Digital profiles

Răzvan Rughiniș

Main topics

1. Introduction. Why care about privacy?
2. **Digital profiles**
3. The ethical perspective. Fairness, harm, autonomy
4. The free market perspective (economics)
5. The cognitive perspective (psychological)
6. The interactional perspective (sociological)
7. Role: Users. Curation & Privacy-enhancing tools
8. Role: Experts. Whistleblowing & Collective action
9. Role: Policymakers. GDPR & Single Digital Market

Take away – Course 1

- Why?
  - Privacy is not cake: Tech is downgrading human autonomy
  - Why now? Emerging policies, investigations, NGO collective action
  - Who cares?
- Sensemaking: Four perspectives
  - Ethical | Free market | Cognitive | Interactional
- Taking action: Three roles
  - User | Expert | Policy-maker
- Privacy = choice in the new world order
  - 4th Industrial Revolution
  - Digital infrastructures & Platform capitalism
  - Surveillance capitalism

Outline – Course 2

- Illusion of control and Data vs. metadata
- Data flows are floods, not trickles
  - Legal harvesting at scale
  - Exposures & leaks
  - Data & China
- Digital profiles
- So what?
  - We are mined for time and attention
  - We are gently nudged in thought and action
  - We are replaced: automation
- Taking action
  - Critical technology analysis
  - Regulating tech, making tech & using tech

1. Illusion of control

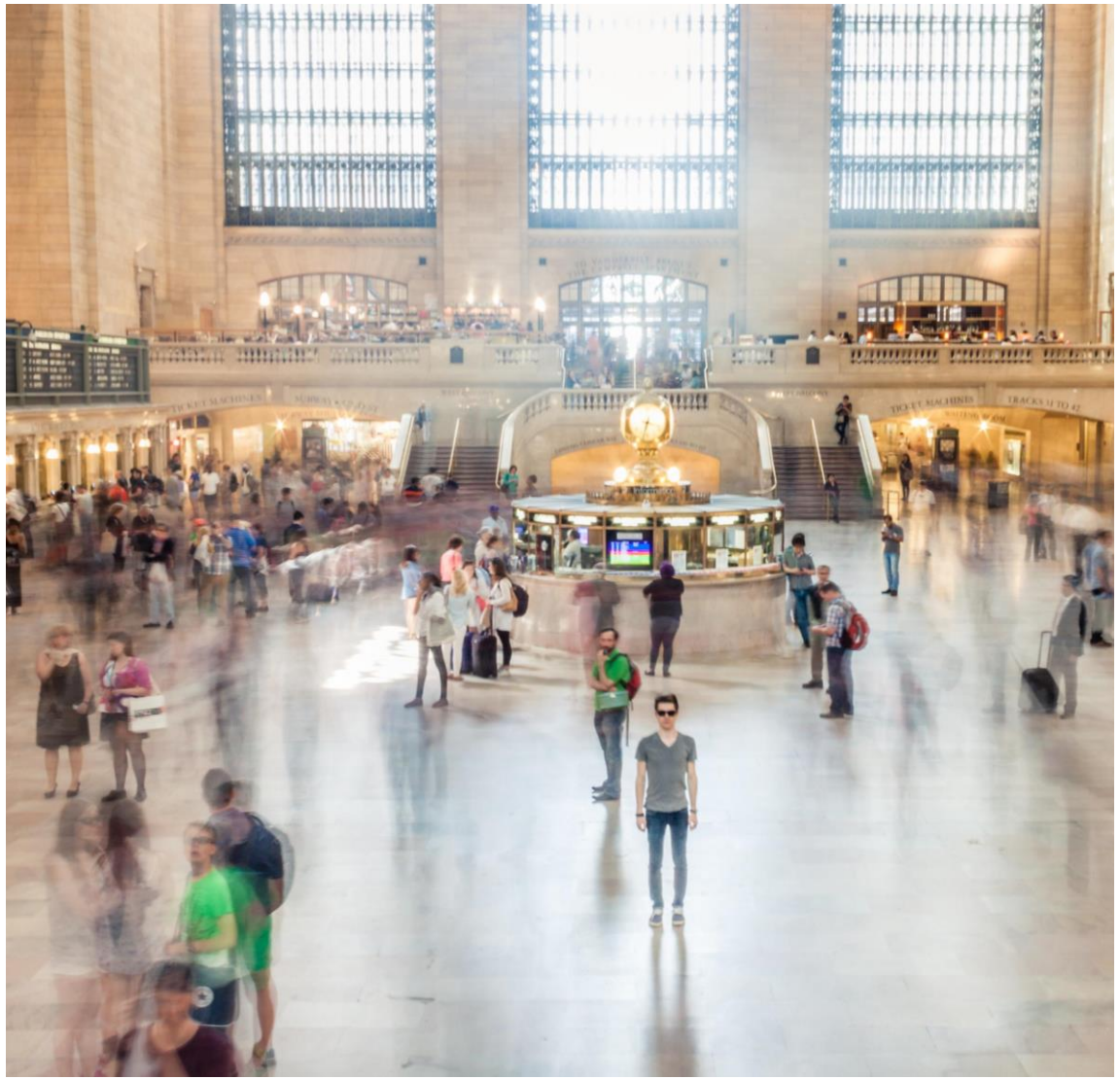
We are transparent

Illusion of control

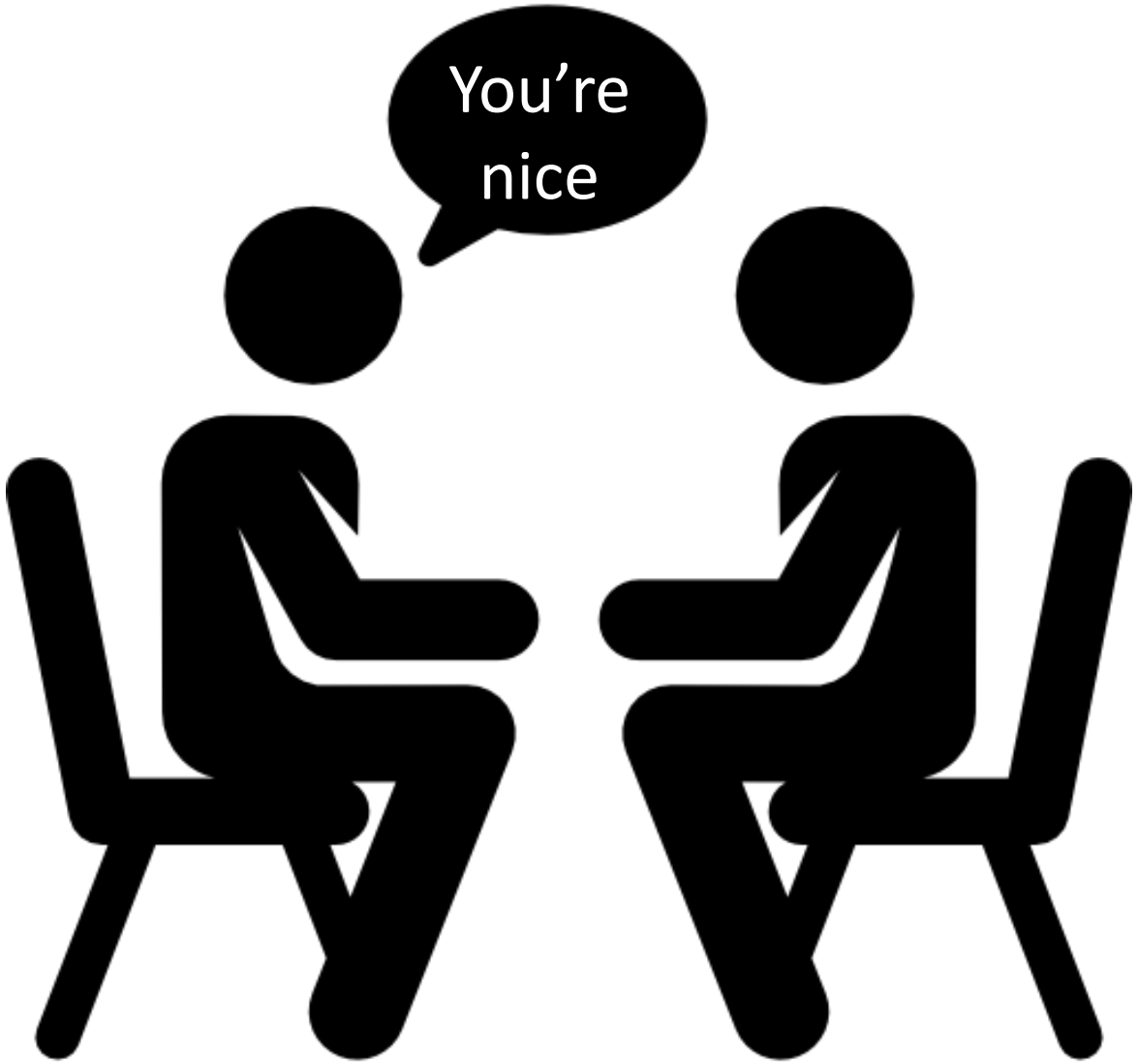
- We feel that we are largely in control of our digital traces
  - I know what data is collected about me
  - I can restrict data flows if I want

Illusion of anonymity

- We feel that we are practically anonymous
  - *Nobody cares specifically about me*
  - *I have nothing to hide*
  - *It's only metadata*
  - *It's only used for advertisement*
    - *„a small price to pay"*



Data



Metadata

Latitude: 44.434577
Longitude: 26.045211

+4072213456

https://www.youtube.com/watch?v=UdQiz0Vavmc

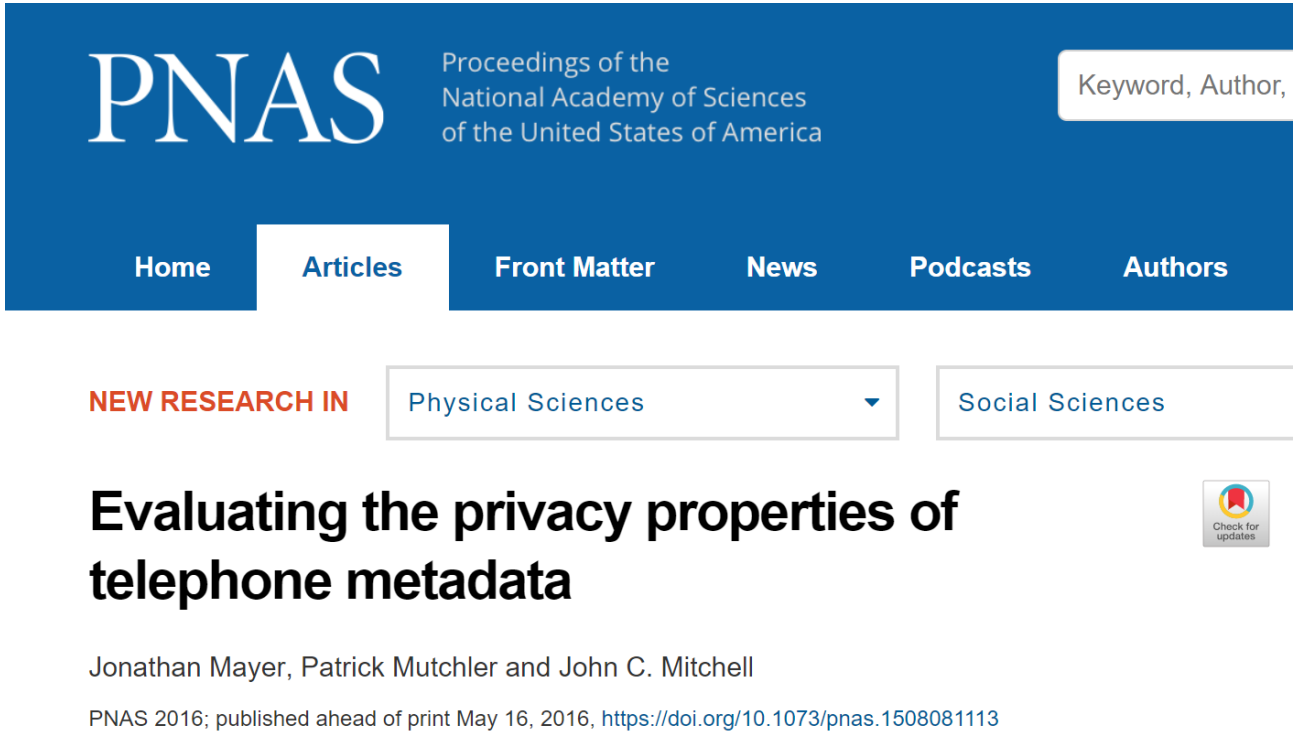
Michael Vincent Hayden is a retired United States Air Force four-star general and former Director of the National Security Agency and Director of the Central Intelligence Agency.

