

The Digital Surveillance Economy

How did we let it happen??

What do we do about it?

Roger Clarke

Xamax Consultancy Pty Ltd, Canberra
Visiting Professor at A.N.U. and U.N.S.W.

<http://www.rogerclarke.com/SOS/DSEP> {.html, .ppt}

ATSE Canberra – 18 July 2018

Copyright
2016-18





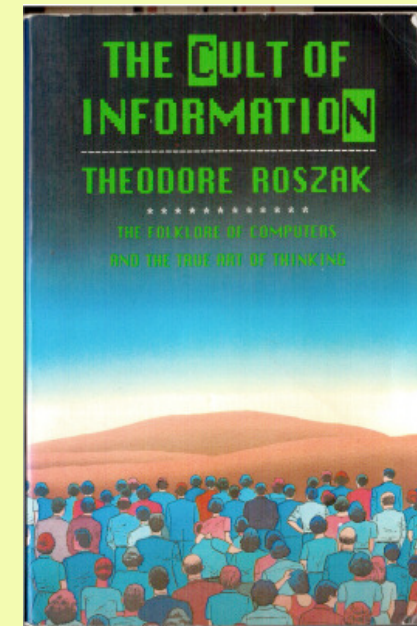
Surveillance Society / Surveillance State

"Technology could be offering the tools for building a surveillance society in which everything people do and are ... is an open book to those who assert some 'right' to monitor them"

Weingarten F.W. (1988) 'Communications Technology: New Challenges to Privacy' J. Marshall L. Rev. 21, 4 (Summer 1988) 735

"[the purpose of computerised surveillance] is to reduce people to statistical skeletons for rapid assessment"

Roszak T. (1986) 'The Cult of Information' Pantheon, 1986



The Digital Surveillance Economy

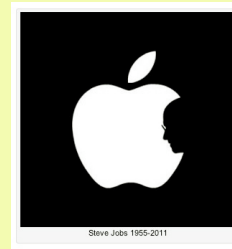
That combination of institutions,
institutional relationships and processes,
which enables **corporations to exploit data
that arises from the monitoring of
people's electronic behaviour**
and on which consumer marketing
corporations have become dependent

The FANGS of The Digital Surveillance Economy

F acebook



A pple



amazo N



G oogle



micro S oft



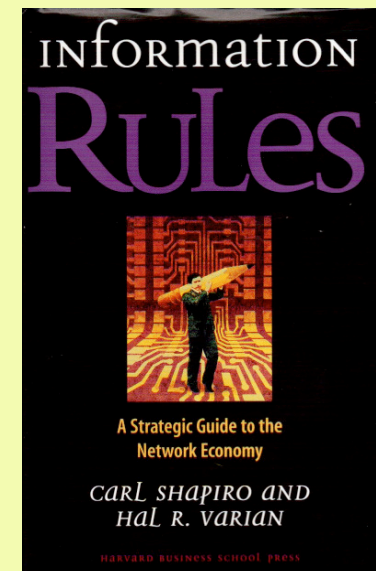
The Textbook Message

"[marketers'] strategy should be to **bribe users to give [marketers the appropriate demographics, which in turn can be passed onto advertisers ...**

“[The game is about] **inducing consumers to give [marketers] the information they want.**

“we expect that many consumers will be happy to sell information about themselves for a nominal amount ...”

