Web, smartphone, AdTech: the privacy viewpoint

Vincent Roca, Pierre Laperdrix

STRATEGIE NATIONALE CYBERSÉCURITÉ

PROGRAMME ET EQUIPEMENTS PRIORITAIRES DE RECHERCHE CYBERSÉCURITÉ

anr

FRANCE 2030

Web, smartphone, AdTech: the privacy viewpoint

IPoP (Interdisciplinary Project on Privacy) project

Joint work **Vincent Roca**, PRIVATICS team leader – **Pierre Laperdrix**, SPIRALS team

PEPR CS winter school, Autrans, January 2024.

Inria

cnrs

contact : vincent.roca@inria.fr

IPoP

https://files.inria.fr/ipop/

Interdisciplinary Project on Privacy

Members

- Part 1: introduction
- Part 2: about privacy regulations
- Part 3: the AdTech ecosystem
- Part 4: technical focus on web and smartphones
- Part 5: is it compliant, desirable, sustainable, and safe?
- Conclusion

Part 1: introduction

- from “ambient privacy” to “massive, ubiquitous data collection”
- from contextual ads to targeted ads
- goals of this presentation

From “ambient privacy” to “massive, ubiquitous data collection” (1970s-now)

Till 1990s’, **“ambient privacy”** is the rule by default
(e.g., recording a familial event requires efforts)
The perceived threat was **“state surveillance”**
(e.g., the SAFARI project led to the creation in 1978 of CNIL and “Loi Informatique et Libertés”)

30-50 years

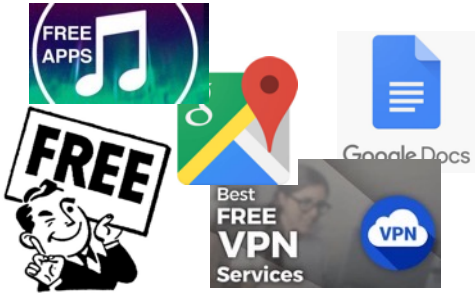
Nowadays, **“massive, ubiquitous data collection”** is the rule
(e.g., preserving ones’ privacy requires efforts)
Nowadays **“surveillance capitalism”** is at the heart of GAFA and is as worrying as “state surveillance”

Q: what happened?

- an “enabler”: by connecting everything, the Internet made it possible
- … but what are the responsibilities of **Advertising Technologies (AdTech)?**

our focus

- On the Internet, everything is **free**…



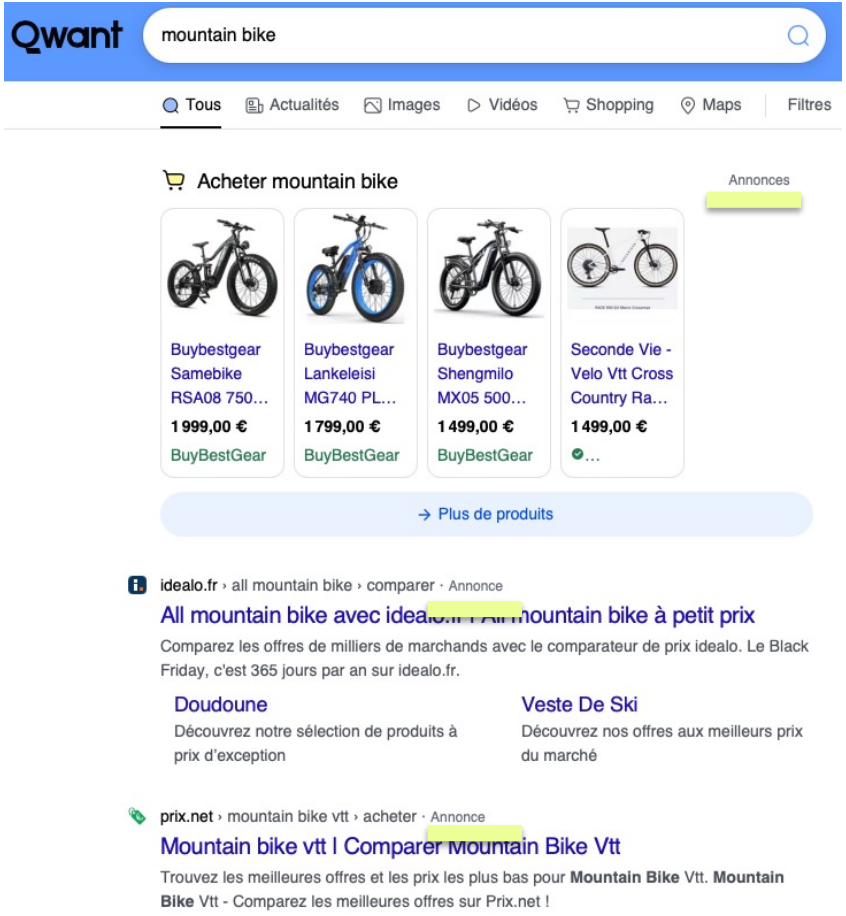
- Direct consequence:

> If you are not paying for it, you're not the customer; you're the product being sold.
>
> posted by **blue_beetle** at **1:41 PM** on August 26, 2010 [562 favorites]

- Common business model: **“free services in exchange of ads”**
  - it could be a valid model, if done correctly, but…

From contextual ads…

- **identify** the topic of a website or search and provide contextual ads
  - e.g., you search “mountain bike” in Qwant search engine ⇒ corresponding ads



The “basic” approach
low impact on privacy ☺

… to targeted ads

- targeted ads carefully selected to increase the probability of “conversion” (e.g., buying a product)
  - e.g., I visit a free news website, I see mountain bike ads, because advertisers know I’m interested in buying one

- targeting requires **profiling** users to know their centers of i

The advanced approach… that works incredibly well!

very high impacts on privacy ☹

- p ...anging **personal data**

Yes, it’s working

- in the 2022 fiscal year:
  - Alphabet total gross revenue: 283 Billion $
  - advertising revenue: **224 Billion $**, i.e., **79% of gross revenue** (*)

- in the 2022 fiscal year:
  - Meta total gross revenue: 116 Billion $
  - advertising revenue: **112 Billion $**, i.e., **97% of gross revenue (**)**

(*) sources:
https://www.statista.com/statistics/266249/advertising-revenue-of-google/
https://abc.xyz/investor/news/earnings/2018/Q4_alphabet_earnings/
(**) sources:
https://blog.digimind.com/fr/agences/facebook-chiffres-essentiels#SocieteCA

No surprise!

When a company has ≥ 80% of gross revenue comes from advertisement…
…it does its best to maximize it!

Alphabet

- top quality services and products, for all situations… and as many opportunities to collect data

personal data

Android Automotive OS (AAOS)

Google solved their “Grand Unified Theory” (GUT) in 2012

Google to unify privacy policy across products

Reuters 25 January 2012

“If you’re signed in, we may combine information you’ve provided from one service with information from other services,” Google’s director of privacy, product and engineering, Alma Whitten wrote in blog post.