Former NSA boss: "We kill people based on metadata"

27,791 views

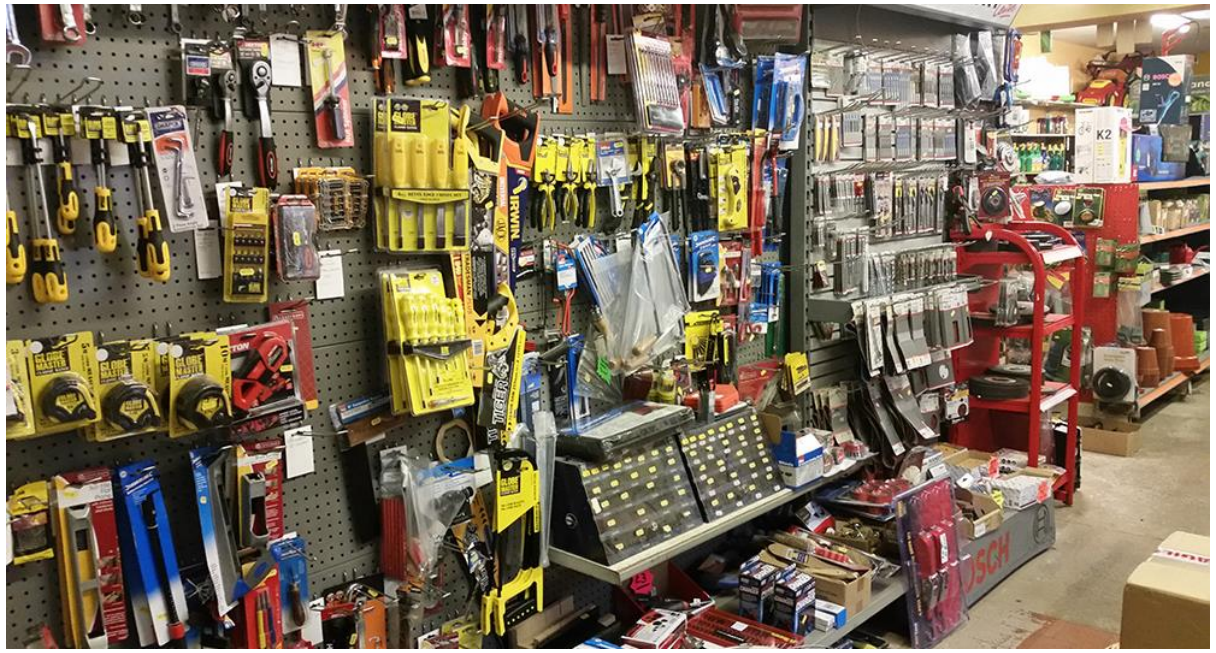
LIKE DISLIKE SHARE

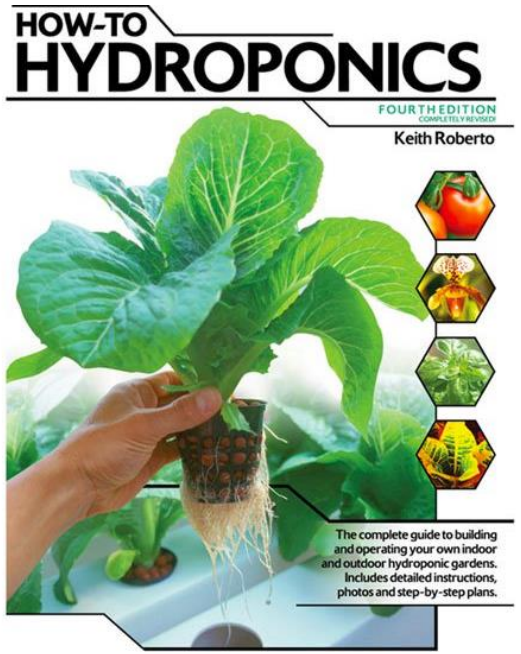
"Stanford computer scientists show telephone metadata can reveal surprisingly sensitive personal information", 2016



We find that telephone metadata is densely interconnected, can trivially be reidentified, enables automated location and relationship inferences, and can be used to determine highly sensitive traits.

“Participant D placed calls to a hardware outlet, locksmiths, a hydroponics store, and a head shop in under 3 weeks”




HOW-TO
HYDROPONICS
FOURTH EDITION
COMPLETELY REVISED
Keith Roberto
The complete guide to building and operating your own indoor and outdoor hydroponic gardens. Includes detailed instructions, photos and step-by-step plans.


NIRVANA
www.headshop.ie
MANAGEMENT RESERVE THE RIGHT TO REFUSE ADMISSION
STRICTLY OVER 18'S ONLY
PLEASE USE THE BELL!
USE BELL
LATE NIGHT OPENING THURSDAY FRIDAY SATURDAY
GROW SHOP
NOW OPEN

Invasion story 1

- Aim: To shock us into awareness
- Paul Dehaye requested his data from Amobee
- June 9 : “likely to suffer from overactive bladder”
- Prediction from The Weather Company on buying more drinks
  - “The overactive bladder [category] targets a mix of weather conditions that cause symptoms of overactive bladder to flare up, enabling advertisers to message when OAB is most likely to be top-of-mind for sufferers”

MyData 2019

PAUL-OLIVIER DEHAYE

PERSONALDATA.IO, DIRECTOR

http://www.dehaye.org

Financial Times 2019

Failing intuitions of disclosure and fair exchange

- We have a keen sense of privacy in interpersonal relations
  - We know what to disclose and what to hide
  - But: how do we deal with ‘friends’, versus friends?
- We assess costs and benefits
  - Is it a balanced transaction for our data vs. what we receive?
  - Strong asymmetry of power and knowledge
    - Google, Amazon, Uber vs. a regular user

2. Data flows

Trickle or deluge?

A flow of privacy scandals

- Users' data is harvested aggressively
  - Apps collect it **legally**, under the shield of T&C
  - Apps collect it in the **shadows**
- **Involuntary** disclosures
- Security **breaches**
  - Huge unsecured datasets
  - Attacks
- Data is **traded** & **consolidated**

Legal harvesting at scale

MIT Technology Review

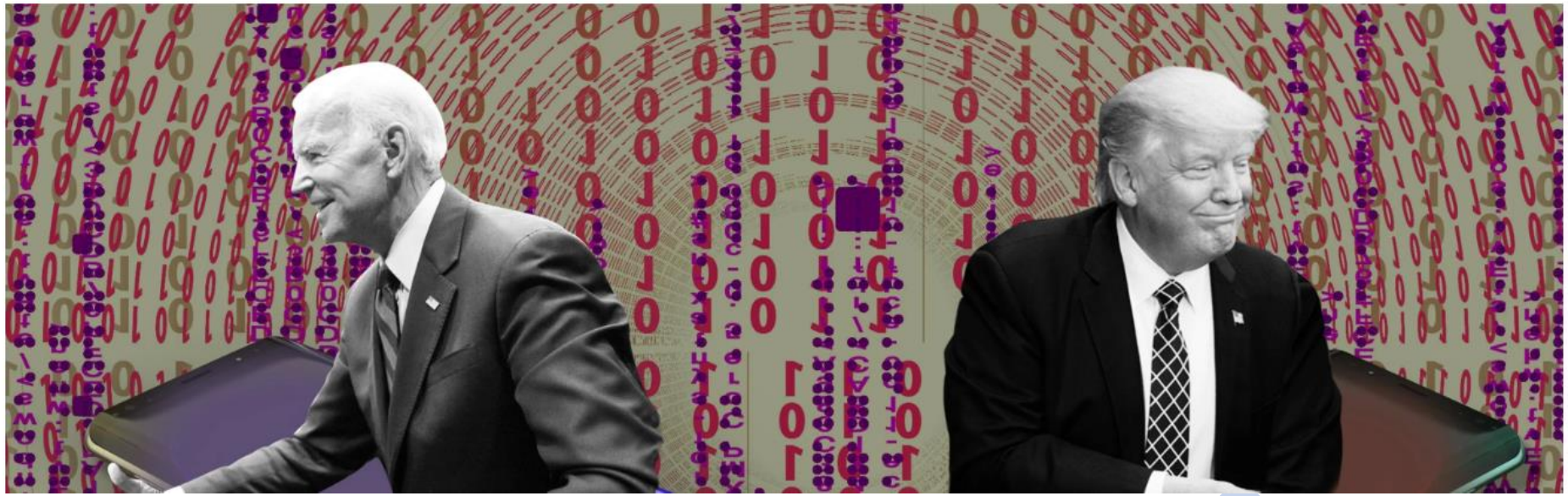
Election 2020

The Trump 2020 app is a voter surveillance tool of extraordinary power

Both presidential campaigns use apps to capture data, but Trump's asks to scoop up your identity, your location, and control of your phone's Bluetooth function.

by **Jacob Gursky** and **Samuel Woolley**

June 21, 2020



MIT Technology Review

“For political movements revolving around a charismatic, illiberal leader, the shift to individualized apps that blur the line between government and private communication is the next step toward independence from both the “mainstream media” and the social-media platforms that allowed them to create a fact-agnostic communication channel in the first place”

THE WALL STREET JOURNAL.

You Give Apps Sensitive Personal Information. Then They Tell Facebook.

Wall Street Journal testing reveals how the social-media giant collects a wide range of private data from developers; 'This is a big mess'

By Sam Schechner and Mark Secada

Feb. 22, 2019 11:07 am ET

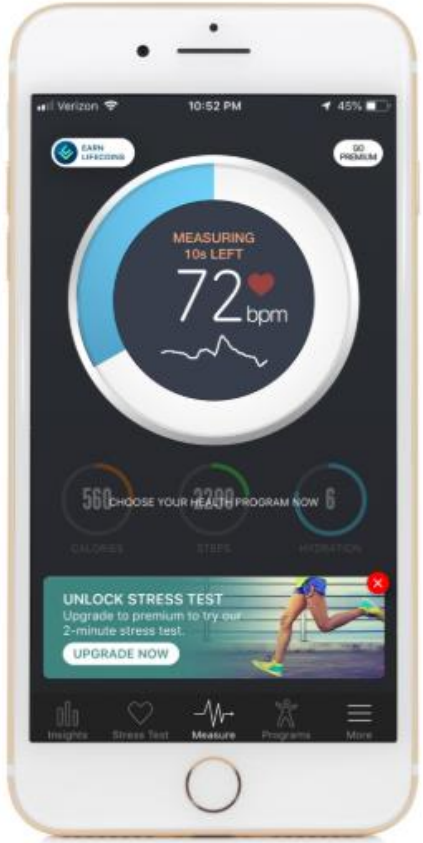
SAVE SHARE TEXT 614 RESPONSES

Millions of smartphone users confess their most intimate secrets to apps, including when they want to work on their belly fat or the price of the house they checked out last weekend. Other apps know users' body weight, blood pressure, menstrual cycles or pregnancy status.

Unbeknown to most people, in many cases that data is being shared with someone else: Facebook Inc. FB -2.05% ▼

The social-media giant collects intensely personal information from many popular smartphone apps just seconds after users enter it, even if the user has no connection to Facebook, according to testing done by The Wall Street Journal. The apps often send the data without any prominent or specific disclosure, the testing showed.

WSJ, 2019



In the Journal's testing, Instant Heart Rate: HR Monitor sent a user's heart rate to Facebook.

In the Journal's testing, Flo Period & Ovulation Tracker told Facebook when a user was having her period.

In the Journal's testing, Realtor.com sent Facebook the location and price of listings that a user viewed.

PHOTOS: AZUMIO INC.; FLO HEALTH INC.; MOVE INC.; APPLE

WSJ, 2019

Spotify's Big Data Scandal: Outcry Against Intruding “Privacy” Policy

Published on August 26, 2015

Bernard Marr in fluencer | + Follow
Internationally best-selling author; keynote speaker; leading business, t...
571 articles

514 93 1

News

Pokémon GO privacy policy updated, now allows collecting information about other apps installed on your device

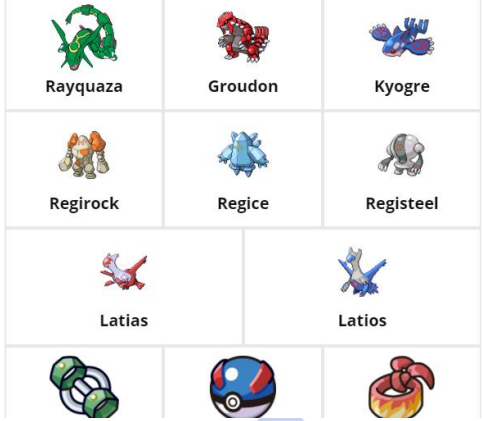
By **Zeroghan** - November 2, 2017

Trainers,

the in-game privacy policy has been updated and now allows collecting information about other applications installed on your device. This change is applicable from November 1, 2017. If you open your app and scroll down to the *"Device information"* section, you will see that a new statement has been added:

> ***...information about other applications installed on your (or your authorized child's) device...***

Generation III



TECH

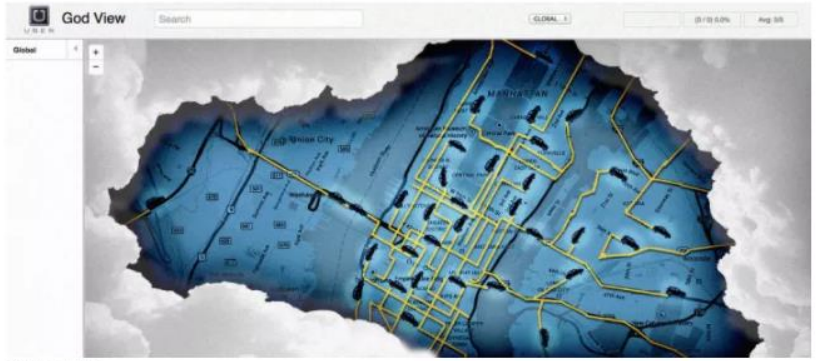
"God View": Uber Investigates Its Top New York Executive For Privacy Violations

In the wake of a BuzzFeed News story, the transit company is looking into the official's tracking of a journalist's location.

Posted on November 19, 2014, at 5:27 a.m.


Johana Bhuiyan
BuzzFeed News Reporter


Charlie Warzel
BuzzFeed News Reporter



BuzzFeed News

Uber said Tuesday that it is investigating its top New York executive for tracking a BuzzFeed News reporter without her permission in violation of what the transit giant says has long been its privacy policy. The company also published its privacy policy for the first time on Tuesday, though it said the policy had always been in effect.