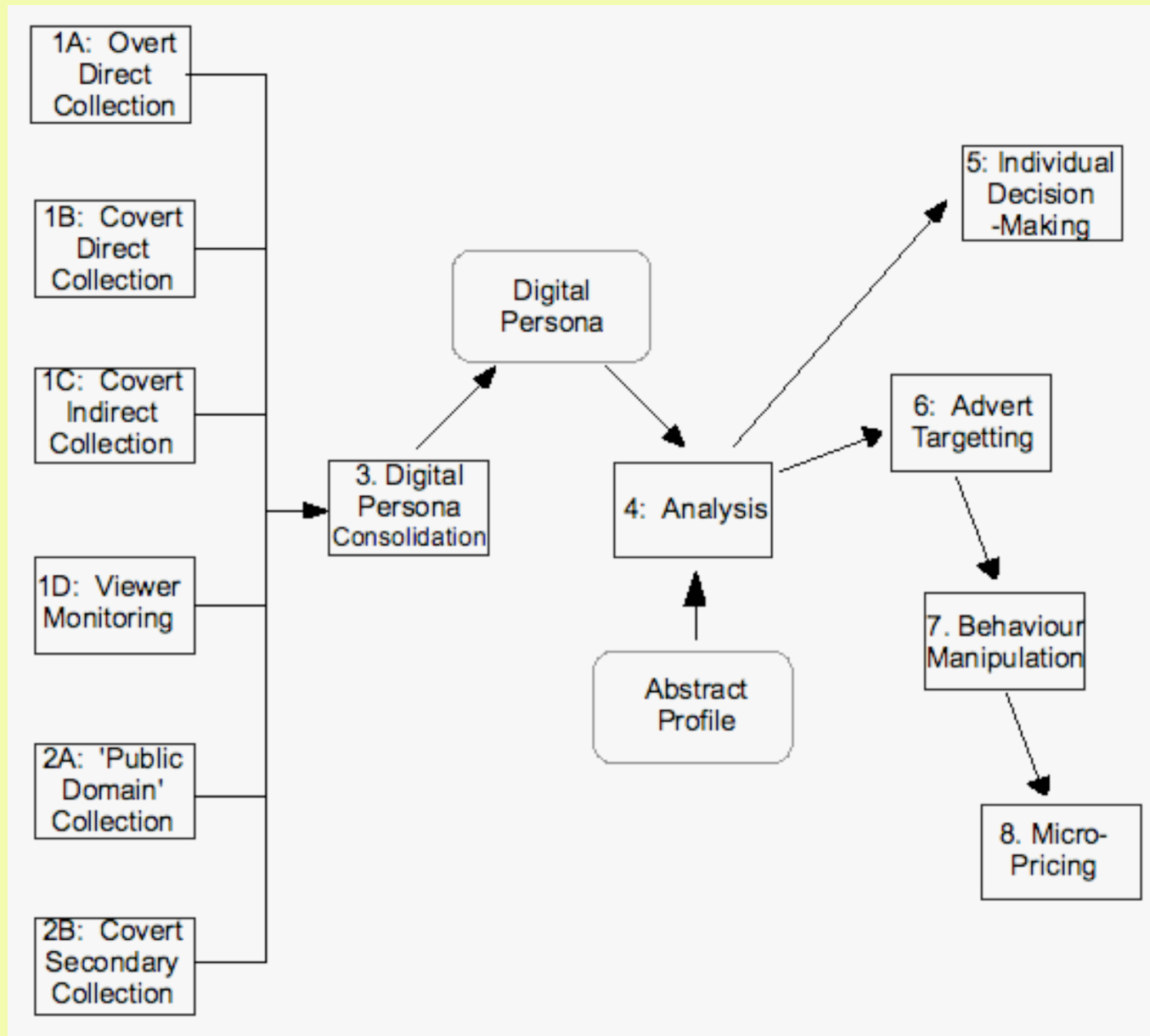
Shapiro C. & Varian H.R. (1999)
'Information Rules: A Strategic Guide
to the Network Economy'
Harvard Business School Press, 1999 (pp. 35-36)



Copyright
2016-18



> 10,000 Google citations



1A. Data Gathering by Direct, Overt and Possibly Consensual Means

- Enquiries
- eCommerce Transactions
- Payment Transactions
- Advertising Clicks
- **Search-Terms**
- Media Experiences
- **Social Media Profiles, Posts, Accesses**
- **The 'Quantified Self'** (i.e. emanating from 'wellness devices' and other 'wearables')
- **Genetic Data** (ancestry.com, et al.)