“In short, we’ll treat you as a single user across all our products, which will mean a simpler, more intuitive Google experience.”

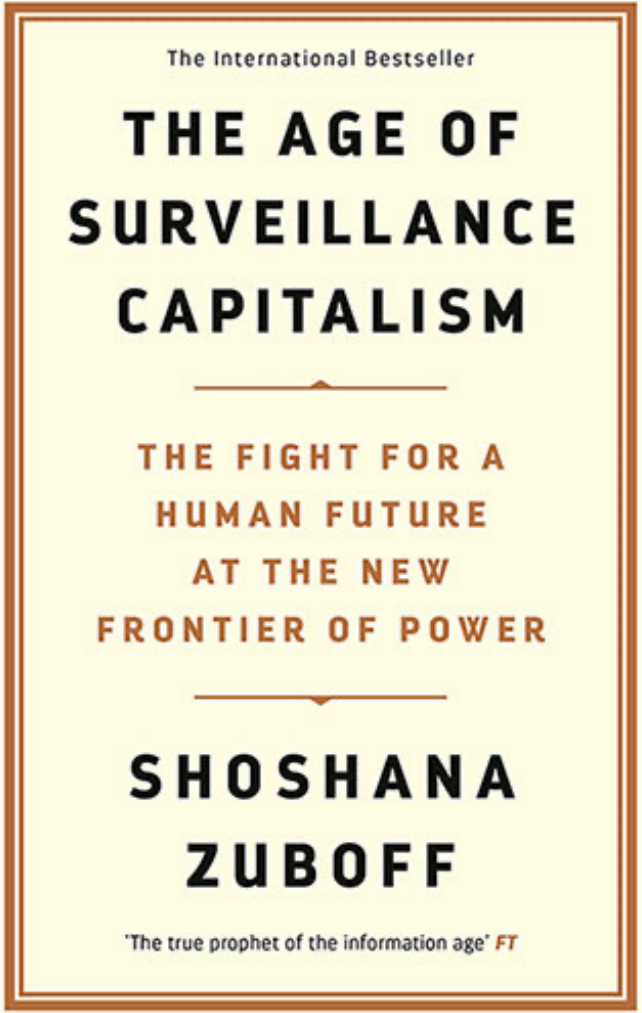
… and across all your devices!

https://businesstech.co.za/news/internet/4419/google-to-unify-privacy-policy-across-products/

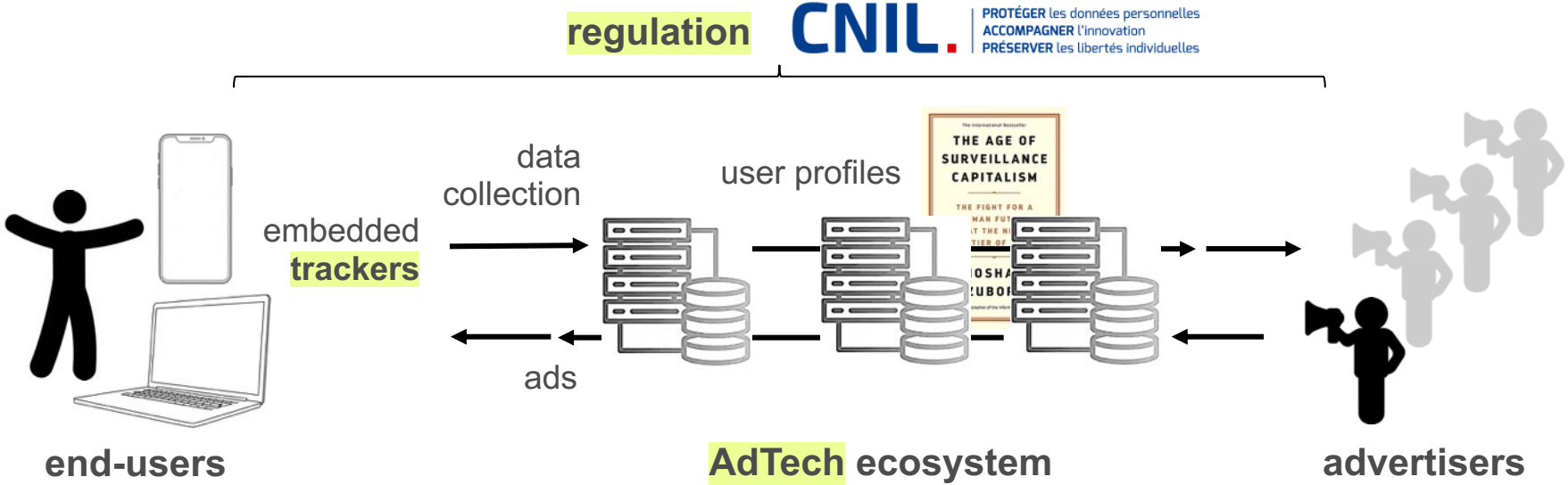
- **Shoshana Zuboff,** Emeritus Professor at Harvard Business School and Associate Professor at Harvard Law School.

  « Bienvenue dans le capitalisme de surveillance ! Les géants du web […] ne cherchent plus seulement à capter toutes nos données, mais à orienter, modifier et conditionner tous nos comportements : notre vie sociale, nos émotions, nos pensées les plus intimes… jusqu'à notre bulletin de vote. En un mot, décider à notre place – à des fins strictement lucratives. Shoshana Zuboff analyse cette mutation monstrueuse du capitalisme, où la souveraineté du peuple est renversée au profit non pas d'un État autoritaire, comme on pourrait le craindre, mais d'une nouvelle industrie opaque, avide et toute-puissante, menaçant dans une indifférence radicale notre libre arbitre et la démocratie. »

https://ife.ee/fr/les-15-livres-francais-de-lannee-pour-comprendre-le-numerique/



- This talk **is not**…
  - a detailed technical analysis of web/smartphone tracking vs. protection
- This talk **is about**…
  - the **AdTech** ecosystem, **regulation, risks,** and a bit of **tracking techs**



Part 2: about privacy regulation

- key concepts
- legal texts: LI&L, GDPR, ePrivacy Regulation, DSA, DMA
- implications
- yes, it does protect us… to a certain point

Is there any hope?

