

PRIVACY: PART I

DAVID MILLARD

DEM@SOTON.AC.UK

ENEMY OF THE STATE (1998): What Technologies are used?



WAS THIS REALISTIC IN 1998?



IS IT REALISTIC **NOW?**



What Could I Find Out About You?
From **Your** Account



What Could I Find Out About You?
From **Your Friend's** Accounts



How Do You Defend Yourself?



Privacy Protection Strategies

F. Asiri and D. Millard, "Unpacking Privacy Practices in SNSs: Users' Protection Strategies to Enforce Privacy Boundaries,"
2018 21st Saudi Computer Society National Computer Conference (NCC), Riyadh, 2018

Technological

Segment Audience

Un-tag

Delete

Block

Deactivate



Privacy
Protection
Strategies

Technological

Segment Audience

Un-tag

Delete

Block

Deactivate

Privacy
Protection
Strategies

Social

Social Stenography

Self Censorship

Falsification

Multiple Spaces

White Walling

Information Asymmetry



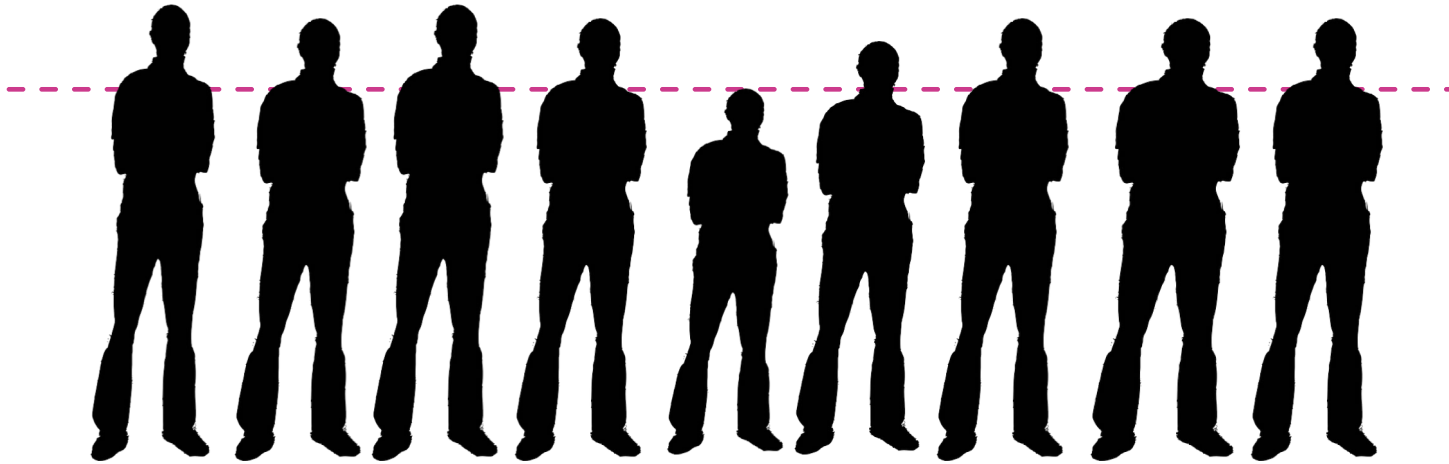
Information Asymmetry



the system
knows more about
you than you have **disclosed**



BOB'S PROFILE SAYS HE IS 6 FOOBARS TALL
WHAT HAS BOB TOLD US; WHAT DO WE KNOW ABOUT BOB?



BOB'S PROFILE SAYS HE IS 6 FOOBARS TALL
WHAT HAS BOB TOLD US; WHAT DO WE KNOW ABOUT BOB?