1B. Data Gathering by Direct Means that are Covert and (at best) Pseudo-Consensual

- 'Click-Stream Data'
- Browser Fingerprints
- HTTP (the Web's carrier protocol)
- HTML5 (the Web's page-markup language)
- Cookies
- Web-bugs / Web-beacons / Tracking Pixels
- Adware / Spyware
- ...

1	Companies	Websites	Wikipedia pages	National laws
2	Google	http://www.google.com/about/company/facts/locations/	https://en.wikipedia.org/wiki/Google	US
3	Facebook	https://www.facebook.com/facebook/info?ref=page_internal	https://en.wikipedia.org/wiki/Facebook	US
4	Twitter	https://about.twitter.com/	https://en.wikipedia.org/wiki/Twitter	US
5	AOL	http://www.aol.com/	https://en.wikipedia.org/wiki/AOL	US
6	Krux	http://www.krux.com/	Not available	US
7	Adobe	http://www.adobe.com/	https://en.wikipedia.org/wiki/Adobe_Systems	US
8	comScore	http://www.comscore.com/	https://en.wikipedia.org/wiki/ComScore	US
9	Amazon.com	http://www.amazon.com/	https://en.wikipedia.org/wiki/Amazon.com	US
10	Visual Revenue	https://www.linkedin.com/company/visual-revenue-inc	Not available	US
11	Fox One Stop Media	http://foxinternationalchannels.com/about/fox-one-stop-media	https://en.wikipedia.org/wiki/21st_Century_Fox	US
12	Turn	http://www.turn.com/	Not available	US
13	Quantcast	https://www.quantcast.com/	https://en.wikipedia.org/wiki/Quantcast	US
14	Criteo	http://www.criteo.com/	https://en.wikipedia.org/wiki/Criteo	FR
15	Lotame	http://www.lotame.com/	Not available	US
16	Datalogix	http://www.datalogix.com/	https://en.wikipedia.org/wiki/Datalogix	US
17	AddThis	http://www.addthis.com/	https://en.wikipedia.org/wiki/AddThis	US
18	Chartbeat	https://chartbeat.com/	https://en.wikipedia.org/wiki/Betaworks	US
19	Optimizely	https://www.optimizely.com/	https://en.wikipedia.org/wiki/Optimizely	US
20	Outbrain	http://www.outbrain.com/	https://en.wikipedia.org/wiki/Outbrain	US

1C. Data Gathering by Indirect Means that are Covert and (at best) Pseudo-Consensual

Various arrangements whereby
interactions with one corporation
are visible to other corporations as well

e.g. stay logged-in
with Google, Facebook, LinkedIn, etc.
and all traffic with all other web-sites can be
communicated to those corporations



TECHNOLOGY PRIVACY

'Over a barrel': We are clueless about how much data we're giving up

By Tim Biggs & Patrick Hatch

16 July 2018 – 3:33pm



16

[View all comments](#)

Article No. 7650
Available on www.roymorgan.com
[Link to Roy Morgan Profiles](#)