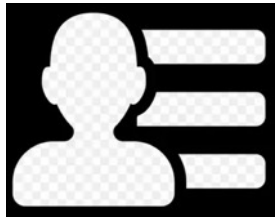
(1989) Eau de Toilette « Vie privée » by Yves Rocher

- almost **50 years** of privacy regulation in FR
  - “Loi Informatique et Liberté” (January 1978)

- ePrivacy Directive (**ePD**)
  - since 2002, to clarify privacy rules… still in application

- EU General Data Protection Regulation (**GDPR**)
  - since May **2018**
  - immediately and uniformly applicable throughout the European Union
  - **additional** rights to natural subjects and requirement to data controllers/processors
  - **above all, sanctions can reach 4% of the annual worldwide gross revenue** (or 20 Million €, whichever is higher)

A cornerstone: personal data



Personal data (“donnée à caractère personnel”):
GDPR, Art. 4, (1): any information relating to a […] natural person […] who can be identified, directly or indirectly […]
To determine whether a person is identifiable, consider all the means likely to be reasonably used by any actor

➔ personal data is **protected** by regulation

Personal data

any type of information

can be identified (any actor, any reasonable means)

natural persons

Another cornerstone: Data controller versus data processor

Data controller (”responsable de traitements”):

An actor is a Data Controller if it is responsible for determining the purposes, and the means of the processing of personal data

how

chooses

why

Data processor (”sous-traitant”):

An actor is a Data Processor when it is dependent on the data controller’s instructions and complies with those instructions

obeys

no choice

There are rights … and obligations

Data controller

(e.g., administration, private company, organization)

is responsible of…

natural persons

Database containing personal data

can be identified directly or indirectly

GDPR obligations to the data controller

- **purpose limitations**
- **minimization**
- **lawfulness**
- **transparency**
- **security**
- **data protection by default**
- **accountability**

- Reminder: a data controller is held **responsible** and can be **fined** up to 4% of annual gross revenue if it fails to comply with its obligations

Making personal data processing legal (1)

- a **legal basis** is needed. Most of the time, for websites/smartphones, it's:
  - **legitimate interest** ➔ basket in an e-commerce site, security, etc.

    no need to ask ☺
  - **consent** ➔otherwise, e.g., for user profiling

    must ask ☹

Making personal data processing legal (2)

- **consent** must be:
  - free ➔ no consequence if user refuses
  - specific ➔ user agrees for a well defined purpose
  - informed ➔ user understands what's taking place
  - unambiguous ➔ clearly given (i.e., opt-in), balanced
  - prior ➔ strictly prior to any data collection, etc.
  - readable and accessible ➔ intelligible, accessible
  - revocable ➔ user can change her mind

It's complex!

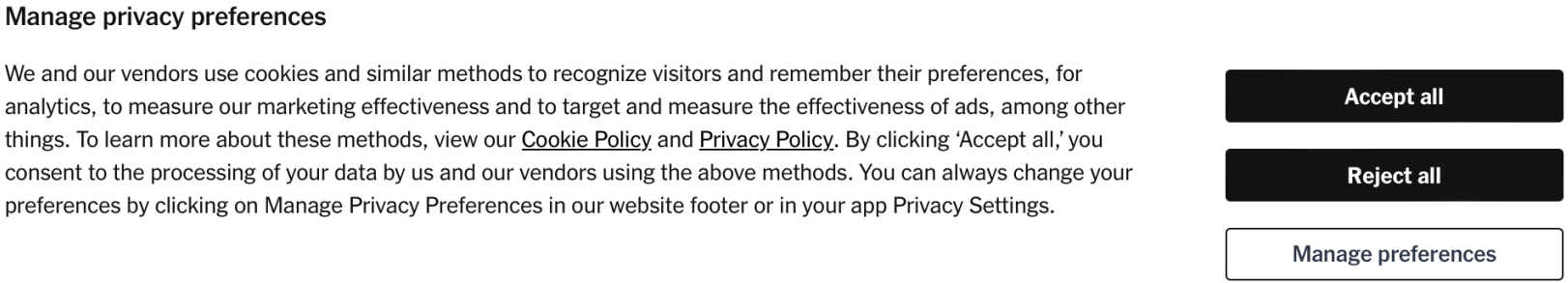
« Are cookie banners indeed compliant with the law? Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners. », Cristiana Santos, Nataliia Bielova and Célestin Matte. *International Journal on Technology and Regulation, 2020.* https://hal.inria.fr/hal-02875447/document

Consent Management Platforms (CMP): help website publishers

- CMPs propose **tools** for publishers to manage consent and compliance

  ⇒ “consent banners” in website (e.g., for EU citizens)

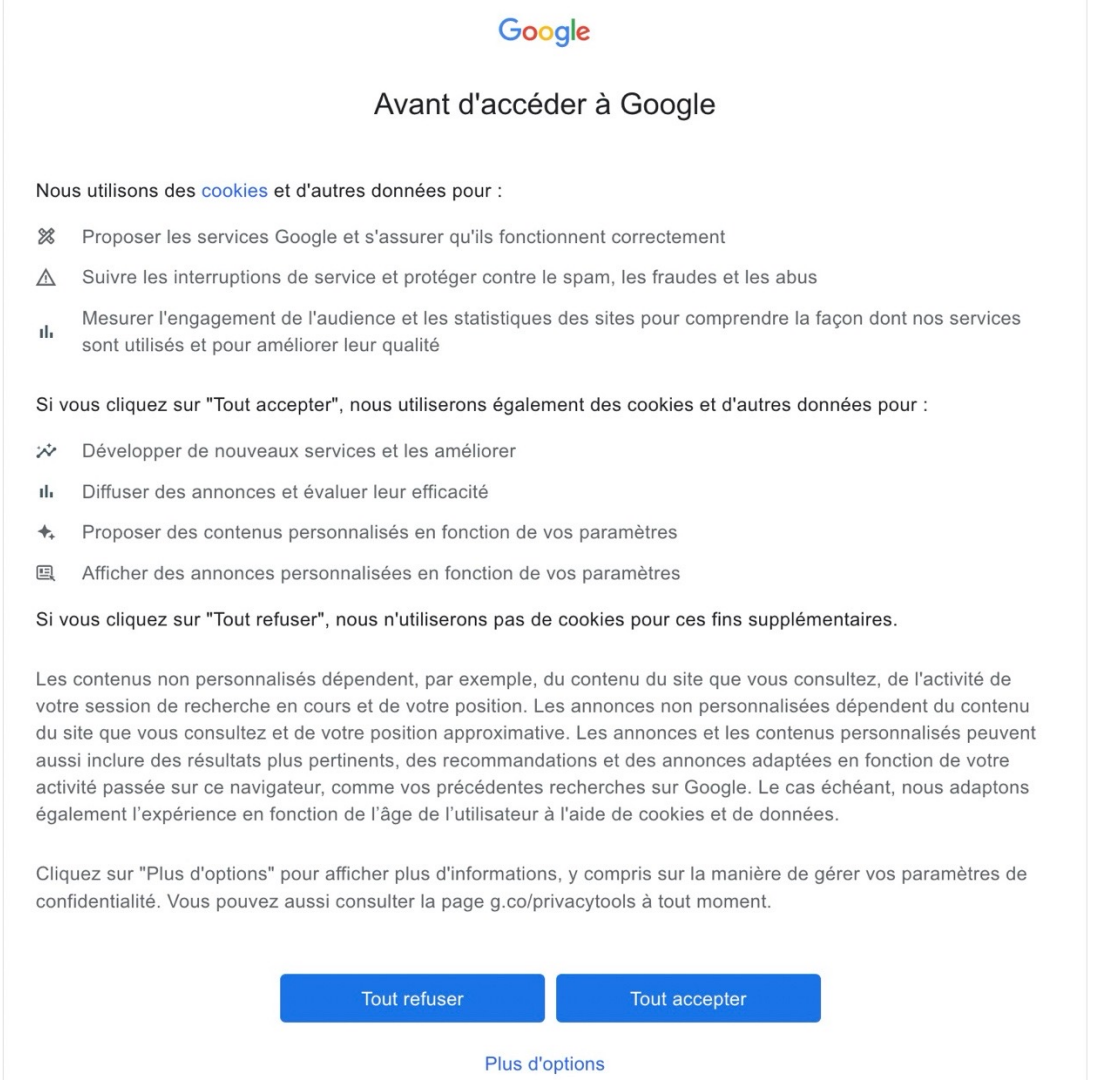
Example of banner, New-York Times
(accessed Jan. 30th, 2024)