COMPARISON



ANNE (24)
HOBBY:
HEFTUKA



BRIE (53)
HOBBY:
BUGDUF



CLARE (47)
HOBBY:
BUGDUF



DAVINA (28)
HOBBY:
HEFTUKA



ANNE (24)
HOBBY:
HEFTUKA



BRIE (53)
HOBBY:
BUGDUF



CLARE (47)
HOBBY:
BUGDUF



DAVINA (28)
HOBBY:
HEFTUKA



EMMA (?)
HOBBY:
BUGDUF

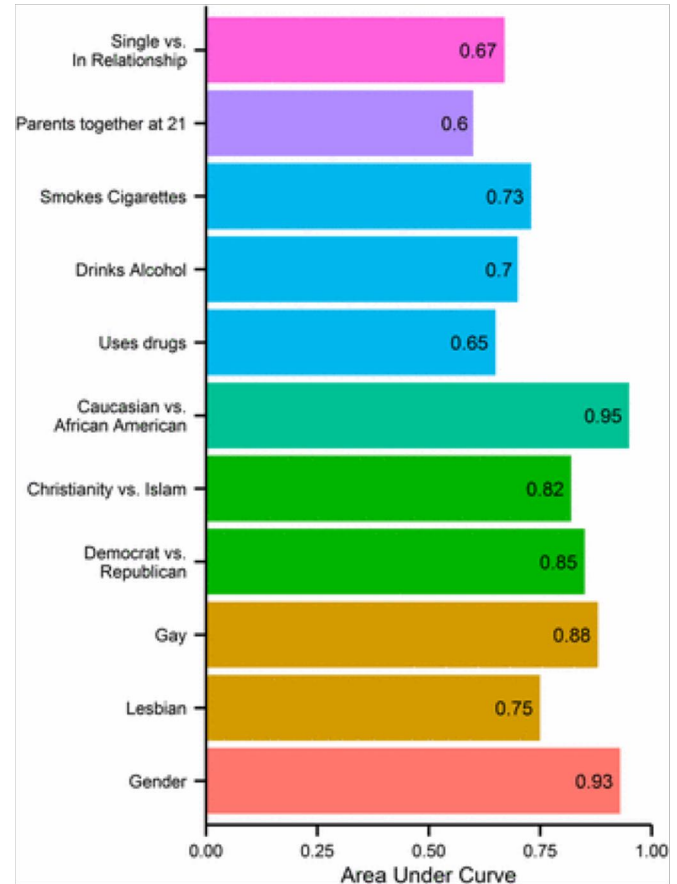
INFERENCE

In 2013 researchers in
Cambridge looked at the
predictive power of
Facebook likes...

Michal Kosinski, David Stillwell, and Thore Graepel. Private traits and attributes are predictable from digital records of human behavior. Proceedings of the National Academy of Sciences. 2013 110 (15) 5802-5805;

In 2013 researchers in Cambridge looked at the predictive power of Facebook likes...

Michal Kosinski, David Stillwell, and Thore Graepel. Private traits and attributes are predictable from digital records of human behavior. Proceedings of the National Academy of Sciences. 2013 110 (15) 5802-5805;



THE DIGITAL SELF

Parkinson, Brian, Laurence, Millard, David, O'Hara, Kieron and Giordano, Richard (2017) The digitally extended self: a lexicological analysis of personal data. *Journal of Information Science*.



THE DIGITAL SELF

- Digital Footprints

Parkinson, Brian, Laurence, Millard, David, O'Hara, Kieron and Giordano, Richard (2017) The digitally extended self: a lexicological analysis of personal data. *Journal of Information Science*.



THE DIGITAL SELF

- Digital Footprints
- 3rd party footprints

Parkinson, Brian, Laurence, Millard, David, O'Hara, Kieron and Giordano, Richard (2017) The digitally extended self: a lexicological analysis of personal data. *Journal of Information Science*.



THE DIGITAL SELF

- Digital Mosaic
 - Digital Footprints
 - 3rd party footprints

Parkinson, Brian, Laurence, Millard, David, O'Hara, Kieron and Giordano, Richard (2017) The digitally extended self: a lexicological analysis of personal data. *Journal of Information Science*.



THE DIGITAL SELF

- Digital Mosaic
 - Digital Footprints
 - 3rd party footprints
- Digital Persona



Parkinson, Brian, Laurence, Millard, David, O'Hara, Kieron and Giordano, Richard (2017) The digitally extended self: a lexicological analysis of personal data. *Journal of Information Science*.