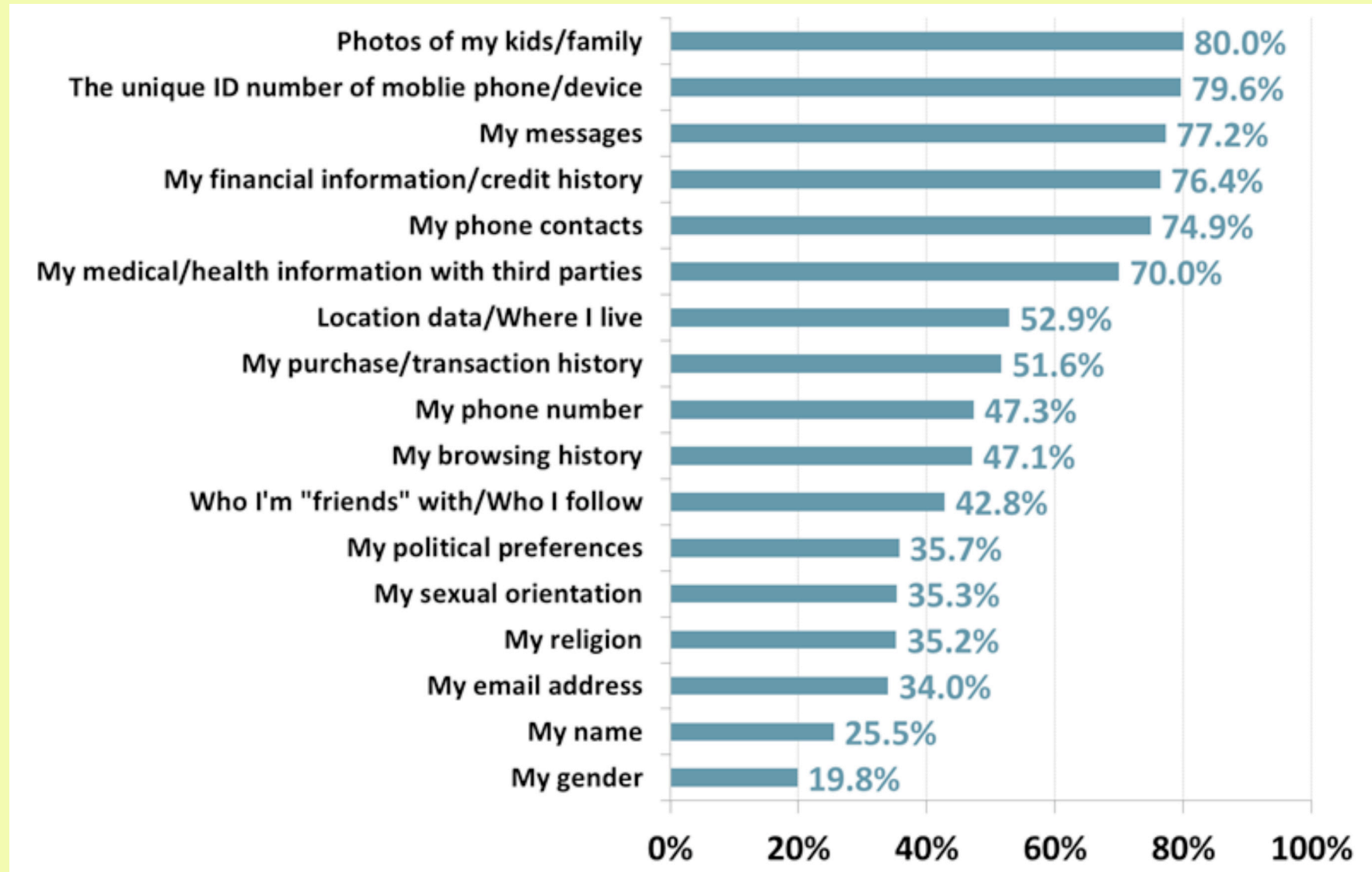
Friday, 6 July 2018

Australians worried about online privacy but slow to act

An in-depth study by Roy Morgan into Australian attitudes towards privacy in the online world has revealed huge concerns exist around how Australians' personal data is used online.

c. 90% of respondents: it is unacceptable for companies to collect this data to tailor ads and offers to consumers:

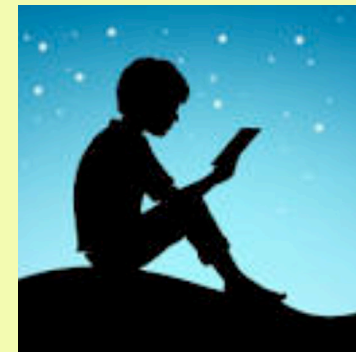
- personal financial data 77% very + 15%
- contents of messages or emails 79% very + 20%
- health and medical data 74% very + 15%