2017 Proceedings of the Conference on Information Systems Applied Research
Austin, Texas USA

ISSN: 2167-1508
v10 n4511

Geolocation Tracking and Privacy Issues Associated with the Uber Mobile Application

Dr. Darren R. Hayes
Pace University
dhayes@pace.edu
Sapienza Università di Roma
darren.hayes@uniroma1.it

Christopher Snow
csnow@pace.edu

Saleh Altuwayjiri
sa07549n@pace.edu

Pace University
New York, NY

"It is clear that Uber is not just saving trip locations from completed rides, they are collecting geolocation data when the app is not being used for a ride and, more interestingly, is being used to monitor rides with competing services."

Exposures & hacks

Invasion story 2

TECHNOLOGY

A Face Is Exposed for AOL Searcher No. 4417749

By MICHAEL BARBARO and TOM ZELLER Jr. AUG. 9, 2006

Thelma Arnold's identity was betrayed by AOL records of her Web searches, like ones for her dog, Dudley, who clearly has a problem.
Erik S. Lesser for The New York Times

Buried in a list of 20 million Web search queries collected by AOL and recently released on the Internet is user No. 4417749. The number was assigned by the company to protect the searcher's anonymity, but it was not much of a shield.

No. 4417749 conducted hundreds of searches over a three-month period on topics ranging from "numb fingers" to "60 single men" to "dog that urinates on everything."

And search by search, click by click, the identity of AOL user No. 4417749 became easier to discern. There are queries for "landscapers in Lilburn, Ga," several people with the last name Arnold and "homes sold in shadow lake subdivision gwinnett county georgia."

It did not take much investigating to follow that data trail to Thelma Arnold, a 62-year-old widow who lives in Lilburn, Ga., frequently researches her friends' medical ailments and loves her three dogs. "Those are my searches," she said, after a reporter read part of the list to her.

Home About

Nathan Ruser
@Nrg8000

Influencing Australian and American National Security Policy since 2018. Monitoring a number of conflicts, especially Syria and Iraq I don't know cyber.

Nathan Ruser
@Nrg8000

Follow

Strava released their global heatmap. 13 trillion GPS points from their users (turning off data sharing is an option). medium.com/strava-enginee ... ... It looks very pretty, but not amazing for Op-Sec. US Bases are clearly identifiable and mappable

10:24 AM - 27 Jan 2018

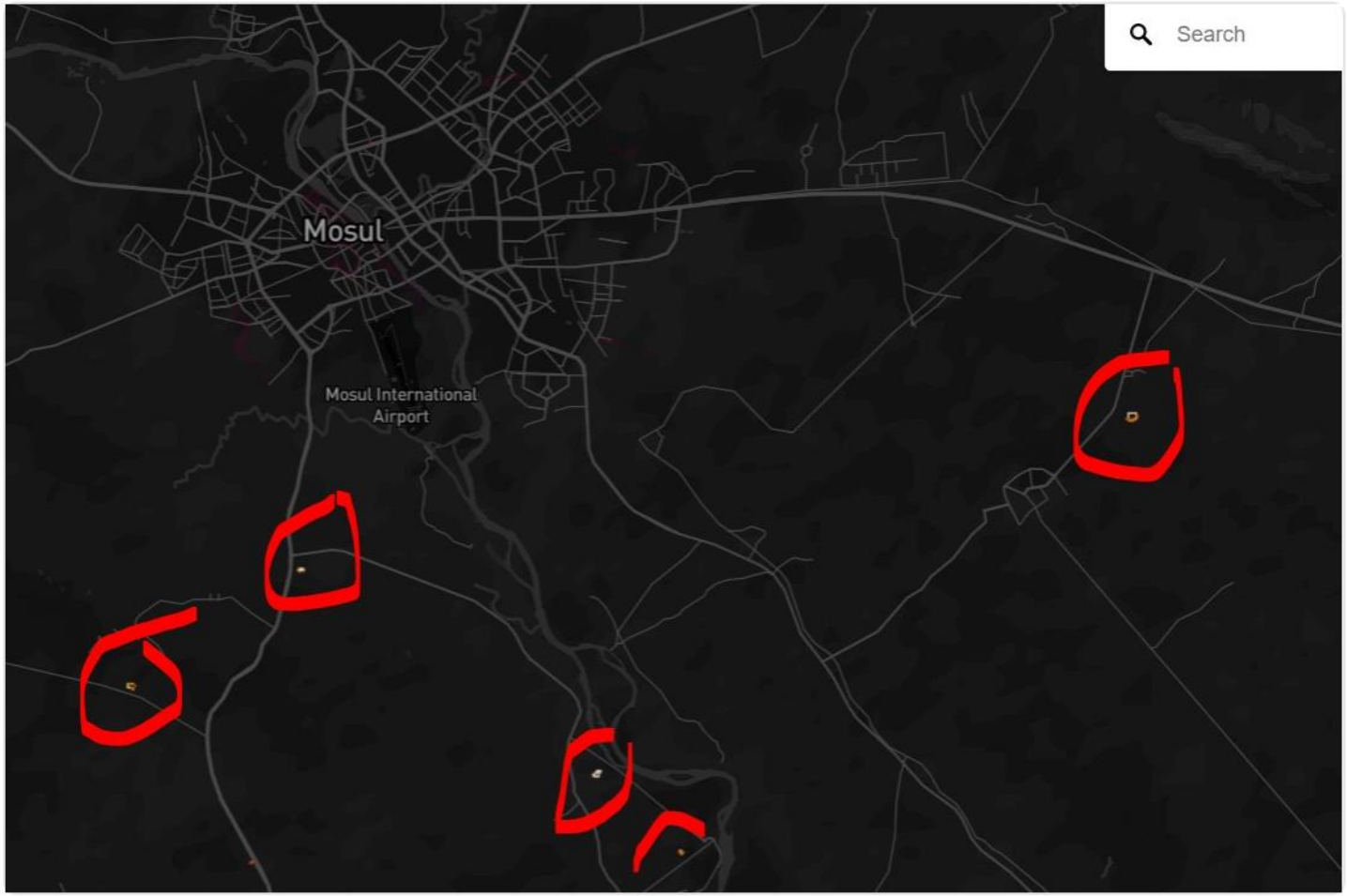
Tobias Schneider
@tobiaschneider

Sweating the small wars at @GPPi · National Security and Middle East Policy · schneider.tbs@gmail.com

5 87 616

Tobias Schneider @tobiaschneider · Jan 27

So much cool stuff to be done. Outposts around Mosul (or locals who enjoy running in close circles around their houses):



GPS

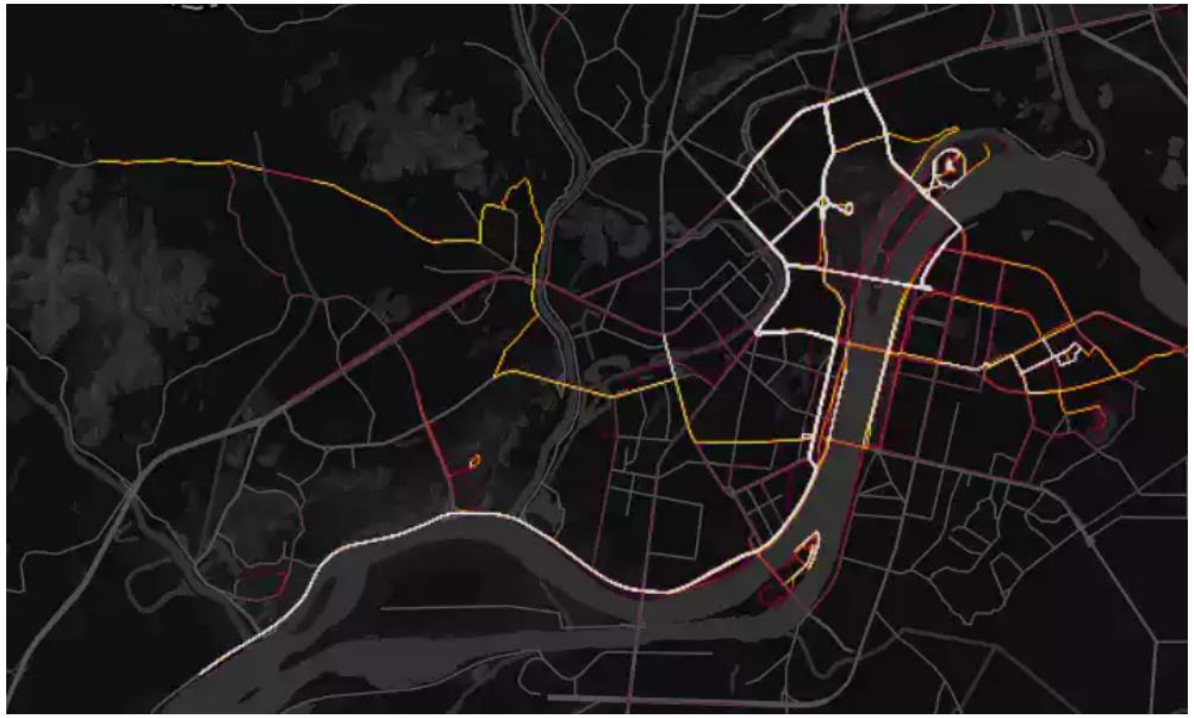
Strava suggests military users 'opt out' of heatmap as row deepens

Fitness-tracking company suggests secret army base locations were made public by users, while militaries around world weigh up ban

Alex Hern

@alexhern

Mon 29 Jan 2018 10.46 GMT



A Strava heatmap displaying the centre of Pyongyang, North Korea. Photograph: Strava heatmap

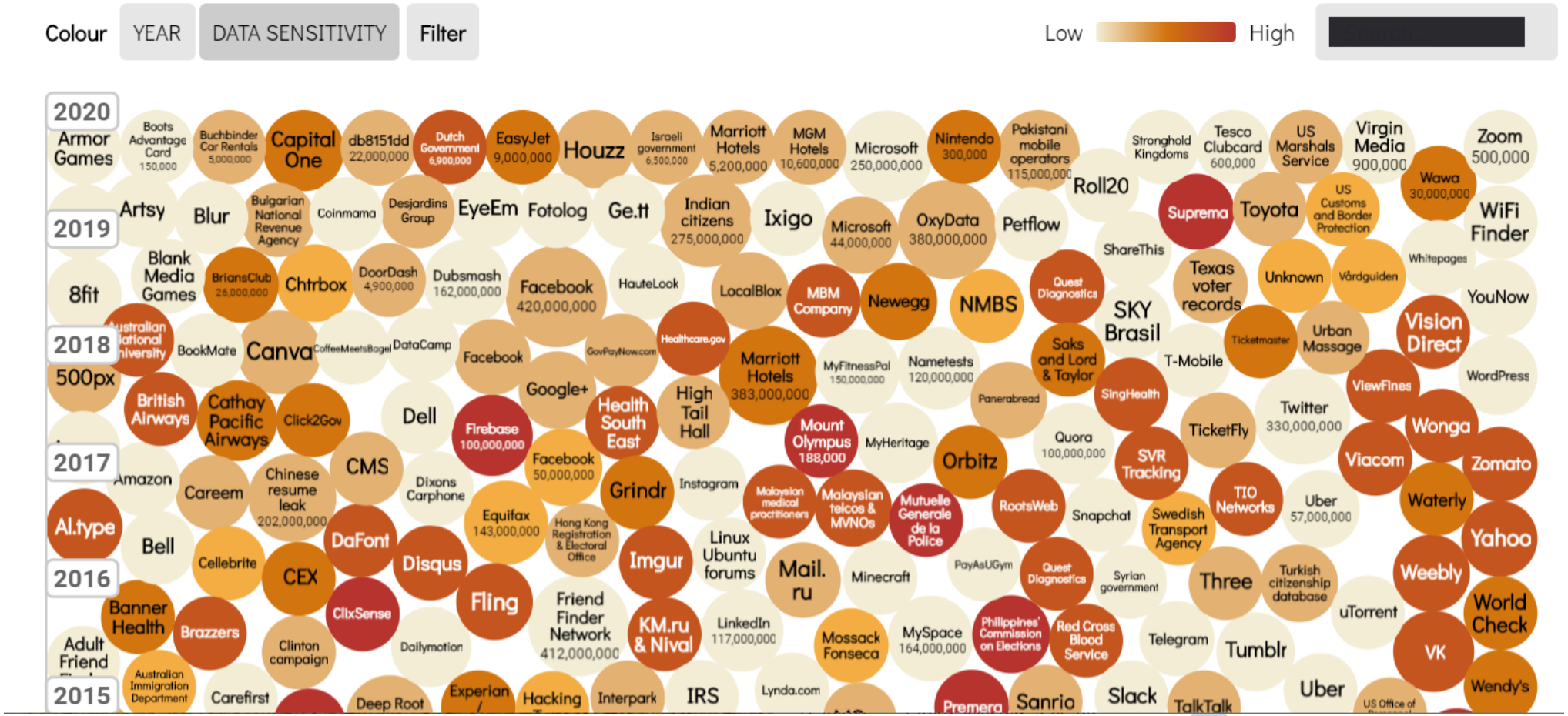
Fitness-tracking company Strava has defended its publication of heatmaps that accidentally reveal sensitive military positions, arguing that the information was already made public by the users who uploaded it.

Following the revelations, militaries around the world are contemplating bans on fitness trackers to prevent future breaches. As well as the location of military bases, the identities of individual service members can also be uncovered, if they are using the service with the default privacy settings.