THE DIGITAL SELF

- Digital Mosaic
 - Digital Footprints
 - 3rd party footprints
- Digital Persona

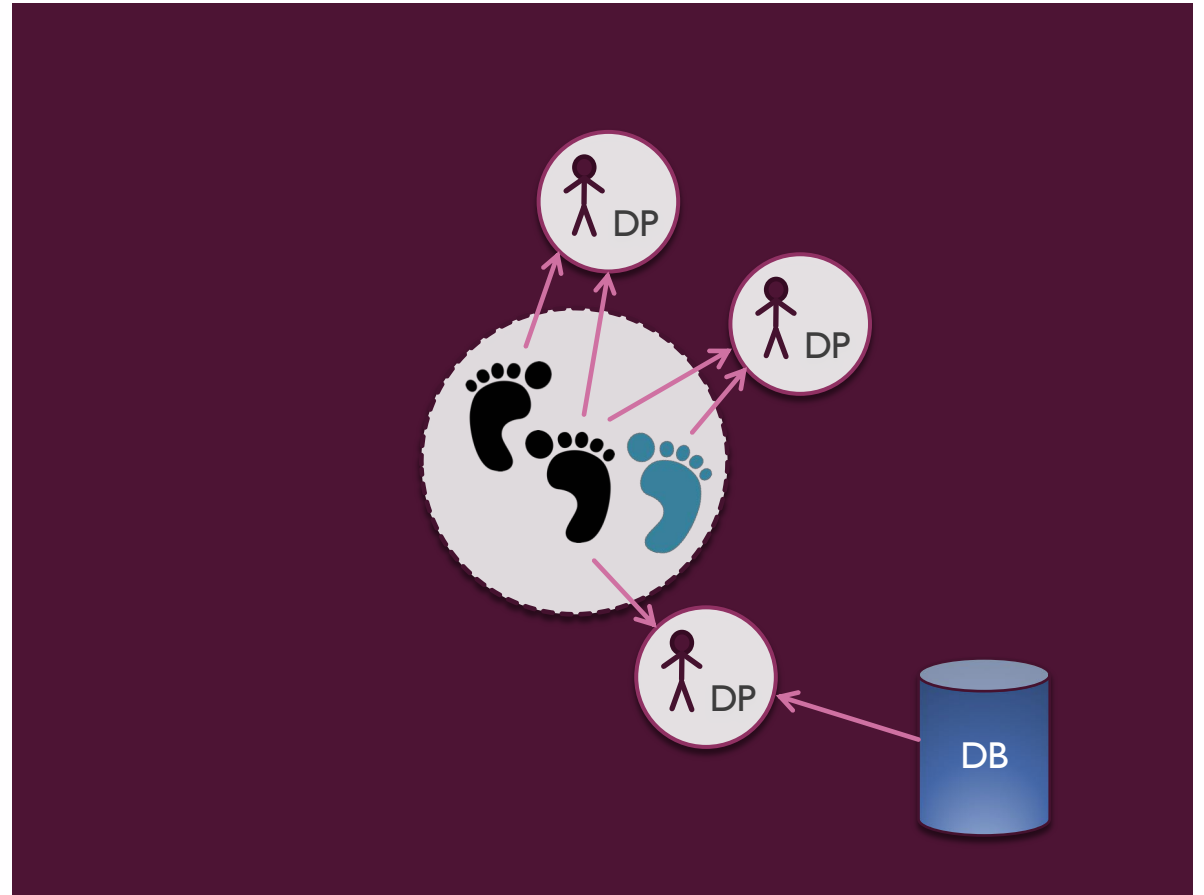


Parkinson, Brian, Laurence, Millard, David, O'Hara, Kieron and Giordano, Richard (2017) The digitally extended self: a lexicological analysis of personal data. *Journal of Information Science*.

THE DIGITAL SELF

- Digital Mosaic
 - Digital Footprints
 - 3rd party footprints
- Digital Persona
 - 3rd party data

Parkinson, Brian, Laurence, Millard, David, O'Hara, Kieron and Giordano, Richard (2017) The digitally extended self: a lexicological analysis of personal data. *Journal of Information Science*.