1D. Viewer Monitoring

Covert and Pseudo-Consensual

- **Viewing text, images, sound and video generates data about the viewer's activities which is exfiltrated to suppliers, incl.:**
 - webmail (cf. email)
 - viewing of downloaded files
 - use of streaming services
 - e-readers
- **Breaches of 'Experiential Privacy'**



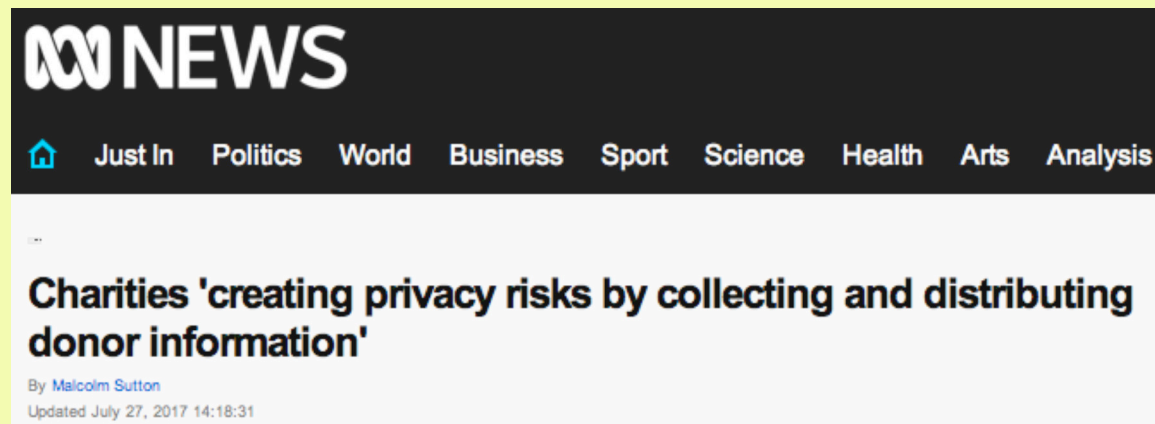
1E. 'Public Domain' Collection Covert and (at best) Pseudo-Consensual

- **Social Media:**
 - Profile-Data
 - 'Likes'
 - Postings
 - Social Networks
 - Inferences about other individuals
- **Open Directory Profiles**
- **Hits on Search-Engine Indexes**
- ...

Trafficking among Industry Players Covert and Non-Consensual

Sale, barter, share, gift, etc.
perhaps camouflaged as 'strategic partnership'

e.g. abuse by Australian charities
of the personal data of their donors
by passing the data on to other charities
which, as part of the process,
gifts the data to marketing services corporations



Google allows third parties to read Gmail users' inboxes


4 July 2018

Copyright
2016-18



☰ Menu

FINANCIAL REVIEW
— NEWS WEBSITE OF THE YEAR —

A 3D-style illustration of a white envelope with a red 'M' logo on the inside, set against a dark background with a subtle grid pattern.

Millions of people are believed to have installed Gmail apps. However, installing them hands the app developers full access to users' inboxes.

by **Natasha Bernal**

Google allows employees at software companies to read millions of **Gmail** users' private messages, it has emerged.

The popular email service, which has more than one billion users around the world, gave hundreds of developers outside the company access to users' inboxes.

They were then able to read and scan private emails to target adverts.

Merger with Existing Data Collections Also Covert and (at best) Pseudo-Consensual

- 'Mailing List' / Database Marketing
- 'Loyalty' schemes
- Credit Bureau Databases
- Telephone Directory data
- Electoral Roll data
- Court Documents
- Court Case Reports
- ...