World's Biggest Data Breaches & Hacks

Select losses greater than 30,000 records

Last updated: 11th May 2020



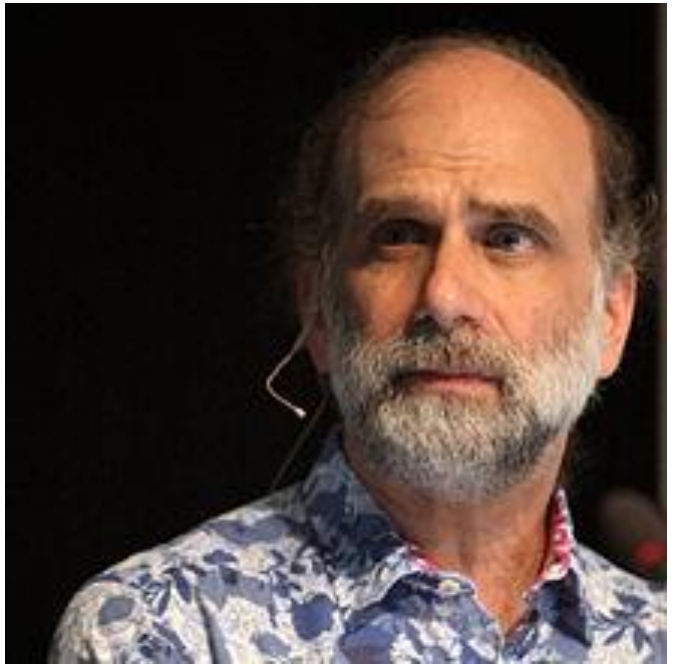
https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

How to factor in…

- Size: Big, Big Data
- Diversity (on-line & off-line)
  - Cookies, card payments, health etc.
- Longitudinal tracking (all your life)
- Data vs. Metadata
- In the shadows
  - Evolving legal surveillance
  - Evolving borderline & abusive surveillance
  - Accumulating data breaches

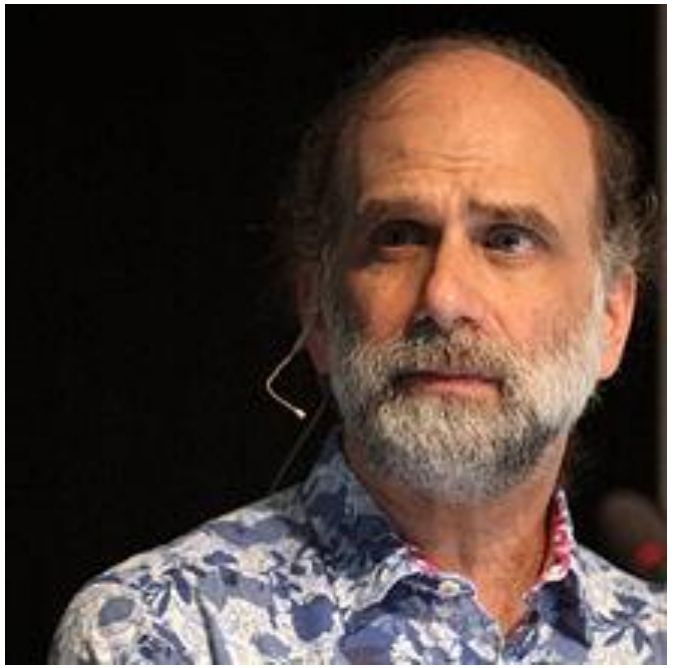
Bruce Schneier: InternetPlus

- „Last year, when my refrigerator broke, the serviceman replaced the computer that controls it. I realized that I had been thinking about the refrigerator backwards: it's not a refrigerator with a computer, it's a computer that keeps food cold." (2015)



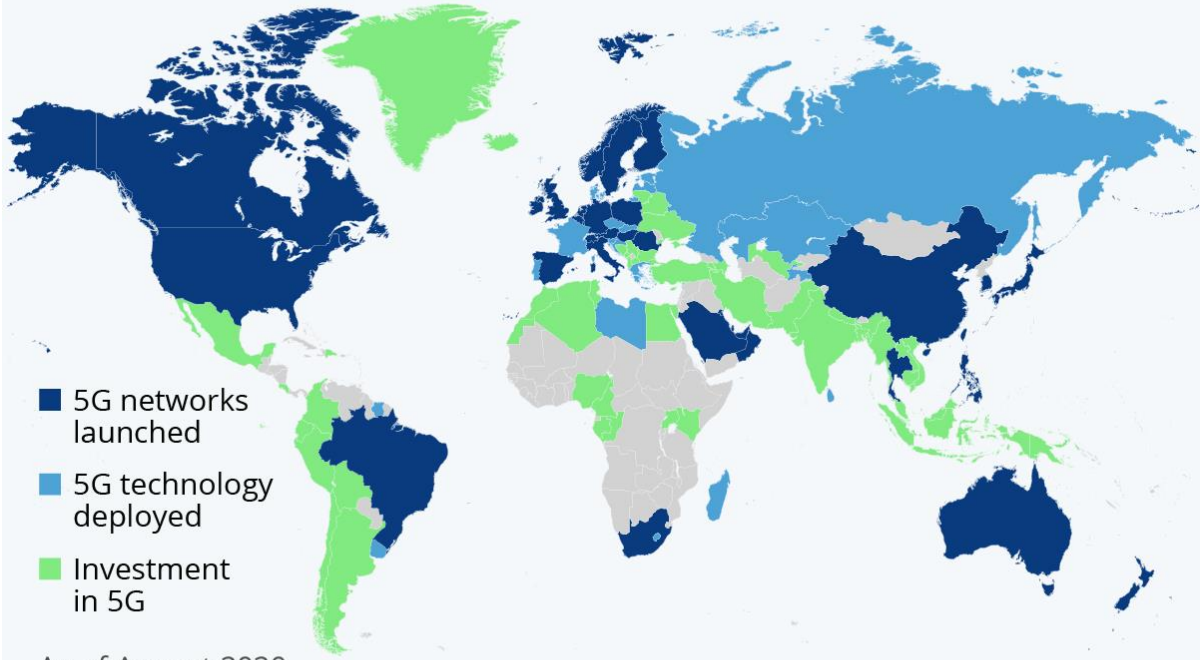
Bruce Schneier: InternetPlus

- The Internet of toasters and refrigerators and thermostats and cars, that's a big part of what I'm talking about, but it's not just that. It's also the Internet of Facebook and power plants and national security and elections and everything else. So I wanted one word to encompass everything. And oddly enough there isn't one. And that might be part of the problem because we're not conceptualizing this as one big complex system. (2018)



Where 5G Technology Has Been Deployed

Countries where 5G networks/technology have been deployed and where 5G investments have been made



As of August 2020

Source: GSA 5G Market Snapshot

statista


Data & China

Zoom

- Headquartered in the US
- The Zoom app appears to be developed by three companies in China, which all have the name 软视软件 (“Ruanshi Software”).
- Two of the three companies are owned by Zoom, and one is owned by an entity called 美国云视频软件技术有限公司 (“American Cloud Video Software Technology Co., Ltd.”)
- 700 employees in China

Marczak & Railton, April 2020

Figure 1: A picture shows the Zoom logo above the name of one of Zoom’s Chinese developer companies, “Ruanshi Software (Suzhou) Ltd.” (Source)

Grindr

- Chinese gaming company Beijing Kunlun Tech Co agreed to sell Grindr LLC, a popular gay dating app it acquired in 2016, for about $608.5 million
- The deal comes after the Committee on Foreign Investment in the United States (CFIUS) asked Kunlun to divest itself of Grindr
- the United States has been increasingly scrutinizing app developers over the safety of personal data they handle, especially if some of it involves U.S. military or intelligence personnel

Reuters, March 2020

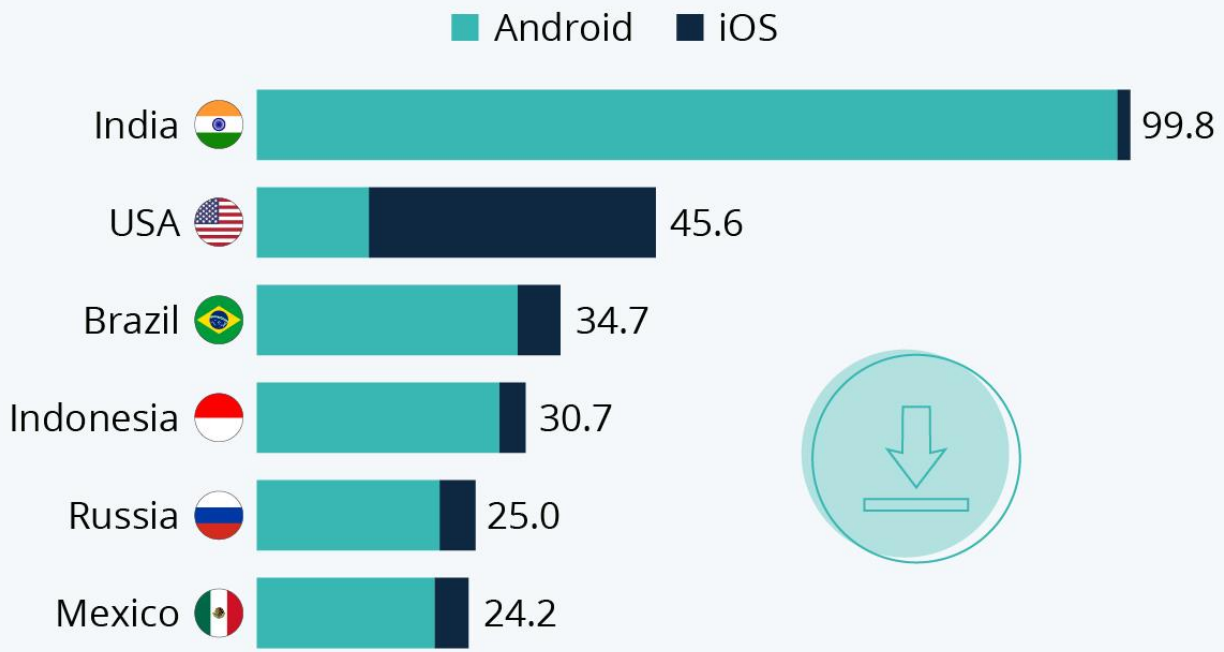
TikTok (ByteDance)

- “Defining social media app of Gen Z”
- Censoring videos that mention the Uighurs, Tiananmen Square, Tibetan independence, or Falun Gong (Washington Post, The Guardian, sept. 2019)
- Oracle&Walmart deal (ArsTehnica 2020)
  - Oracle will hold a 12.5 % stake in TikTok Global at its inception and will also serve as the cloud hosting provider
  - Walmart will hold another 7.5% stake.
  - The remaining 80%: ByteDance

Feroza Aziz and the Uighur viral video

Where TikTok Has Been Downloaded the Most

Number of TikTok downloads in 2020, by operating system (in millions)



Based on figures for 55 countries as of June 30, 2020.
Source: Priori Data

Facial recognition data

- Adam Harvey: project Megapixels
- Microsoft pulls off MS Celeb – the largest facial recognition database (2019)
  - Used by Chinese companies (SenseTime and Megvii)
- Duke MTMC (Duke University) and Brainwash (Stanford University) also taken offline

Microsoft quietly deletes largest public face recognition data set

Stanford and Duke universities also remove facial recognition data

Facial recognition technology is demonstrated at an exhibition in Fujian province, China © Reuters

Project Megapixels

- “several computer vision image datasets created by US companies and universities were unexpectedly also used for research by the National University of Defense Technology in China, along with top Chinese surveillance firms including SenseTime, SenseNets, CloudWalk, Hikvision, and Megvii/Face++ which have all been linked to oppressive surveillance in the Xinjiang region of China”

An image from the MegaFace face recognition training dataset taken from the U.S. Embassy of Madrid Flickr account

TRANSNATIONAL FLOWS OF FACE RECOGNITION IMAGE TRAINING DATA

Project Megapixels

Project Megapixels

- Over 24 million non-cooperative, non-consensual photos in 30 publicly available face recognition and face analysis datasets
  - Over 15 million face images are from Internet search engines, over 5.8 million from Flickr.com,
  - over 2.5 million from the Internet Movie Database (IMDb.com)
  - nearly 500,000 from CCTV footage
  - Over 6,000 of the images were from US, British, Italian, and French embassies (mostly US embassies)
- All images were collected without any explicit consent ("in the wild“)
- Only about 25% of the citations are from the United States while the majority are from China