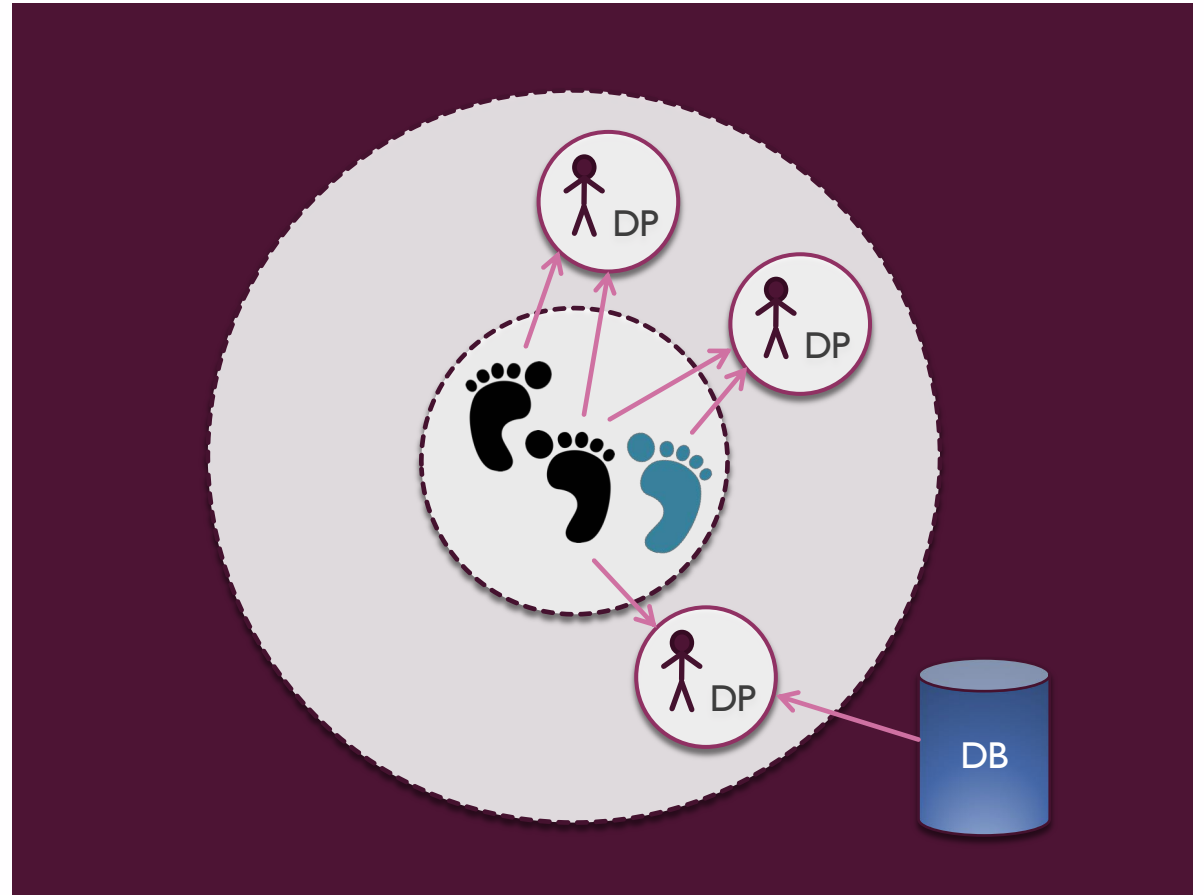
THE EXTENDED DIGITAL SELF

- Digital Mosaic
 - Digital Footprints
 - 3rd party footprints
- Digital Persona
 - 3rd party data

All together is the
Extended Digital Self

Note: Your EDS includes
footprints and data that belongs to
others!

Parkinson, Brian, Laurence, Millard, David, O'Hara, Kieron and Giordano, Richard (2017) The digitally extended self: a lexicological analysis of personal data. *Journal of Information Science*.