3. Consolidation of Digital Personae

- A model of an individual's public personality, based on data, maintained by transactions, and intended for use as a proxy for the individual
- Dependence on identifiers:
 - Loginids
 - IP-Addresses
 - Browser-Fingerprints
 - GPS Coordinates
 - Loose Inferencing Techniques
- Name-Address-DoB is not a necessary identifier

Data Brokers Supporting The Digital Surveillance Economy



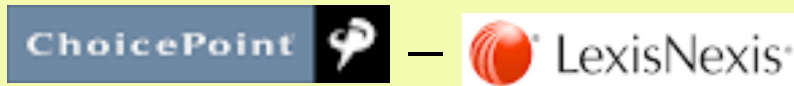
2.5bn 'customer relationships'



1500 'data partners'



'AdTruth ID'



'TrueID' incl. biometrics



All Australian credit data



In 540,000 mobile apps



Actively targets 'activists'



Micropayment data



3bn cookies, 2bn device-IDs



>700bn instances of personal data



MasterCard, Visa, Amex

...

Is all of this legal??

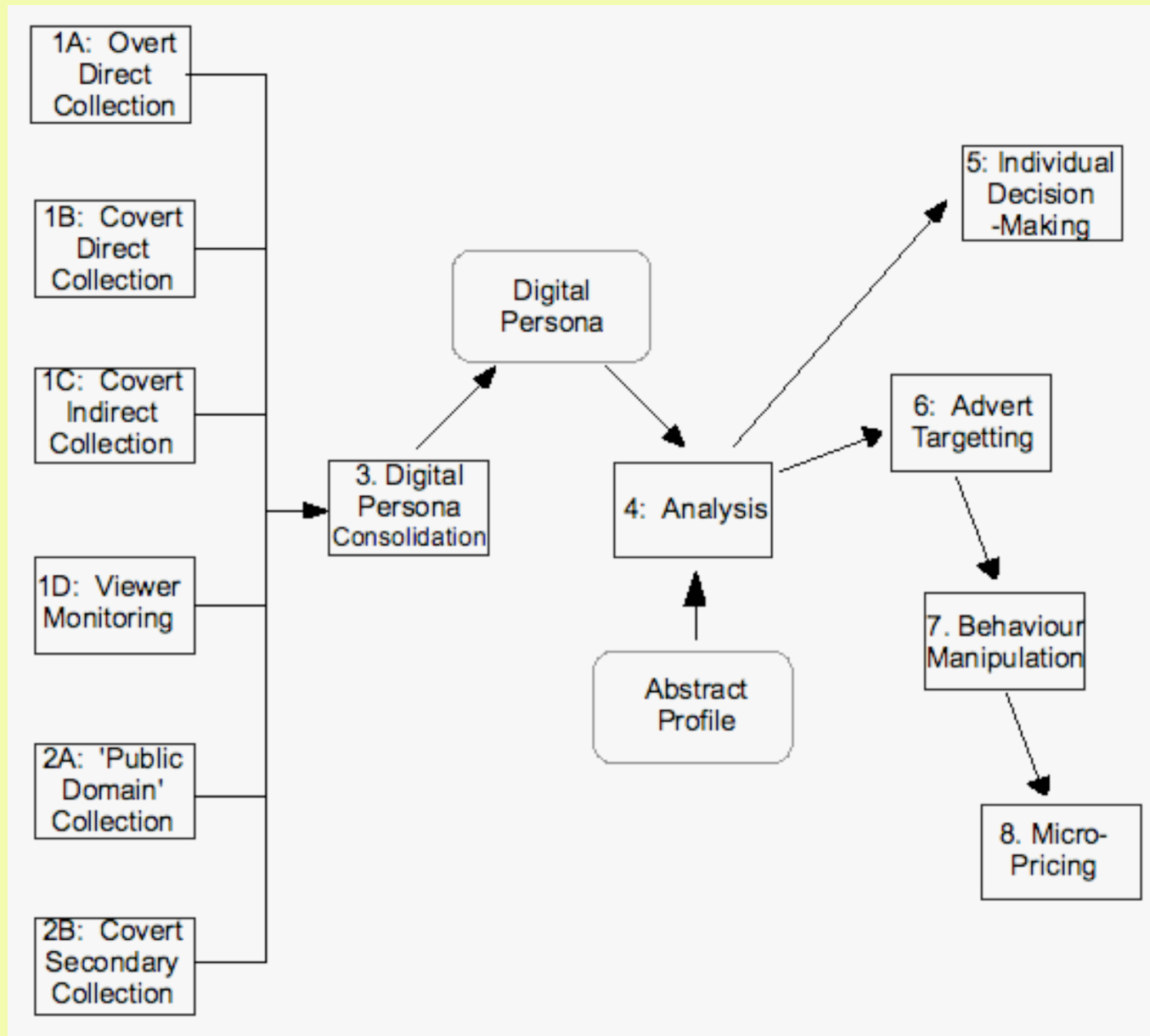
- **Australia**
 - Privacy Act (Cth), but almost vacuous
 - Further dilution in favour of 'open data'
 - Office of the Aust. Info. Commissioner (OAIC)
 - Privacy Commissioner
- **USA**
 - No generic statutory protections
 - Federal Trade Commission (FTC)
- **EU**
 - General Data Protection Regulation (GDPR)
 - Data Protection Commissioners
(at EU and National levels)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)