Project Megapixels

The New York Times

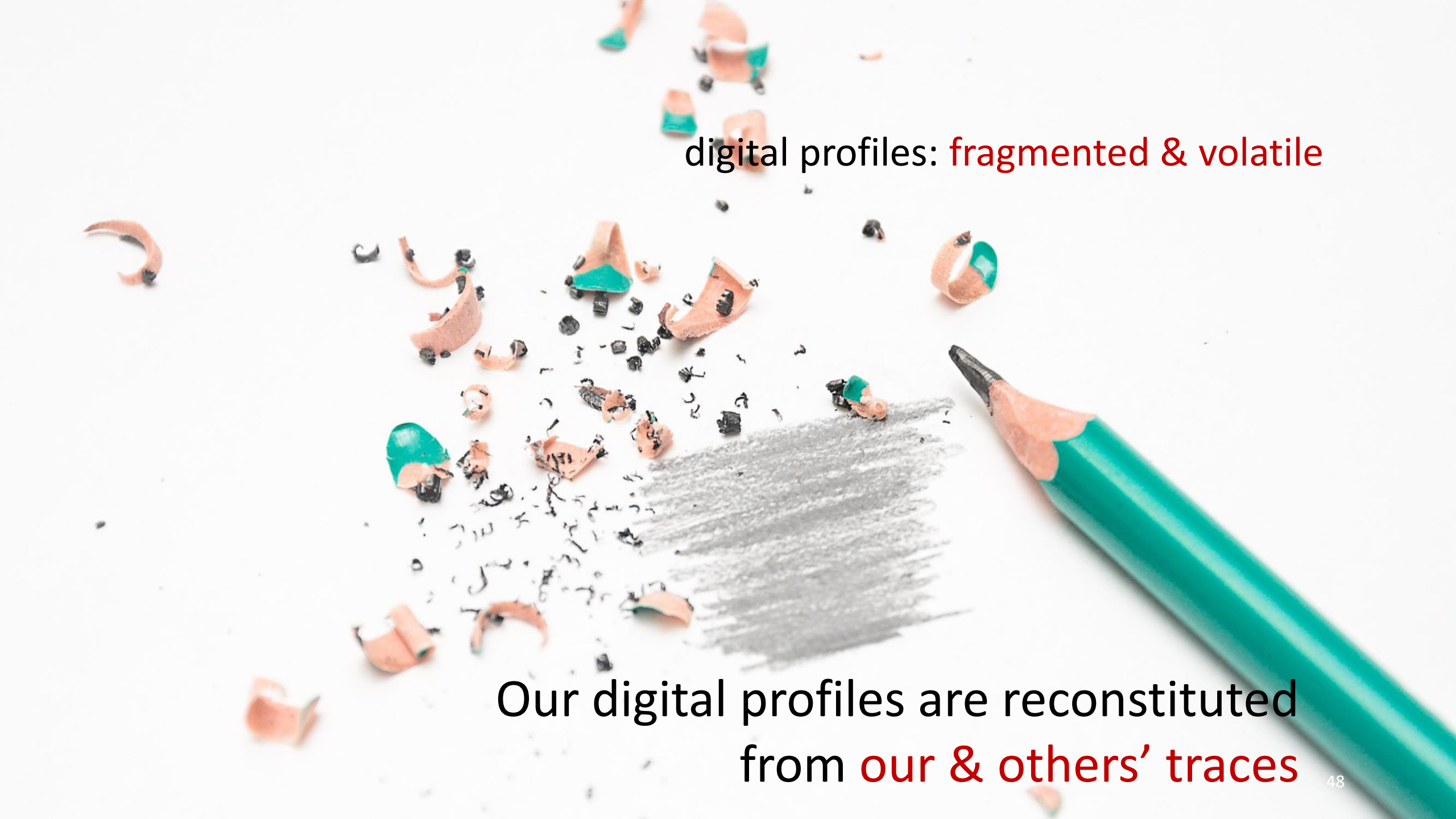
India Bans Nearly 60 Chinese Apps, Including TikTok and WeChat

The move is part of the tit-for-tat retaliation after the Indian and Chinese militaries clashed earlier this month.

Filming a TikTok video in Hyderabad, India, in February. Noah Seelam/Agence France-Presse — Getty Images

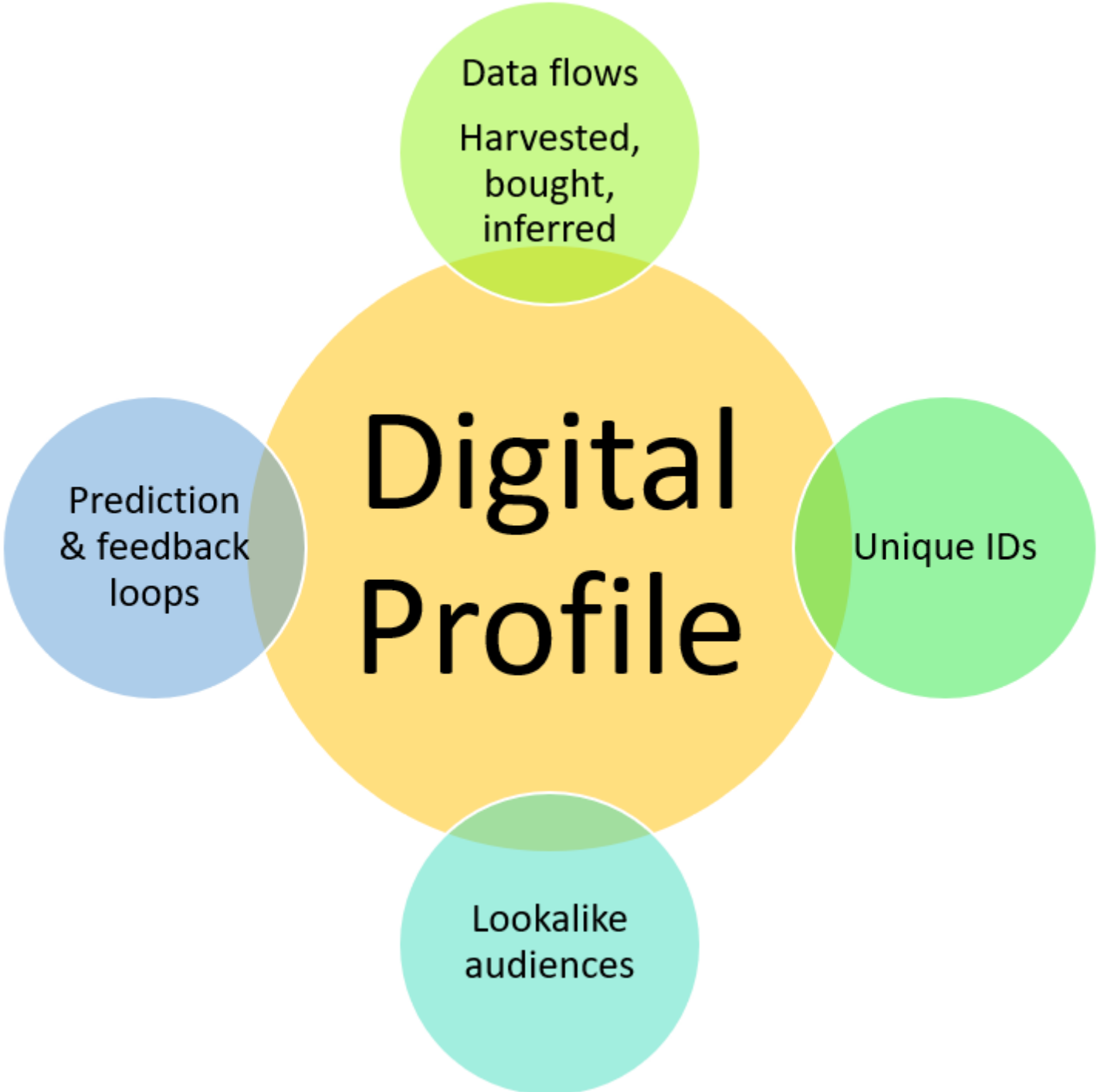
June 29, 2020

3. Digital profiles



digital profiles: fragmented & volatile

Our digital profiles are reconstituted from our & others' traces


Data flows
Harvested, bought, inferred
Prediction & feedback loops
Digital Profile
Unique IDs
Lookalike audiences

Apps

- The ten apps were observed transmitting user data to at least 135 different third parties involved in advertising and/or behavioural profiling.
- The Android Advertising ID, which allows companies to track consumers across different services, was transferred to at least 70 different third parties
- Other shared data: IP address and GPS location of the user, personal attributes including gender and age, and various user, activities

OUT OF CONTROL

How consumers are exploited by the online advertising industry

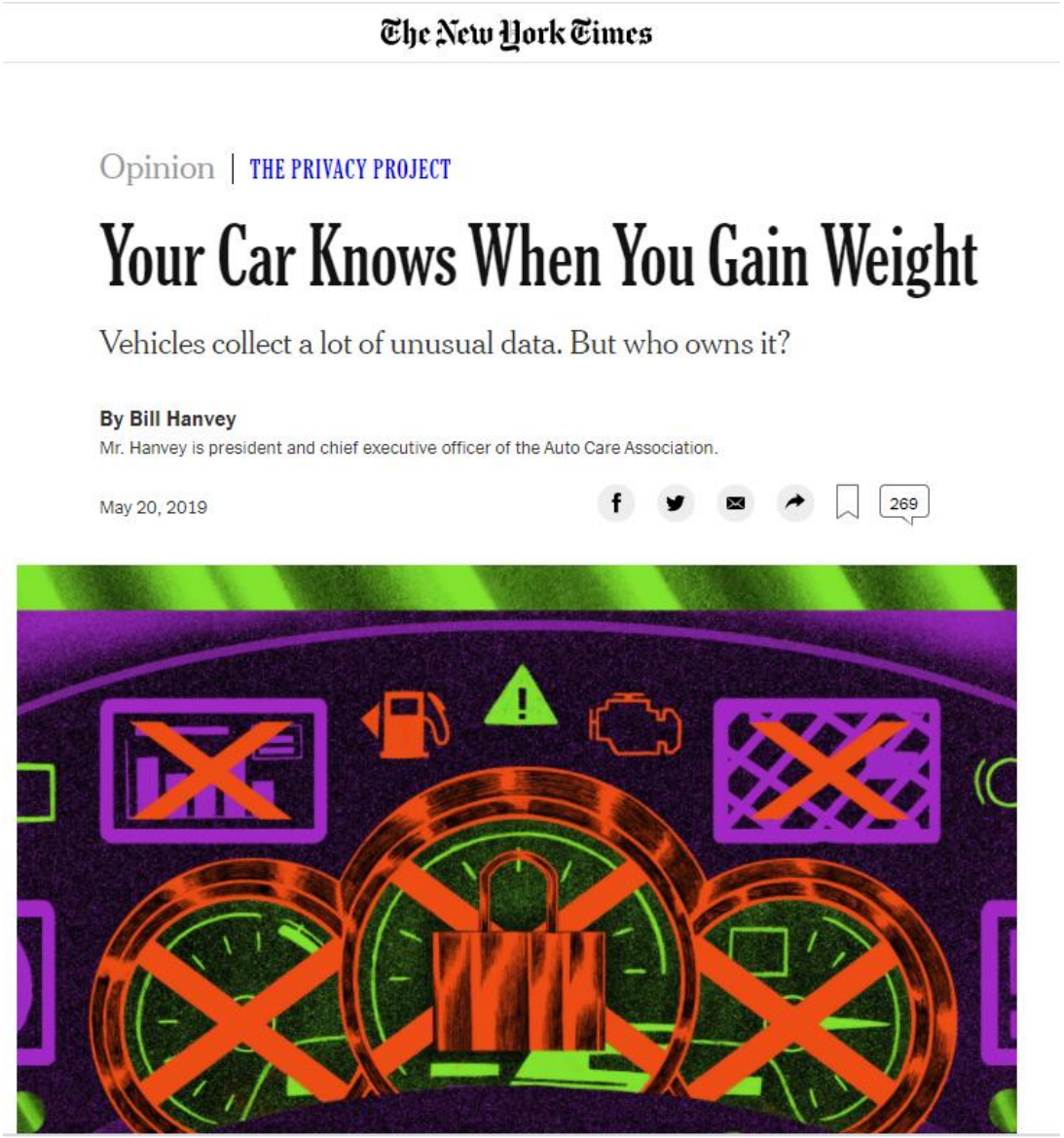
Norwegian Consumer Council 2020

App	Summary of findings
Clue	Sends birth year to **Amplitude**, **Apptimize**, and **Braze**. Sends Advertising ID to **Adjust**, **Amplitude**, and **Facebook**.
Grindr	Sends GPS coordinates to **AdColony**, **Braze**, **Bucksense**, **MoPub**, **OpenX**, **Smaato**, **PubNative**, **Vungle**, and others. Sends the IP address to **AppNexus** and **Bucksense**, and information about "relationship type" to **Braze**. Sends Advertising ID to all of these third parties and others, except **Braze.**
Happn	Sends country, gender and age segment of the user to **Google**. Sends Advertising ID to **Adjust** and **Facebook**.
Muslim: Qibla Finder	Sends IP address to **Appodeal**. Sends Advertising ID to **AppLovin**, **Appodeal**, **Facebook**, and **Liftoff**.
My days	Sends GPS coordinates and Wi-Fi access point information to **Neura**, **Placed**, and **Placer**. Sends IP address and a list of installed apps on the phone to **Placed**. Sends Advertising ID to **AppLovin**, **Liftoff**, **Google**, **Ogury Presage**, and **Placed**.
My Talking Tom 2	Sends IP address to **Mobfox**, **PubNative**, and **Rubicon Project**. Sends Advertising ID to **AppsFlyer**, **AppLovin**, **Facebook**, **IQzone**, **ironSource**, **Mobfox**, **Outfit7**, and **Rubicon Project**.
OkCupid	Sends GPS coordinates and answers to personal questions to **Braze**. Sends detailed device information to **AppsFlyer**. Sends Advertising ID to **AppsFlyer**, **Facebook** and **Kochava**.
Perfect365	Sends various location data such as GPS coordinates and Wi-Fi access point information to **Fysical**, **Safegraph**, and **Vungle**. Sends GPS coordinates unencrypted to **Receptiv**. Sends Advertising ID to **Amazon**, **Chocolate**, **Facebook**, **Fluxloop**, **Fyber**, **Fysical**, **InMobi**, **Inner-Active**, **Ogury Presage**, **Safegraph**, **Receptiv**, **Unacast**, **Unity3d**, and **Vungle**.
Tinder	Sends GPS position and "target gender" to **AppsFlyer** and **LeanPlum**. Sends Advertising ID to **AppsFlyer**, **Branch**, **Facebook**, and **Salesforce** (**Krux**).
Wave Keyboard	Sends Advertising ID to **Crashlytics**, **Facebook**, **Flurry**, **OneSignal**.