Yes, it can work ☺

- Google maps, youtube, etc.
  - refusing is as easy as accepting
  - why?

See: https://www.cnil.fr/fr/cookies-la-cnil-sanctionne-google-hauteur-de-150-millions-deuros-et-facebook-hauteur-de-60-millions



Pseudonymisation versus anonymization

- anonymizing a database enables to escape GDPR obligations
  - a natural person CAN NO LONGER be identified
- but pseudonymized data remains personal data
  - e.g.: {hash(email), geolocation info}
  - AdTech companies claim they manipulate ”anonymized data”, which is wrong

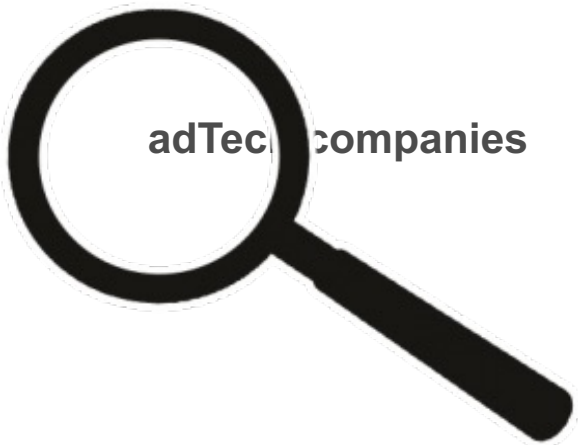
→ **Personal data** (“donnée à caractère personnel”):
GDPR, Art. 4, (1): any information relating to a […] natural person […] who can be identified, directly or indirectly […]
To determine whether a person is identifiable, consider all the means likely to be reasonably used by any actor

Recap

- almost **50 years** of privacy regulation
  - two cornerstones: “personal data” and “data controller”
- main benefit of GDPR: a **major sanction** power
  - up to 4% of the annual worldwide gross revenue
  - yes, it works
- AdTech companies and website publishers have **obligations**
  - **consent** and legitimate interest are two common legal basis for websites
  - obtaining a valid end-user consent is not easy
- pseudonymized data remains personal data and GDPR still applies

Part 3: the AdTech ecosystem

- the big picture (high level view)
- more in details



website publisher

AdTech companies

- create user profiles
- manage ad opportunities via Real Time Bidding (RTB)

Overview (case of targeted ads)

end-user's browser

advertisers

website publisher

AdTech companies

- create user profiles
- manage ad opportunities via Real Time Bidding (RTB)

adds 3rd party scripts

€

keeps €

free website and service

personal data collection

RTB: who's interested by a young & fashion user?

RTB winner ad + €€

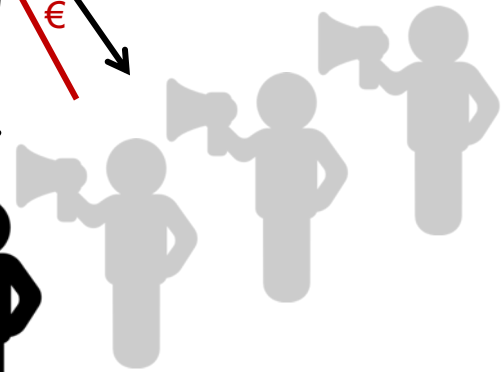
€

targeted ad displayed on web site (in less than 100ms)

end-user's browser

gives consent

advertisers



- previous figure is for **targeted** ads
- Q: what's happening if user **does not consent** to personal data collection?

Manage privacy preferences

We and our vendors use cookies and similar methods to recognize visitors and remember their preferences, for analytics, to measure our marketing effectiveness and to target and measure the effectiveness of ads, among other things. To learn more about these methods, view our Cookie Policy and Privacy Policy. By clicking 'Accept all,' you consent to the processing of your data by us and our vendors using the above methods. You can always change your preferences by clicking on Manage Privacy Preferences in our website footer or in your app Privacy Settings.