INFORMED CONSENT

“Informed consent, according to the common view, is **agent-centered** and **subjective**. It has to be **given freely**, with sufficient knowledge and understanding of **use, risks, consequences** and **alternative options**.

Valid consent can only be given regarding **specific parties** and a **specific offer** at a **specific moment** of time.”

244 HOURS

time for average US Internet user to read
their relevant privacy policies for a year

54 BILLION HOURS

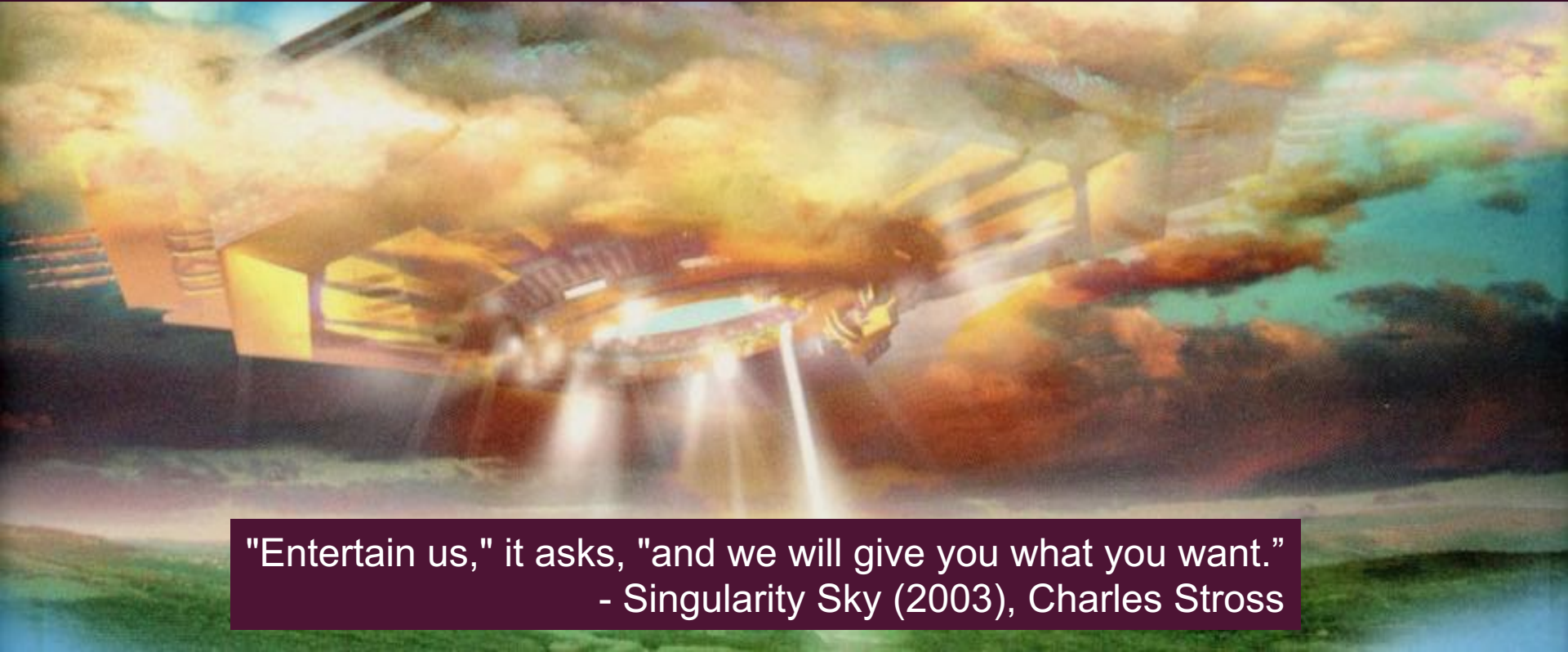
for all US users

6 MILLION PERSON YEARS



Is Consent Possible?