Norwegian Consumer Council 2020

Cars

- Cars not only know how much we weigh but also track how much weight we gain. They know how fast we drive, where we live, how many children we have — even financial information. Connect a phone to a car, and it knows who we call and who we text.
- But who owns and, ultimately, controls that data? And what are carmakers doing with it?


The New York Times

Opinion | THE PRIVACY PROJECT

Your Car Knows When You Gain Weight

Vehicles collect a lot of unusual data. But who owns it?

By Bill Hanvey

Mr. Hanvey is president and chief executive officer of the Auto Care Association.

May 20, 2019

269

Hanvey 2019, NY Times The Privacy Project

THE PRIVACY PROJECT

Companies and governments are gaining new powers to follow people across the internet and around the world, and even to peer into their genomes. The benefits of such advances have been apparent for years; the costs — in anonymity, even autonomy — are now becoming clearer. The boundaries of privacy are in dispute, and its future is in doubt. Citizens, politicians and business leaders are asking if societies are making the wisest tradeoffs. The Times is embarking on this monthslong project to explore the technology and where it's taking us, and to convene debate about how it can best help realize human potential.

Our digital profiles | 1

- Accumulated traces in Big Datasets processed by ML
  - Incomplete but inferred
  - Consolidated / enriched data
  - Anonymous but predictive
- Lookalike audiences
  - Half individual, half collective

Our digital profiles | 2

- “Quantcast knows a lot about you – even if you know nothing about Quantcast” (Privacy International - PI)
- Composed of:
  - Thousands (?) of data points
  - Long lists of events – ex. websites we visited
  - Declared & inferred socio-demographic and geographic categories
    - Gender, age, income, household structure, zip code
  - Declared & inferred lifestyle labels
  - Some true, some approximative, some false
- Basis for prediction & intervention
- Basis for decisions about us

Our digital zombie persona

PI Lead Frederike Kaltheuner

- “More than 600 apps had access to my iPhone data” (BBC interview)
- “Over the course of a single week, Quantcast has amassed over 5300 rows and more than 46 columns worth of data including URLs, time stamps, IP addresses, cookies IDs, browser information and much more” (PI investigation)

Invasion story 3

- “Uncannily specific”
- Predicted: gender, age, number of children and their ages, education level, and gross yearly household income
- Travel and leisure to Canada
- Frequent transactions in Bagel Restaurants
- City Prosperity:World-Class Wealth
- Alcohol at Home Heavy Spenders
- Baby Nappies & Wipes
  - “wrong, very wrong”

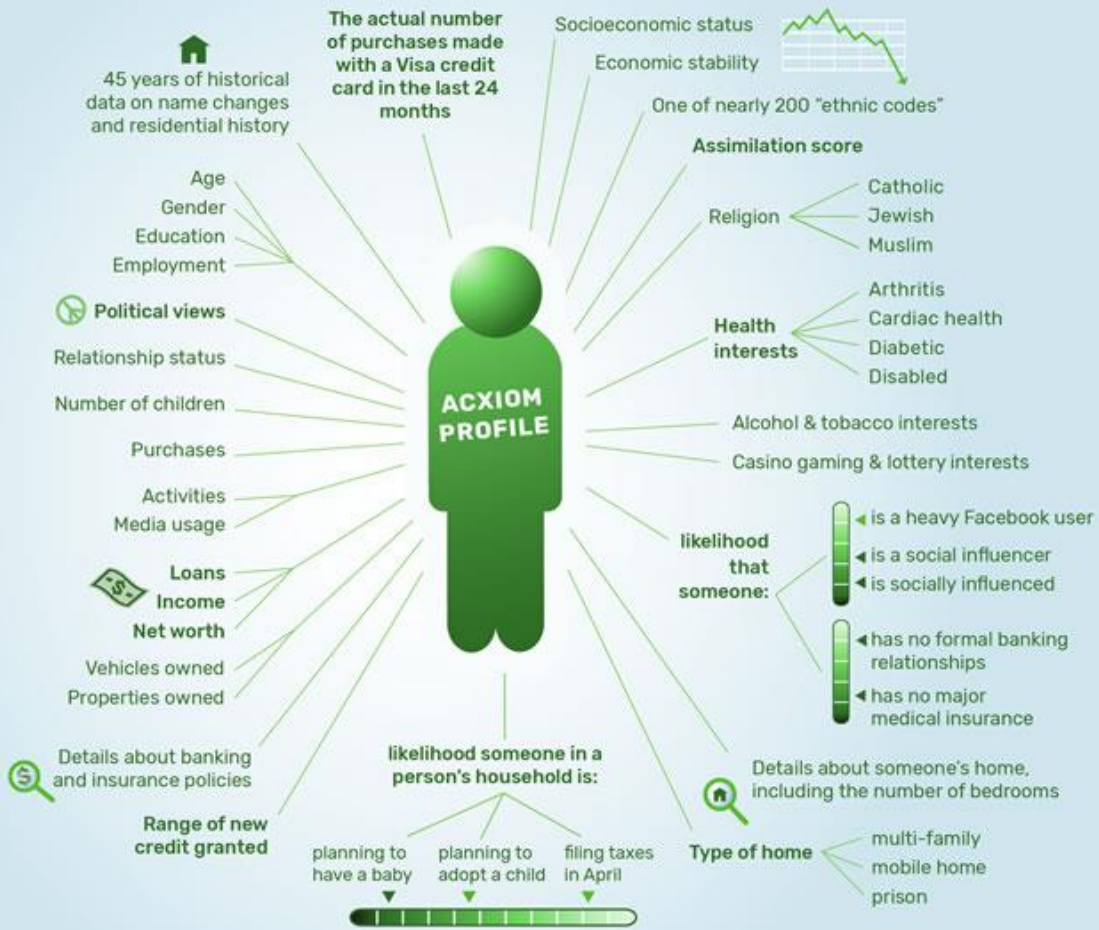
(PI investigation)

- “It is impossible for me to understand why I am classified and targeted the way I am;
- It is impossible to reconstruct which data any of these segmentations are based on and - most worryingly –
- It is impossible for me to know whether this data can (and is) being used against me.”

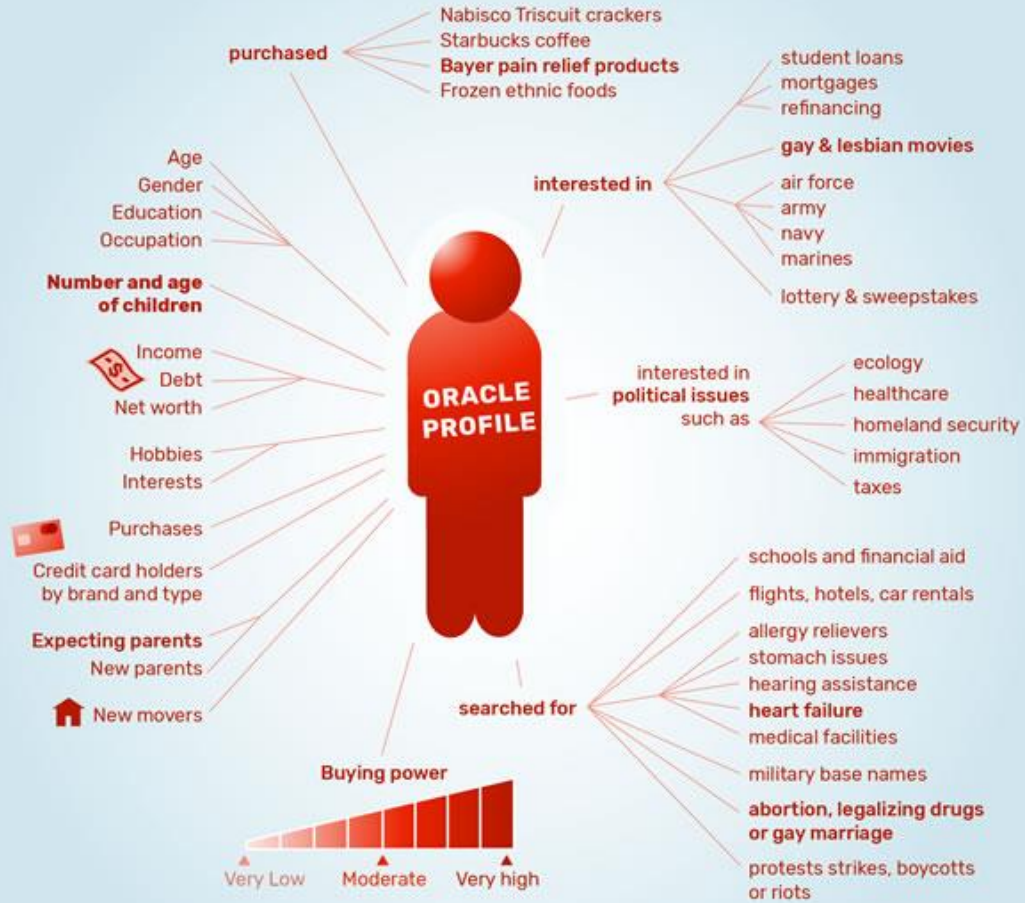
(PI investigation)

DATA BROKERS HAVE EXTENSIVE PROFILE INFORMATION ON ENTIRE POPULATIONS

Examples of data on consumers provided by Acxiom and Oracle

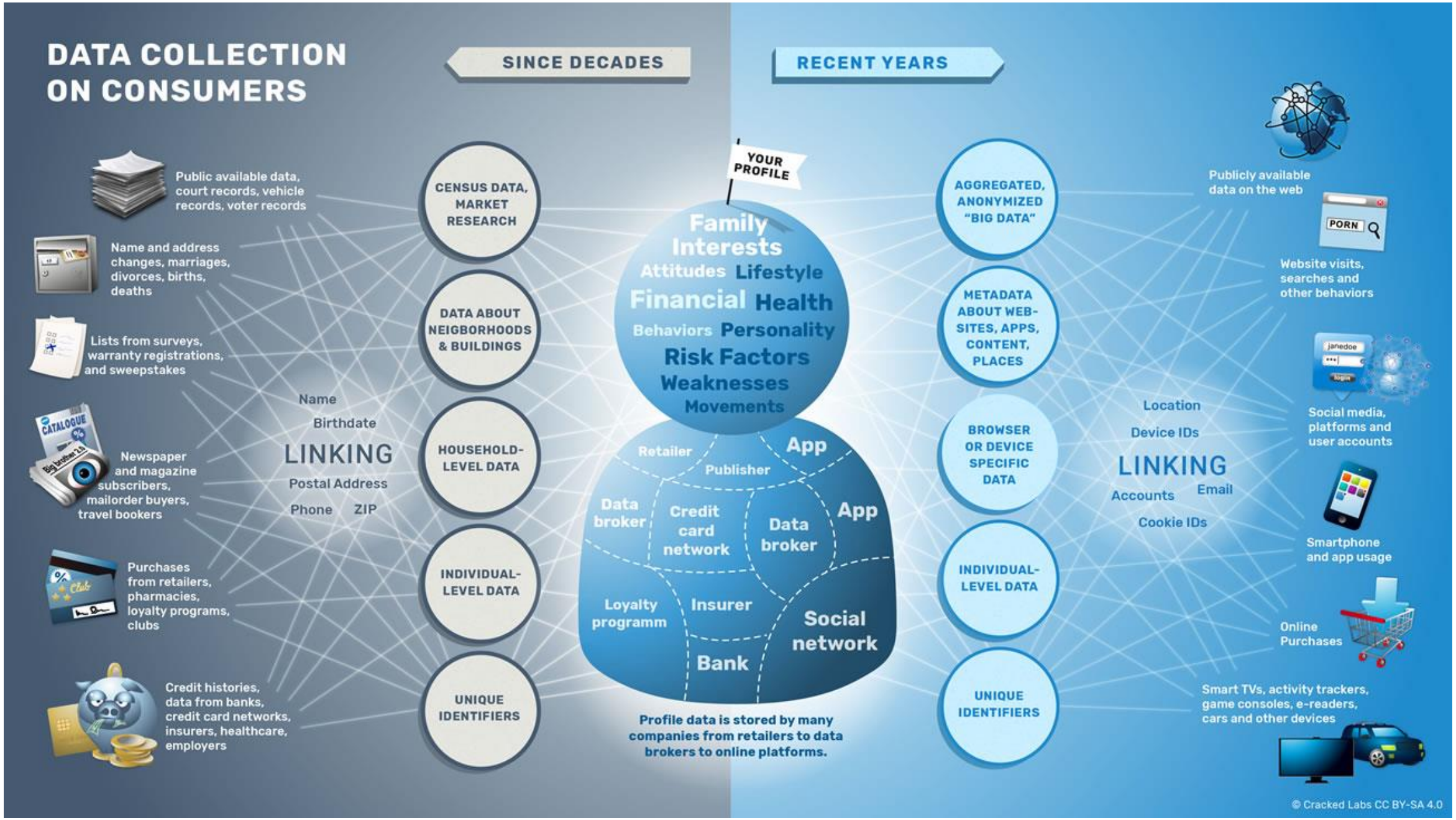


Acxiom provides of up 3,000 attributes and scores
on 700 million people in the US, Europe, and other regions.