Accept all

Reject all

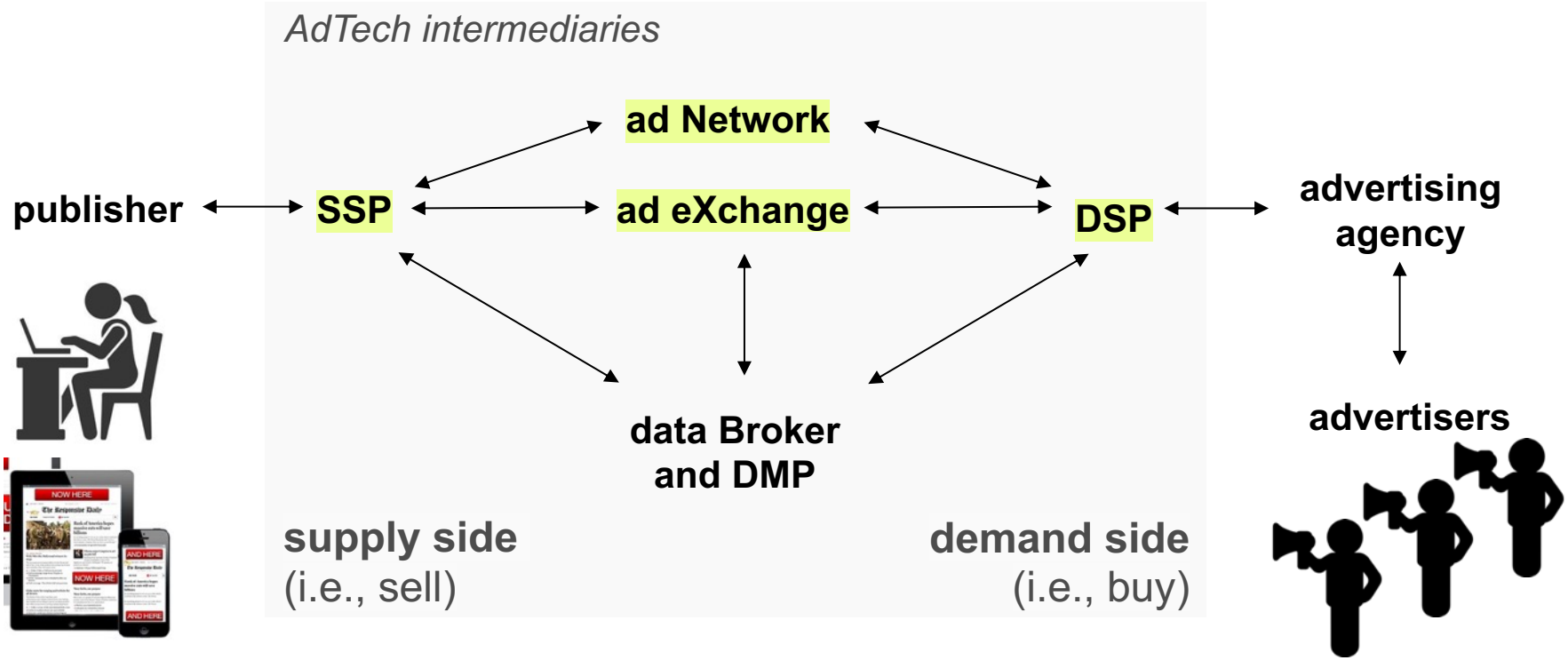
Manage preferences

end-user clicks "reject all"

By clicking “I refuse everything”

- **no** personal data is collected
- AdTech **cannot** update the user profile
- AdTech **cannot** launch a RTB with user profile
- **contextual** ad only

More in details: focus on AdTech



CNIL : “Les enchères en temps réel (RTB), un système complexe”, B. Poilvé, Jan. 2020. https://linc.cnil.fr/fr/les-encheres-en-temps-reel-rtb-un-systeme-complexe

… with some vocabulary

supply side (i.e., sell)

- **publisher**: owner of a website (or app), having inventory to sell
- **inventory**: space available for ads in a website or app
- **impression**: an ad view by end-user
- **SSP** (supply side platforms): enable to sell inventory across several ad networks and adX

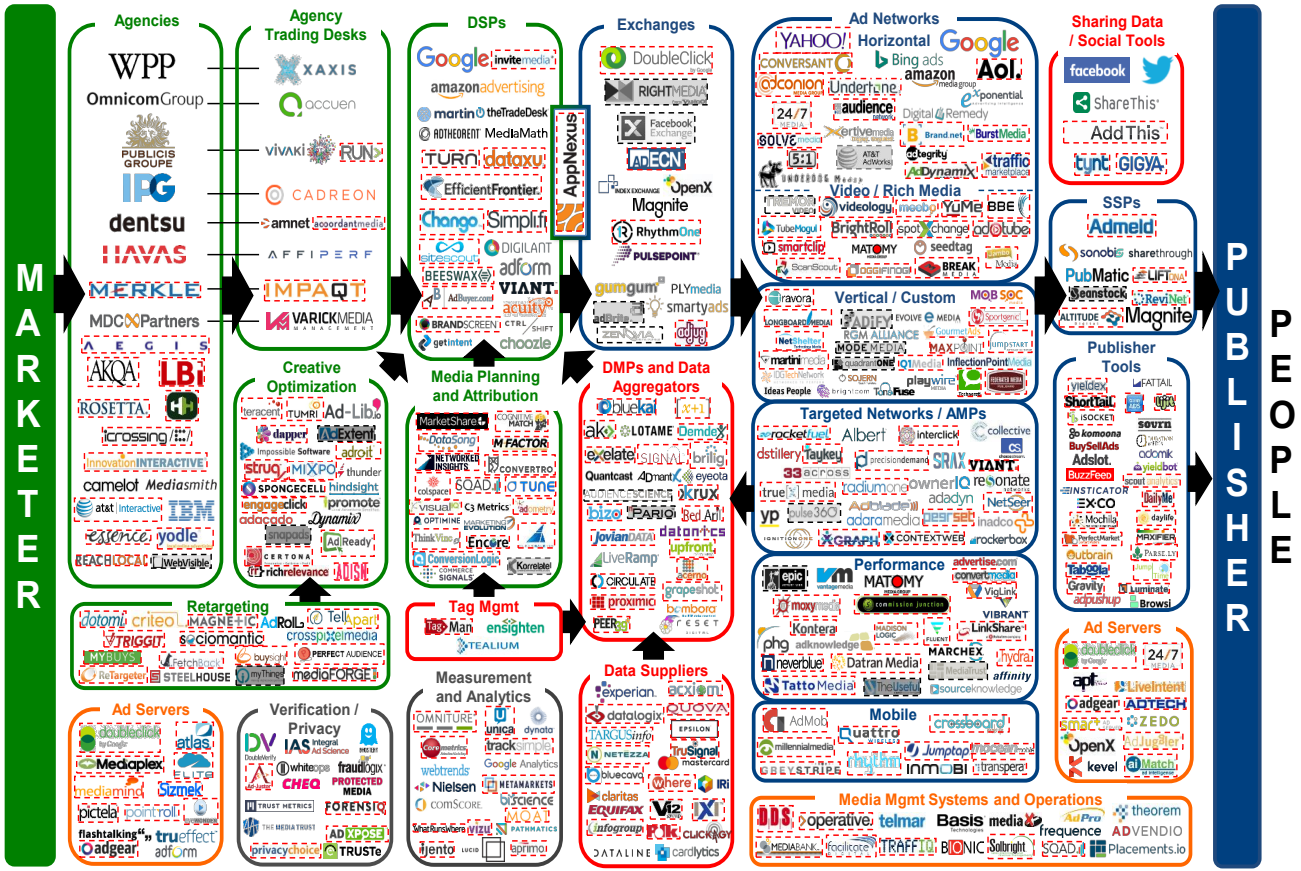
demand side (i.e., buy)

- **advertiser**: wants to buy inventory
- **conversion**: each time a user completes a goal set by the advertiser (e.g., buying a product)
- **DSP** (demand side platforms): enable advertisers to buy inventory from several ad networks and adX

- **adTech**: tools used to create/run/manage/optimize advertising campaigns
- **ad network**: broker between group of publishers and group of advertisers
- **ad eXchange (AdX)**: platform that facilitates SSP/DSP processes