THE DATAVORES



"Entertain us," it asks, "and we will give you what you want."
- Singularity Sky (2003), Charles Stross

“If you’re not paying,
you’re the product”

THE INTERNET OF SHIT

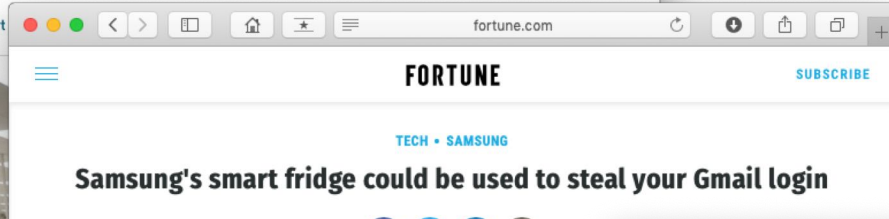


nordic.businessinsider.com

There's a simple reason why your new smart TV was so affordable: It's collecting and selling your data

Follow @BINordic 3,010 followers

Ben Gilbert



FORTUNE

TECH • SAMSUNG

Samsung's smart fridge could be used to steal your Gmail login

Facebook Twitter LinkedIn Email



forbes.com

How A Creep Hacked A Baby Monitor To Say Lewd Things To A 2-Year-Old

74,555 views | Aug 13, 2013, 06:35pm

Kashmir Hill Forbes Staff
Welcome to The Not-So Private Parts where technology & privacy collide

See Also

- 1 Wireless Baby Monitor



MASS SURVEILLANCE

Mass surveillance, by commercial organisations and governments, have led some to proclaim the **death of privacy**



theguardian.com

the guardian

Surveillance

Mass internet surveillance threatens international law, UN report claims

Actions of intelligence agencies are 'corrosive of online privacy', Ben Emmerson says in response to Edward Snowden leaks



'Bulk access technology is indiscriminately corrosive of online privacy', warns Ben Emmerson. Photograph: Sarah Lee for the Guardian

Owen Bowcott and Spencer Ackerman

Wednesday 15 October 2014 09:55 BST

MASS SURVEILLANCE

“If you keep within the law,

and the government keeps within the law, and its employees keep within the law, and the computer holding the database doesn't screw up, and the system is carefully designed according to well-understood software engineering principles and maintained properly, and the government doesn't scrimp on the outlay, and all the data are entered carefully, and the police are adequately trained to use the system, and the system isn't hacked into and your identity isn't stolen and the local hardware functions well,

you have nothing to fear”

MASS SURVEILLANCE

2014 China
announces
plans for new
social credit
system



MASS SURVEILLANCE

Correctional Offender Management Profiling for
Alternative Sanctions (COMPAS) – USA
Assesses risk of repeat crimes

Durham Constabulary's Harm Assessment Risk
Tool (HART) - UK
Assesses risk of repeat crimes

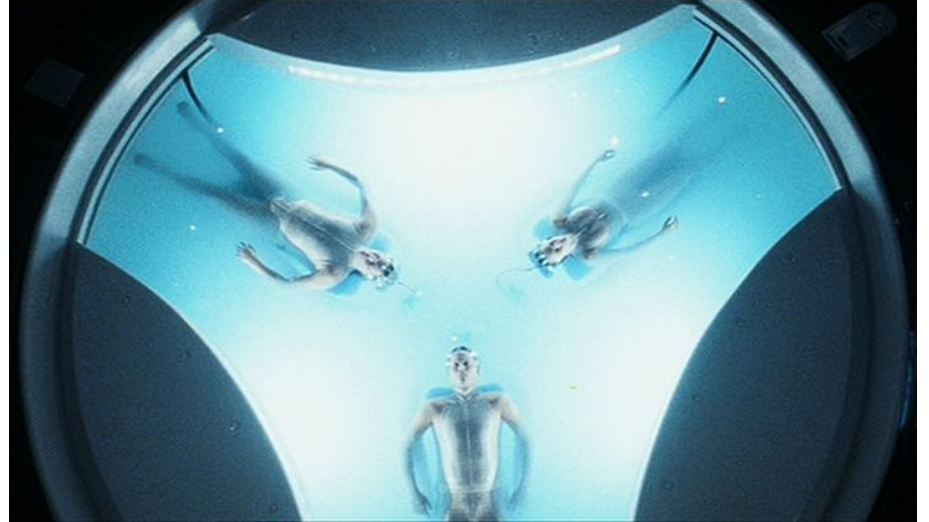
Angwin, J., Larson, J., Mattu, S. and Kirchner, L. (2016). Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks. Propublica. Available at: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>