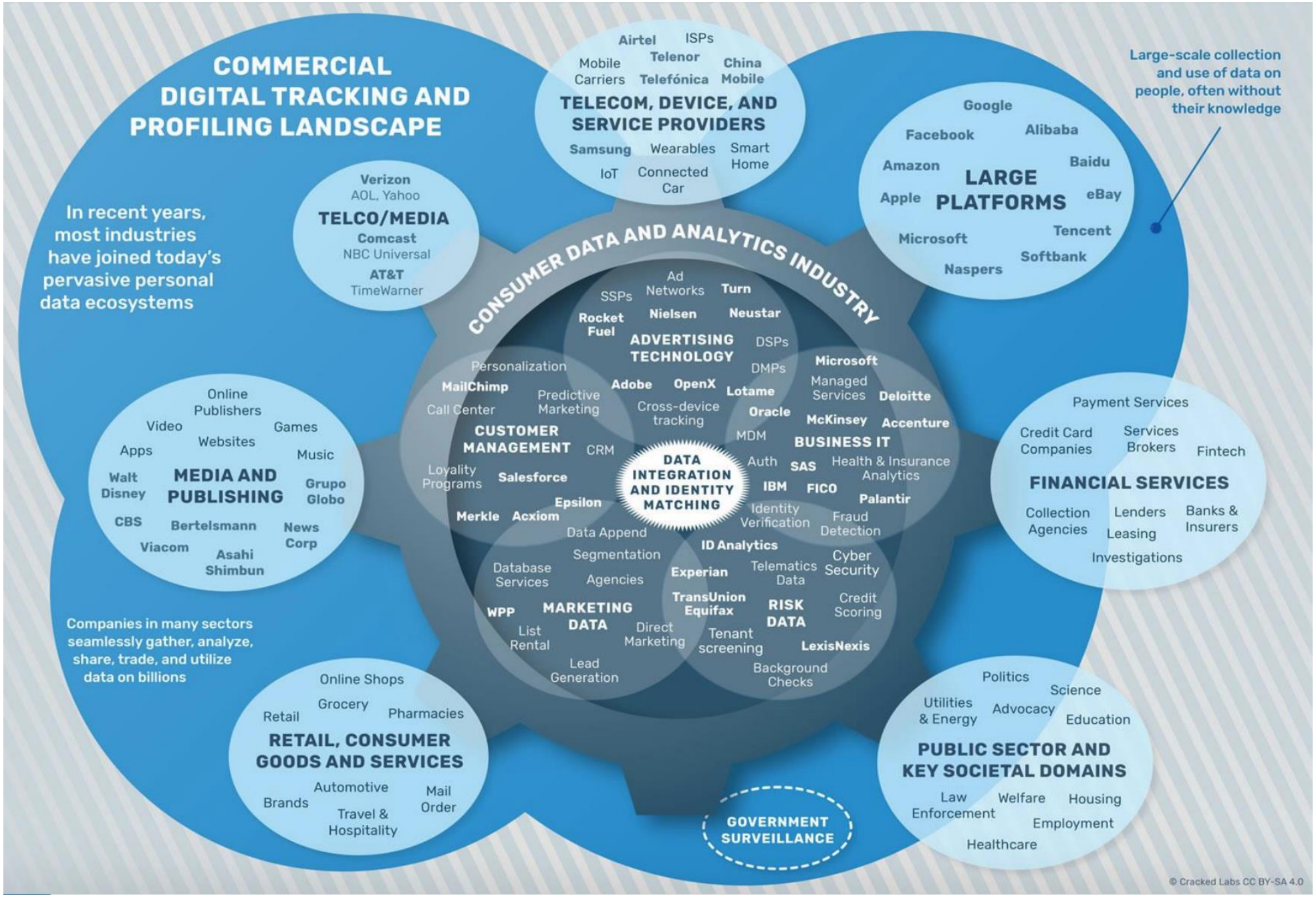


Oracle sorts people into thousands of categories
and provides > 30,000 attributes on 2 billion consumer profiles

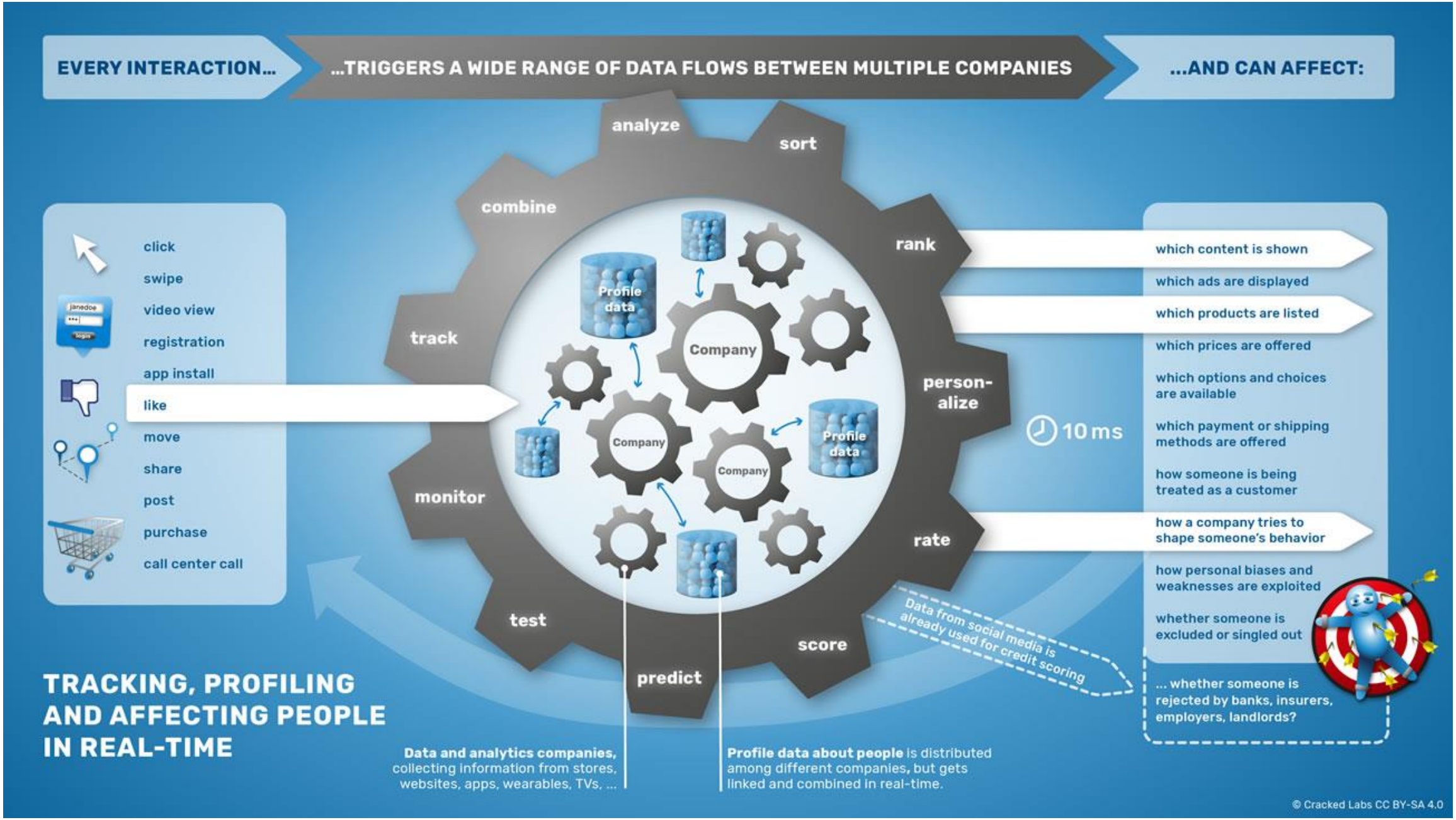
Source: [CrackedLabs 2017]



Source: [CrackedLabs 2017]



Source: [CrackedLabs 2017]



Source: [CrackedLabs 2017]

Case study: Quantcast

- Adtech giant
- Private company founded in 2006 in San Francisco
- Measures & predicts audiences based on digital tracking & AI
- Audience measurement for more than 100 mil. web destinations
  - Consolidated with data brokers & credit agencies
- Nov. 2018: Privacy International filed a breach of privacy complaint with EU data protection authorities, for adtech user profiling practices
  - Against: Quantcast, Acxiom, Oracle, Citreo, Tapad, Equifax, Experian

Guess your audience.
Or know your audience?

Machine Learning Application: Prediction

Until machine learning started to inform prospecting, finding new customers was based upon a small set of characteristics with limited accuracy for real prediction. With new AI driven analytics, we now have the opportunity to locate and predict the real-time behaviour of new users, across the web, based on granular, live behavioural models of current users. The more massive and fresh the data, the deeper the behavioural analysis, the more precise the recognition and learning, and the more successful the targeting. Whereas past algorithms drew on panel measurement and a stale, generic past to guess the future, today's precise one-to-one reading of present behaviour can predict it.

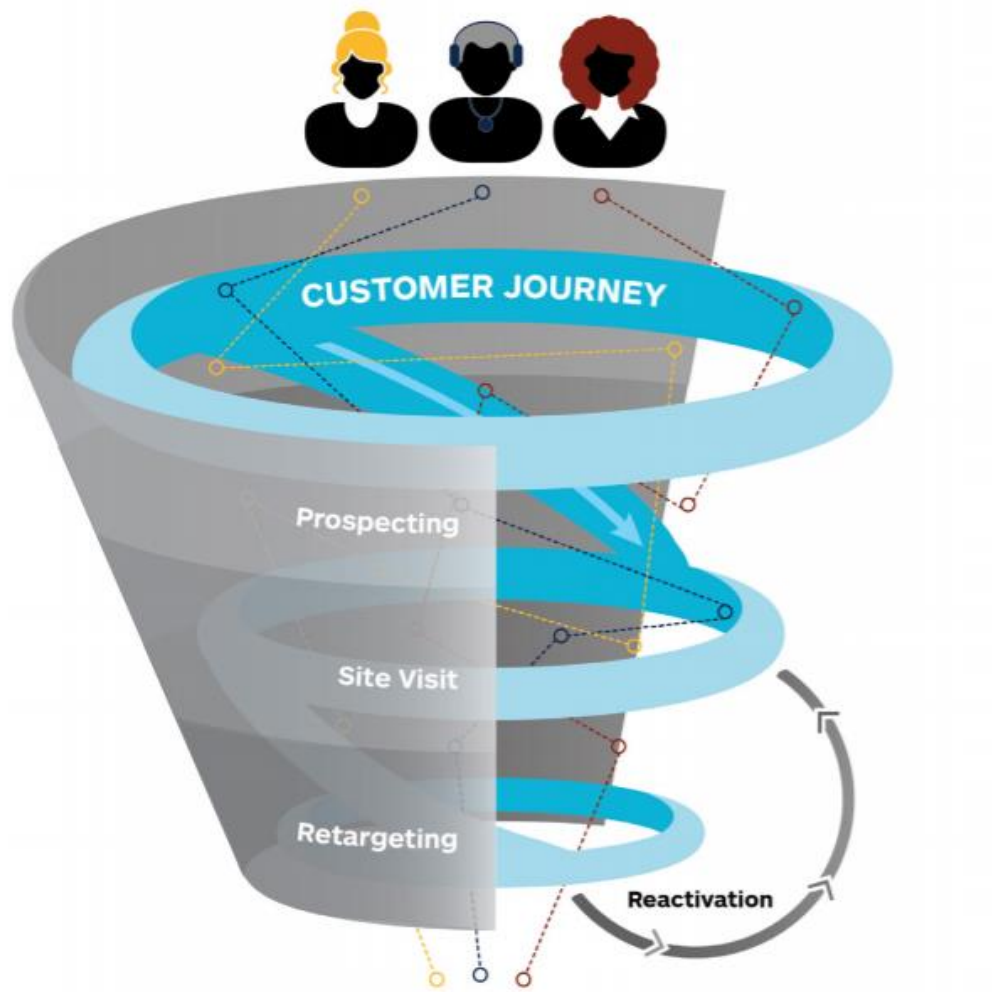
Marketing Use Case: Prospecting

Say goodbye to the funnel and say hello to an always-on learning loop of audience information. The chance to reach ideal customers in real time throughout their purchasing journey—including at key, pre-market moments of influence that establish a brand's primacy in a customer's mind, BEFORE they ever visit a website. The opportunity to evaluate a potential customer's up-to-the second interest level, as well as their closeness to conversion. And the ability to serve fewer ads with greater relevancy, resonance and impact—cutting costs and delivering dramatically higher ROI.

Quantcast | 2019

RETHINKING THE RETAIL SALES FUNNEL

Most consumers shop at only a select number of online and offline storefronts. However, they often spend several hours a day on various social media sites, blogs, and review sites where they perform product research and learn about new brands. As many of these content sites are monetised by display ads, there are tremendous opportunities for retailers to interest consumers in their brand and bring them closer to a purchase.