The big list of AdTech companies

The advertising tech landscape (2022)…

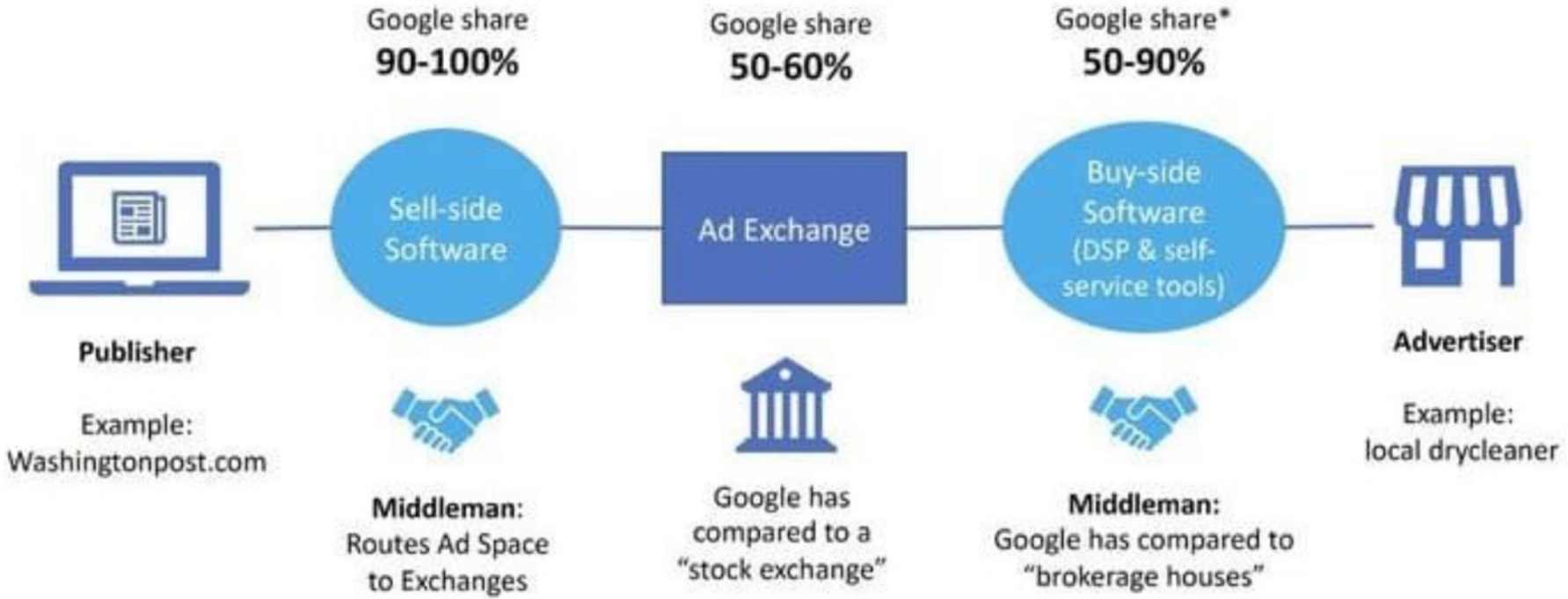


Denotes acquired company

Denotes shuttered company

https://lumapartners.com/content/lumascapes/display-ad-tech-lumascape/

The reality: an unbalanced balance of power



« **La domination des marchés publicitaires de Google** », Pixel de Tracking, 25 oct. 2020
https://www.pixeldetracking.com/fr/la-domination-publicitaire-de-google

Recap

- organized around AdTech companies (i.e., SSP/ad eXchange/DSP/DMP) that
  - create and manage user profiles
  - launch RTB (real-time biddings) for each targeted ad opportunity
  - trigger the ad of the winner to be displayed
  - all of this in <100 ms
- advertisers financially support publishers
- Google largely dominates AdTech

Part 4: technical focus on web and smartphones

- the rush towards stable pseudonyms (identifiers?)
- a few web technics to track users
- the end of 3rd party cookies: a good news?

A wealth of technics in use

end-users

tracking

- 1st and 3rd party cookies
- respawnable cookies
- tracking pixels
- cross-site tracking
- browser fingerprinting
- hardware fingerprinting
- Google Tag Manager (GTM)
- script injection
- URL decoration
- CNAME cloaking
- other technics to hide as 1st party cookie

Attract a lot of academic research, PRIVATICS and SPIRAL included

Goals:

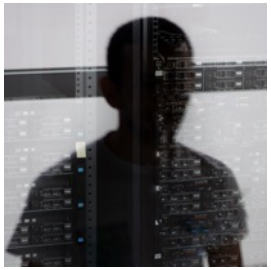
- detecting
- protecting
- measuring
- understanding

Tracking is a three steps process

- **Step 1-** (generate and) collect IDs (pseudonyms) that are:
  - stable across **time**
  - stable across **space**, i.e., across websites, across smartphone apps, across devices…
- **Step 2-** collect and transmit contextual data along with the ID
  - e.g., website, browsing history, app name, apps running, geolocation, etc.
  - the nature of contextual data is only limited by
    - technical limitations ⇒ e.g., web browser or app permissions
    - legal limitations ⇒ e.g., user consent in EU
- **Step 3-** share with other AdTech companies
  - alone, a tracking company has a limited view of what a user is doing on the web
  - by sharing its data, user profiling becomes much more accurate

Stable IDs (pseudonyms) are the cornerstone

- stable IDs are perfect for **tracking users** on the long term



AdTech companies
⇒ end-user uses app1 regularly

app1 active
time=3644692301s
id=68:a8:6d:28:ce:1f

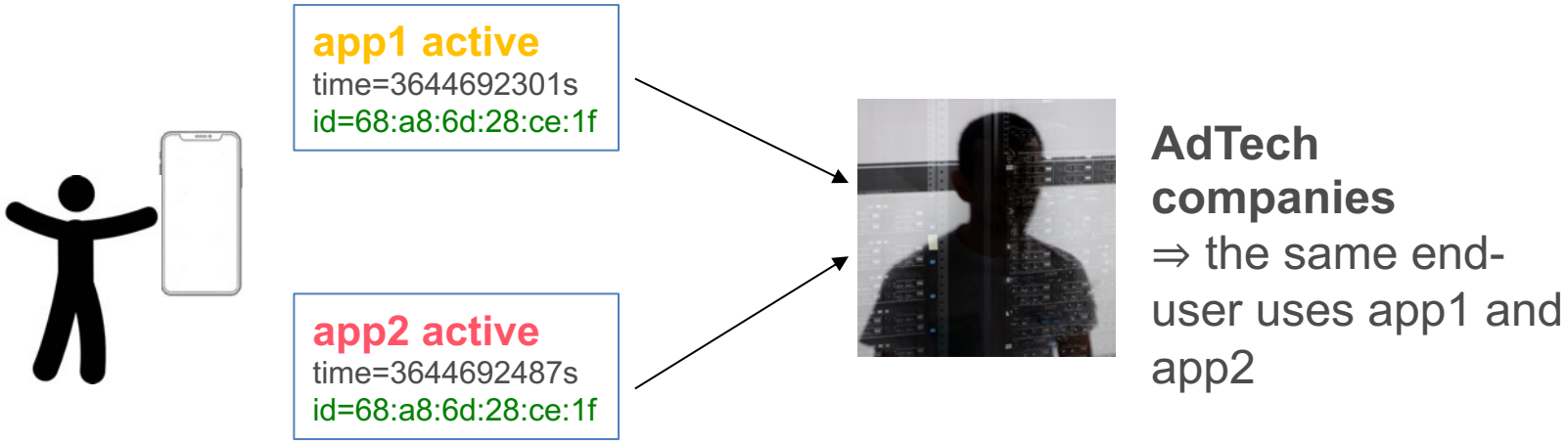
app1 active
time=3644695613s
id=68:a8:6d:28:ce:1f

