adsabs.harvard.edu/\#abs/2017arXiv171205627C

Chua, YJ (2019) Privacy and discrimination of consumers in a world of ubiquitous computing