 In force

OJ L 119, 4.5.2016, p. 1–88 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)

ELI: <http://data.europa.eu/eli/reg/2016/679/oj>



4. Analysis

- Inferences are drawn about an individual
- e.g. **Compare each Digital Persona with 'abstract consumer profiles'**, which may be:
 - *ad hoc* / rule-of-thumb / heuristic
 - based on studies and experiments re personality-types, attitudes and / or long-term and short-term interests
 - the 'Big Five' psychographic classification: extraversion, neuroticism, agreeableness, conscientiousness, and openness

5. Decision-Making about Individuals

- Based on the digital persona and the organisation's inferencing techniques
- Contexts include initiation and admin of:
 - Loans
 - Insurance
 - Employment
 - Health Care
 - Social Welfare
 - ...

5. Decision-Making about Individuals Consumer Safeguards

- Financial Services Ombudsman ??
- Telecommunications Industry Ombudsman ??
- **Insurance Industry Ombudsman ???**
- Health Care Complaints Commissions ??
- Employment Tribunals ??
- Centrelink and the AAT ??
- State Govt Offices of Fair Trading ??
- Privacy Law ??
- **Aust Consumer Law / Consumer Credit Code ??**

6. Ad Targeting

- Web-sites that attract consumers' attention rent out space in the user's browser-window
- **Based on each consumer's Digital Persona, ads are selected and/or customised**
- The process reflects the persona's recorded demographics, preferences, attitudes and interests
- **Such 'narrowcast' ads are much more effective than old-style, mass-market 'broadcast' ads**
- A highly-developed, real-time process auctions ad space in consumers' browser-windows

6. Ad Targetting Consumer Safeguards

- Advertising Standards Bureau ??
- Australian Competition & Consumer Comm'n (ACCC) ??
- Australian Comms and Media Authority (ACMA) ??
- Computer Crimes statutes ??
(influenced by the CoE Convention on Cybercrime)
- **Aust Consumer Law / Consumer Credit Code ??**

7. Consumer Behaviour Manipulation

- **Tightly-targeted and well-timed ads can be highly persuasive, and can have a decisive and predictable effect on consumers' decisions and actions:**
"Nudging for profit [exploits the fact] that individuals systematically behave in nonrational ways"
- However, researchers are divided on the degree of effectiveness of targeted ads

Packard Y. (1964) 'The Naked Society' McKay, New York, 1964

Calo R. (2014) 'Digital Market Manipulation'
George Washington Law Review 82, 4 (2014) 995–1051

8. Micro-Pricing

- Marketers use digital persona to gauge the point at which buyer-resistance is likely to arise
- The offer is pitched just below each individual consumer's resistance-point, extracting the maximum revenue from each individual
- This disadvantages most consumers compared with longstanding pre-set fixed-price offers
- Consumers naively accept the marketer's pitch that the consumer's been given a 'special offer'

OLD-WORLD: what the market as a whole will bear

NEW-WORLD: what the individual consumer will bear

Is Micro-Pricing Legal ??