app1 active
time=3644697600s
id=68:a8:6d:28:ce:1f

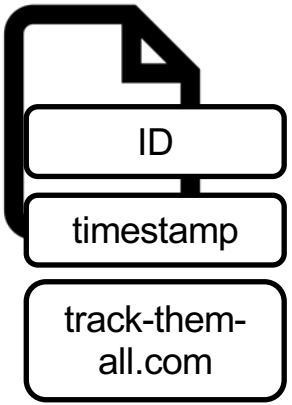
time

Stable IDs (pseudonyms) are the cornerstone (2)

- stable IDs are perfect to **correlate** information collected from several apps/websites
  - and therefore refine a **user profile**



Ex. 1 of ID: the Web cookie



- small file that can store any information up to 4 kB
- any website can create one
- by default, they **persist** even if the browser is closed

Cookies are the main mechanisms to identify users on the Internet

Great for **usability** (e.g., logging users automatically, e-commerce basket)

Great for **tracking** users without them knowing

Ex. 1 of ID: the Web cookie (2)

Cookie
Value:Id=123
Domain:track-them-all.com

https://site1.com
1st visit

get /picture.jpg

set-cookie: id=123

track-them-all.com

https://site1.com
2nd visit

get /picture.jpg

cookie: id=123

track-them-all.com

https://site2.com
1st visit

get /picture.jpg

cookie: id=123

track-them-all.com

track-them-all.com knows that I visited site1.com twice and site2.com once

Ex. 2 of “stateless” ID: browser fingerprinting

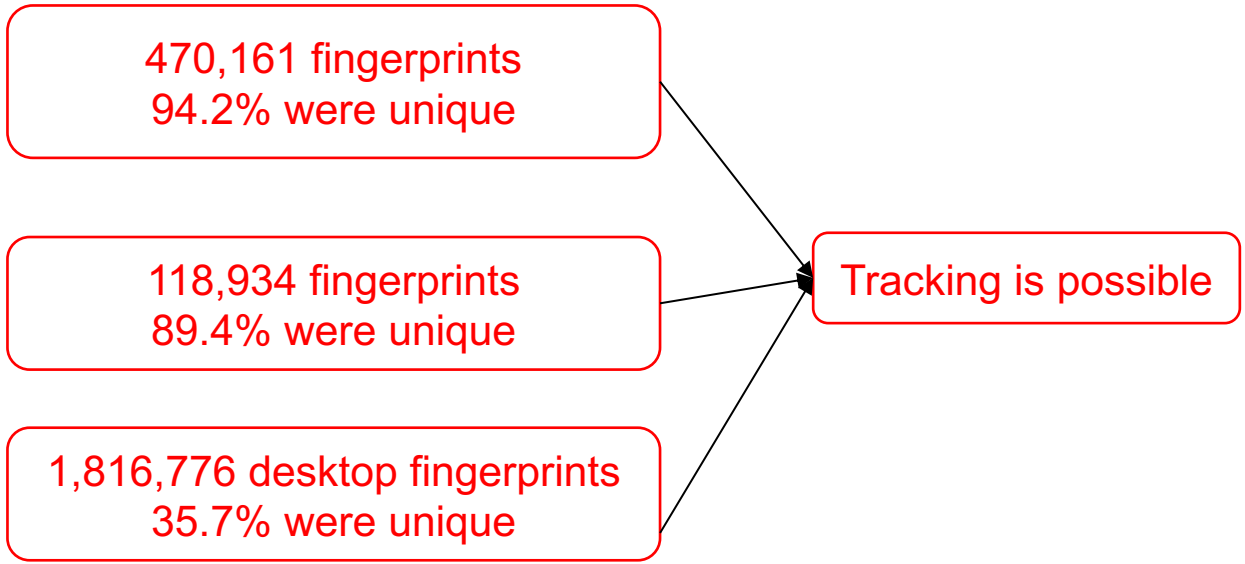
Attribute	Value
User agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.0.0 Safari/537.36
HTTP headers	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 gzip, deflate, br en-US,en;q=0.9
Fonts	Century Schoolbook, Source Sans Pro Light, DejaVu Sans Mono, Bitstream Vera Serif, URW Palladio L, Bitstream Vera Sans Mono...
Platform	Win32
Screen resolution	3840x2160x24
Timezone	-480 (UTC+8)
Battery level	38%
WebGL vendor	NVIDIA Corporation
WebGL renderer	GeForce GTX 3070 Ti/PCIe/SSE2
Canvas	Cwm fjordbank glyphs vext quiz, 😀 Cwm fjordbank glyphs vext quiz, 😀
Browser extensions	

Ex. 2 of “stateless” ID: browser fingerprinting

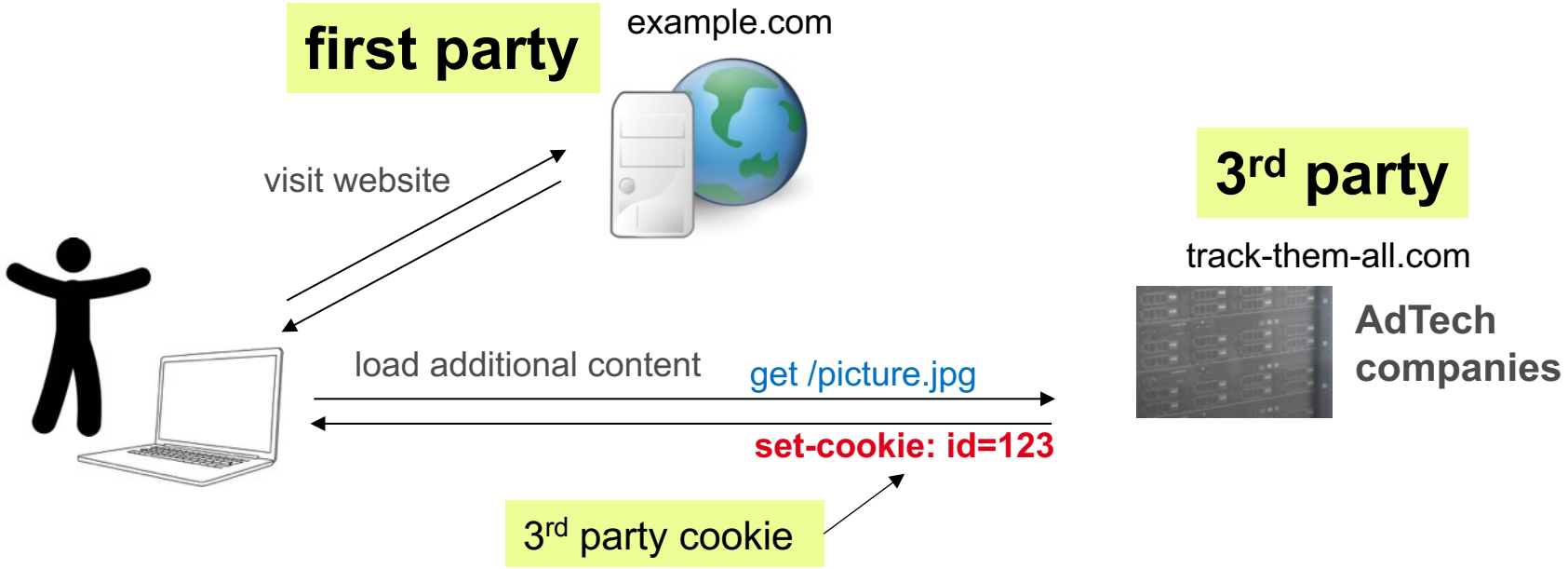
What makes fingerprinting a threat to online privacy?