67% OF USERS START A PURCHASE ON ONE DEVICE AND CONTINUE ON ANOTHER[2]

8 HOURS 40 MINS

THE AVERAGE UK CONSUMER ABSORBS 8 HOURS, 40 MINUTES OF MEDIA A DAY, OF WHICH **43%** IS DIGITAL[3]

Measuring prospecting efforts

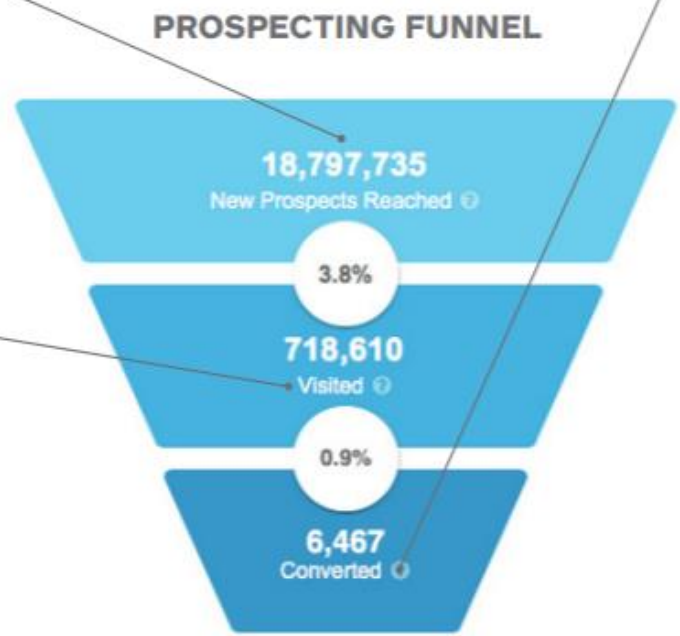
The aim of prospecting is to move a consumer through from awareness of a brand to consideration of their products. This is hard to do as those consumers targeted by prospecting will most likely never have heard of your brand. With this in mind there are three core metrics that we can measure prospecting by to ensure that we get a balanced view of advertising tactics across the funnel.

NEW PROSPECTS REACHED

The number of new cookies targeted that have not been to the advertiser's website before. This number allows you to see how many new prospects you reached with your campaign.

VISITED

As it suggests, this is the number of those new prospects targeted who went on to visit the site (3.8% in this example). The higher it is, the more relevant the prospects being targeted are.

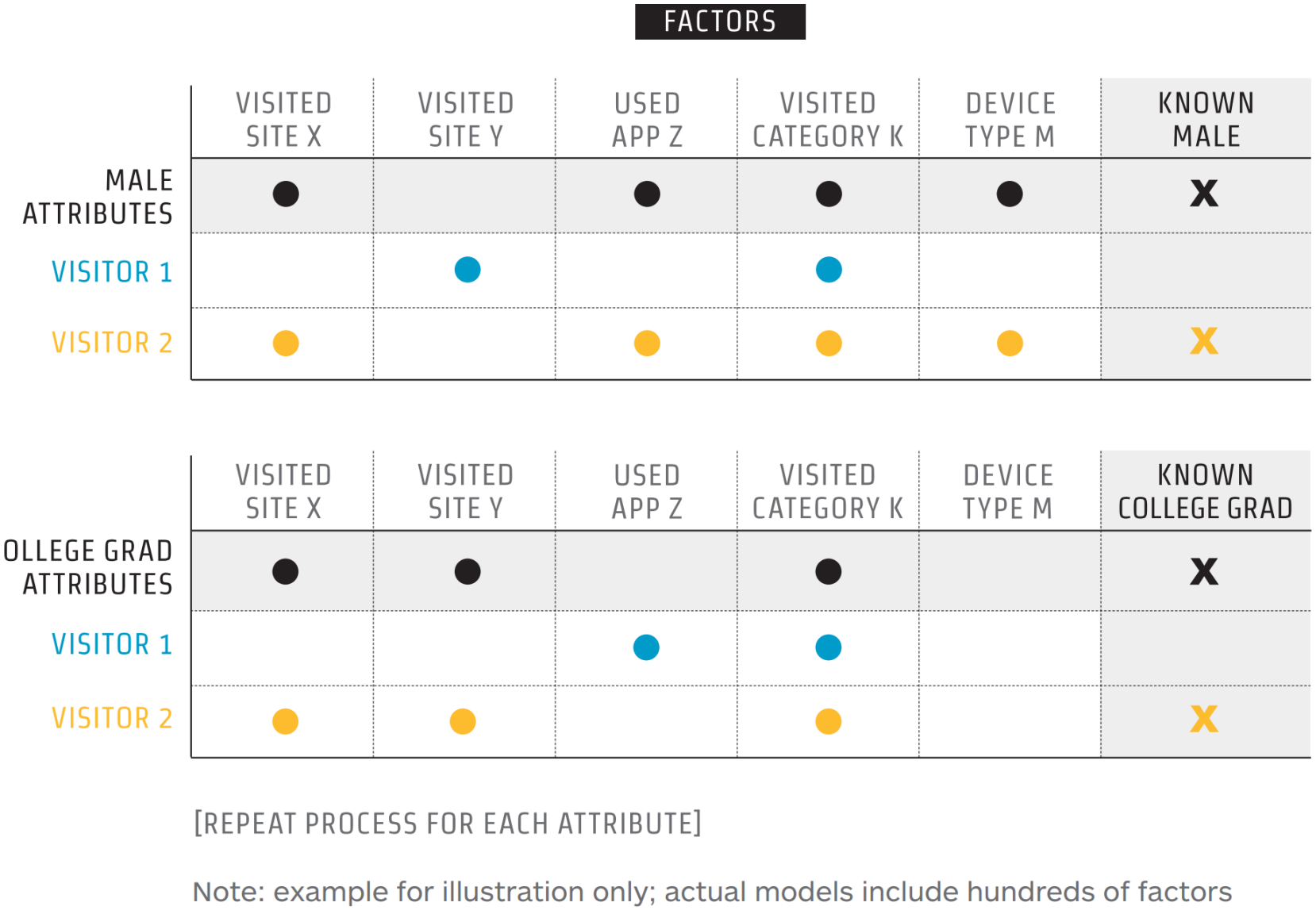


CONVERTED

This tells us how many of the prospects targeted went on to convert (0.9% in the example), allowing advertisers to understand how many net new customers they have driven from their campaign. This can be compared to the site average to show the percentage of incremental conversions driven by display advertising.

74 Charlotte Street, London, W1T 4QJ E uk@quantcast.com T +44 (0)203 322 7863 W quantcast.com

ADVERTISE
quantcast



"How does Quantcast statistical modelling work?

1. Start with reference data from registrations and surveys

2. Examine characteristics of reference and measured users (which can include sites visited, apps used, app usage frequency, content categories, device type and many more)

3. Infer attributes for each user based on similarity to reference users

4. Validate inferences against reference data and external census data"

Quantcast, 2014

So what?

- We are mined for time and attention
- We are gently nudged
  - Brute data vs. prediction products (Shoshanna Zuboff)
  - Feedback loops: vicious circles
- We are replaced: automation

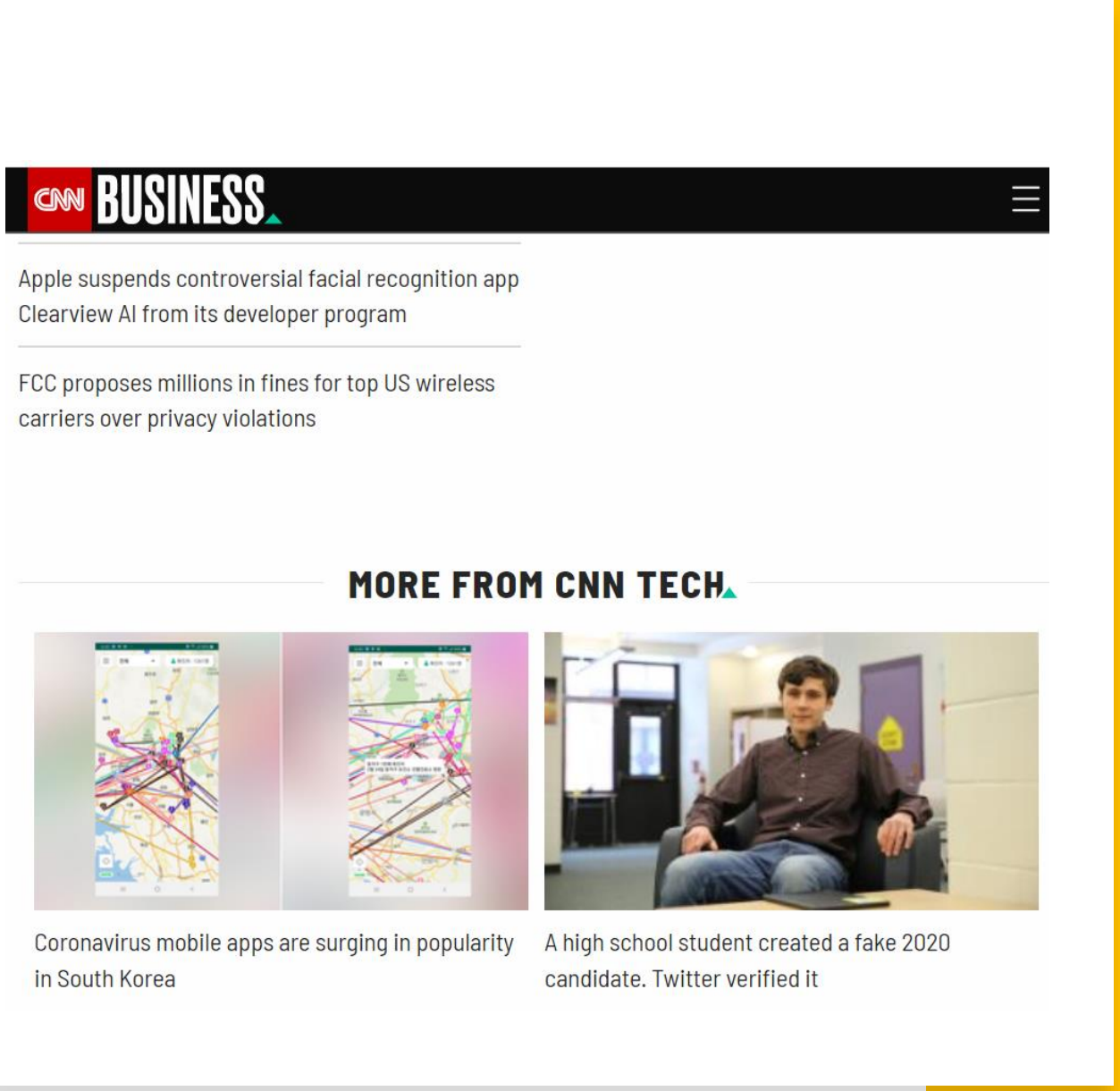
6. Awareness & action

Critical tech evaluation

Using tech, making tech, regulating tech

Critical tech news analysis

- Tech promises vs. solutionism
  - What are the human and social challenges?
  - How is expertise transformed?
  - How is responsibility allocated?
  - What are the business models involved?
  - What are the ecological implications?
- Critical issues
  - Consolidation of surveillance capitalism & new extraction economies
  - Digital gaps & inequalities
  - Quantification of everything
  - Attention management



Critical tech news analysis

- What tech is in focus?
- Overview of current and expected social impact
  - Wikipedia & other encyclopedic entries
  - Controversies
- What is included and what is excluded from the news?
- How does the news favors, marginalizes or ignores:
  - Various categories of people, countries, organizations affected by the tech?
  - Impact on market freedom (competition, information asymmetries)
  - Relevant policies and regulations?

Take away – Course 2

- Illusion of control: Data vs. metadata
- Data flows are floods, not trickles
  - Legal harvesting at scale
  - Exposures & leaks
  - Data & China
- Digital profiles
- So what?
  - We are mined for time and attention
  - We are gently nudged in thought and action
  - We are replaced: automation
- Taking action
  - Critical technology analysis
  - Regulating tech, making tech & using tech

Further reading | 1

- Bruce Schneier, 2018, Internet Plus: Now Everything Can Be Hacked!
- Bill Marczak and John Scott-Railton, April 2020, Move Fast and Roll Your Own Crypto. A Quick Look at the Confidentiality of Zoom Meetings.
- Maria Abi-Habib, June 2020, India Bans Nearly 60 Chinese Apps, Including TikTok and WeChat
- Norwegian Consumer Council 2020. Out of control. How consumers are exploited by the online advertising industry.
- NYTimes – The Privacy Project
- Aliya Ram and Madhumita Murgia, Data brokers: regulators try to rein in the 'privacy deathstars', Financial Times, 2019
- Buolamwini, Joy. 2016. How I'm fighting bias in algorithms. TEDxBeaconStreet.
- Cardona, Melisande. 2016. Geo-blocking in Cross-border e-Commerce in the EU Digital Single Market. European Commision
  - Infographic available here
- Cheney-Lippold, John. 2017. We Are Data: Algorithms and The Making of Our Digital Selves. NYU Press
- Couch, Christina. Ghosts in the machine

Further reading | 2

- Ekström, Andreas. 2015. The moral bias behind your search results. TEDxOslo
- Hammond, Kristian. 2016. 5 unexpected sources of bias in artificial intelligence. In TechCrunch.com
- Mancini, Pia. 2015. Future Scenarios for algorithmic accountability and governance
- O'Neil, Cathy. 2016. Weapons of math destruction. Crown.
- O'Neil, Cathy. 2017. The end of blind faith in big data must end. TED Talks
- ProPublica, 2016. Machine Bias
- Quantcast, 2014. Understanding digital audience measurement.
- Slavin, Kevin, 2011. How algorithms shape our world. TEDGlobal
- Spielkamp, Matthias. 2017. Inspecting Algorithms for Bias.

Further reading | 3

- Nicole Lindsay, 21 May 2019, Adtech Giant Quantcast Facing GDPR Investigation into Breach of Privacy
- Padraig Belton & Matthew Wall, Interview with Frederike Karltheuner: 'More than 600 apps had access to my iPhone data', BBC
- Frederike Karltheuner, Privacy International, "I asked an online tracking company for all of my data and here's what I found"
- Sara Watson, 2020, Data is the New "____", dis magazine
- Sara Watson, 16 June 2014, Data Doppelgängers and the Uncanny Valley of Personalization, The Atlantic