Oswald, Marion and Grace, Jamie and Urwin, Sheena and Barnes, Geoffrey, Algorithmic Risk Assessment Policing Models: Lessons from the Durham HART Model and 'Experimental' Proportionality (August 31, 2017). Information & Communications Technology Law

MASS SURVEILLANCE

Correctional Offender Management Profiling for
Alternative Sanctions (COMPAS) – USA
Assesses risk of repeat crimes

Durham Constabulary's Harm Assessment Risk
Tool (HART) - UK
Assesses risk of repeat crimes



The Minority Report – Phillip K. Dick

Angwin, J., Larson, J., Mattu, S. and Kirchner, L. (2016). Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks. Propublica. Available at: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>

Oswald, Marion and Grace, Jamie and Urwin, Sheena and Barnes, Geoffrey, Algorithmic Risk Assessment Policing Models: Lessons from the Durham HART Model and 'Experimental' Proportionality (August 31, 2017). Information & Communications Technology Law

MASS SURVEILLANCE

Correctional Offender Management Profiling for
Alternative Sanctions (COMPAS) – USA
Assesses risk of repeat crimes

Durham Constabulary's Harm Assessment Risk
Tool (HART) - UK
Assesses risk of repeat crimes

Discriminates against **black people**

Discriminates against **poor people**

The Minority Report – Phillip K. Dick

Angwin, J., Larson, J., Mattu, S. and Kirchner, L. (2016). Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks. Propublica. Available at: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>

Oswald, Marion and Grace, Jamie and Urwin, Sheena and Barnes, Geoffrey, Algorithmic Risk Assessment Policing Models: Lessons from the Durham HART Model and 'Experimental' Proportionality (August 31, 2017). Information & Communications Technology Law

MASS SURVEILLANCE

This is a Problem for
Society as Whole

The screenshot shows a web browser displaying a news article. The browser's address bar contains the text "Search or enter website name". The article's main title is "The Cambridge Analytica Files" in a large, bold, yellow font. To the left of the title is a white icon of a padlock inside a hexagonal network structure. Below the title is a yellow banner with the text "A year-long investigation into Facebook, data, and influencing elections in the digital age". The article is organized into a "Key stories" section, which features several story cards. Each card has a portrait of a person at the top, followed by a headline in yellow and white text, and a short summary in white text on a dark background. The first large card features a man with red hair and a headline about 50 million Facebook profiles. Other smaller cards mention a Brexit whistleblower, Facebook's week of shame, and a former Cambridge Analytica executive speaking out. The page also includes a "Hide" button in the top right corner and a comment count of 266 at the bottom right.

The Cambridge Analytica Files

A year-long investigation into Facebook, data, and influencing elections in the digital age

Key stories

Hide

Revealed / 50 million Facebook profiles harvested for Cambridge Analytica in major data breach

484

The Brexit whistleblower / 'Did Vote Leave use me? Was I naive?'

Revealed: the ties that bound Vote Leave's data firm to controversial Cambridge Analytica

Facebook's week of shame / The Cambridge Analytica fallout

Speaking out / Former Cambridge Analytica exec

Revealed: Brexit insider claims Vote Leave team may have breached spending limits

Whistleblower alleges that electoral spending rules could have been manipulated over controversial donation and that Vote Leave 'tried to delete key evidence'

Politicians can't control the digital giants with rules drawn up for the analogue era

Andrew Rawnsley

266

Raid / Investigators spend seven hours at Cambridge

Facebook told me it would act swiftly on data misuse -

Richard Brautigan
(1967)

I like to think
(it has to be!)
of a cybernetic ecology
where we are free of our labors
and joined back to nature,
returned to our mammal
brothers and sisters,
and **all watched over
by machines of loving grace.**



Dave Millard (dem@ecs.soton.ac.uk)

[@hoosfoos](#)