Aust. Consumer Law / Consumer Credit Code 2010



<http://consumerlaw.gov.au/>

- misleading and / or deceptive conduct (s.18) ??
- false and misleading representations (s.29) ??
- 'unfair conduct' (nonesuch) ???
- **'unconscionable conduct' / 'undue influence'** (ss.21-22) ??
- 'unfair contract terms' (ss.24-25) ??
- ... ??

Threats to Individuals

- **Asymmetry** of Information and Market Power
- **Impulse Buying** / **'Compulsive Purchasing'** of unnecessary and/or unduly expensive items
- **Discrimination**, Blacklisting, 'Weblining'
- **Unfair Decisions** based on inaccurate data, partial personae, and conflated personae
- **Automated Decision-Making**, lack of transparency, no accountability, no redress
- **'Chilling Effect'** / **'Psychic Numbing'**

Broader Impacts

- **Chilling of Important Behaviours**
Arts, Culture, Society, Politics
Science, Technology, Economics
- **'Corpocracy'** – a politico -economic system
in which corporations dominate governments
- **'Digital Demagoguery'** – Trump's Tweets,
Erdogan's Rallies, Central European Populism
- **Risk of Sterility / Passivity**
cf. East Germany under the Stasi

Impacts on the Polity



+



Manipulation of Voters' Behaviour

Add in 'Reds under the Bed'
and National Sovereignty Issues

'it's okay if our politicians manipulate us'

'it's not okay if outsiders manipulate us'

Facebook faces £500,000 fine from UK data watchdog

© 11 July 2018

The UK's data protection watchdog intends to fine Facebook £500,000 for data breaches - the maximum allowed.

The Information Commissioner's Office said Facebook had failed to ensure another company - Cambridge Analytica - had deleted users' data.

The ICO will also bring a criminal action against Cambridge Analytica's defunct parent company SCL Elections.

And it has raised concerns about political parties buying personal information from "data brokers".



Voices

Facebook's fine for data breaches won't reduce the web's appetite for our personal information

The truth is, modern society is now so indebted to, and reliant on, data analytics that we would barely function without its benefits

Will Gore | @willjgore | 6 days ago | 1 comment

Natural Controls

- **Economic** Factors / Cost-Benefit-Risk Trade-Off (cf. the 'invisible hand' of market forces)
- **Reputational** Factors / 'the court of public opinion', media articles, social media
- **Targeted Action** by a powerful party
- **Collective Action** by the affected public

Regulatory Alternatives

Intervention is justified where natural controls are inadequate / 'market failure' occurs

- Formal Regulation
- Co-Regulation
- Industry Self-Regulation
- Organisational Self-Regulation

Scenarios

1. **Consumers Wake Up** to the situation, and turn the tide through collective action
2. **Parliaments or Regulators Intervene** in order to moderate corporate dependence on consumer surveillance
3. **New Market Players Arrive**, using a less consumer-rapacious business model
4. **Formal Standards** reflect consumer needs
5. **The Default:** Consumers meekly accept intensive and continual surveillance, data-trafficking and control of their behaviour

The Digital Surveillance Economy

How did we let it happen??

What do we do about it?

Roger Clarke

Xamax Consultancy Pty Ltd, Canberra
Visiting Professor at A.N.U. and U.N.S.W.

<http://www.rogerclarke.com/SOS/DSEP> {.html, .ppt}

ATSE Canberra – 18 July 2018

Copyright
2016-18