- it’s really easy to collect all this data. No need for extra permissions
- several studies have investigated the diversity of browser fingerprints

“Hiding in the Crowd: an Analysis of the Effectiveness of Browser Fingerprinting at Large Scale”



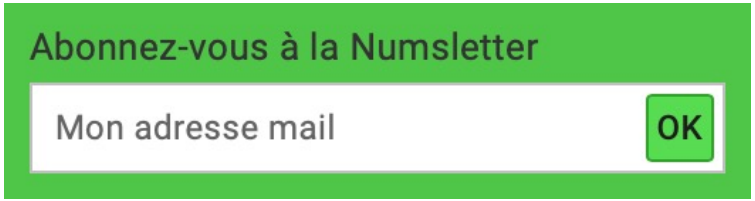
End of 3rd party cookies: a good news for privacy?



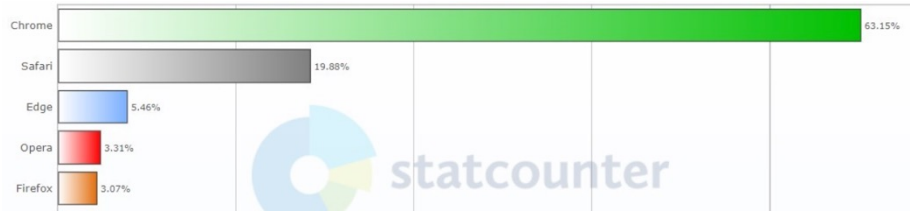
- 3rd party cookies **already banned** from most of browsers for years **except Chrome**
- but Google declared they would do so too in 2022, then 2023, finally 2024!
  - it's complex for AdTech

Several solutions…

- **hide** 3rd party cookies (to be banned) as 1st party cookies (non concerned)
  - CNAME cloaking, server-side GTM, etc.
- **other forms** of ID
  - Web and smartphone fingerprints, IP
- switch to **“logged” environments**
  - contractual relationship between user/publisher ⇒ user already consented
  - email address is convenient ⇒ **hash(email) is the new ID**
  - a stable ID across time and space (majority of users use the same email) ☺
  - “subscribe to our newsletter”:
    trick to collect the users’ email



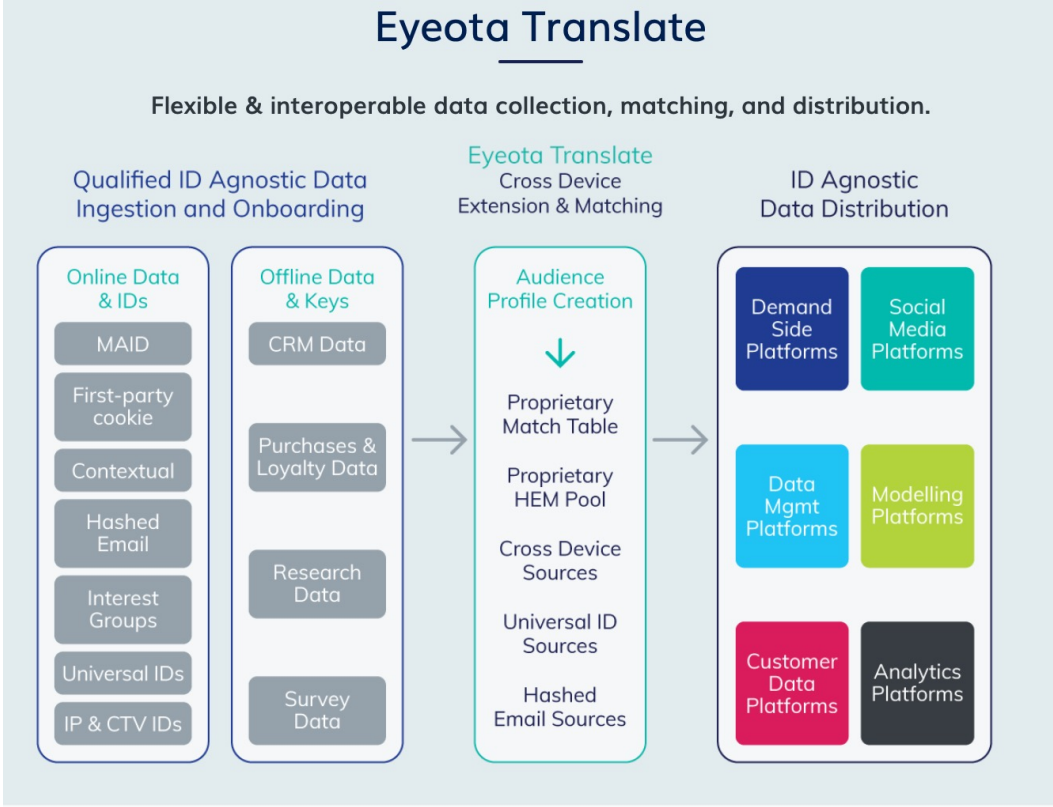
Several solutions… (2)



- the ultimate approach:
  - create your own browser
  - convince 63% of users to use it
  - convince them they should remain logged all the time (required to access your numerous services)
  - convince them it's privacy friendly ☺
- pros ☺
  - you **monitor** all their browsing history directly within the browser
  - you can use data for **your own purposes** (unless they objected by visiting their privacy control page and understood)
  - you have a **key advantage** over all competitors
- cons
  - none (risk of being dismantled for monopoly is null)

Several solutions… (3)

- importance of ID management
  - more than ever, in a post-cookie world, heterogeneous ID matching is a requirement



What our customer's say

"By using the Eyeota Translate solution we can continue to activate our panel-based data and enable amplification of our audiences to serve our customers in a cookieless world."

Commercial Director at YouGov

Recap

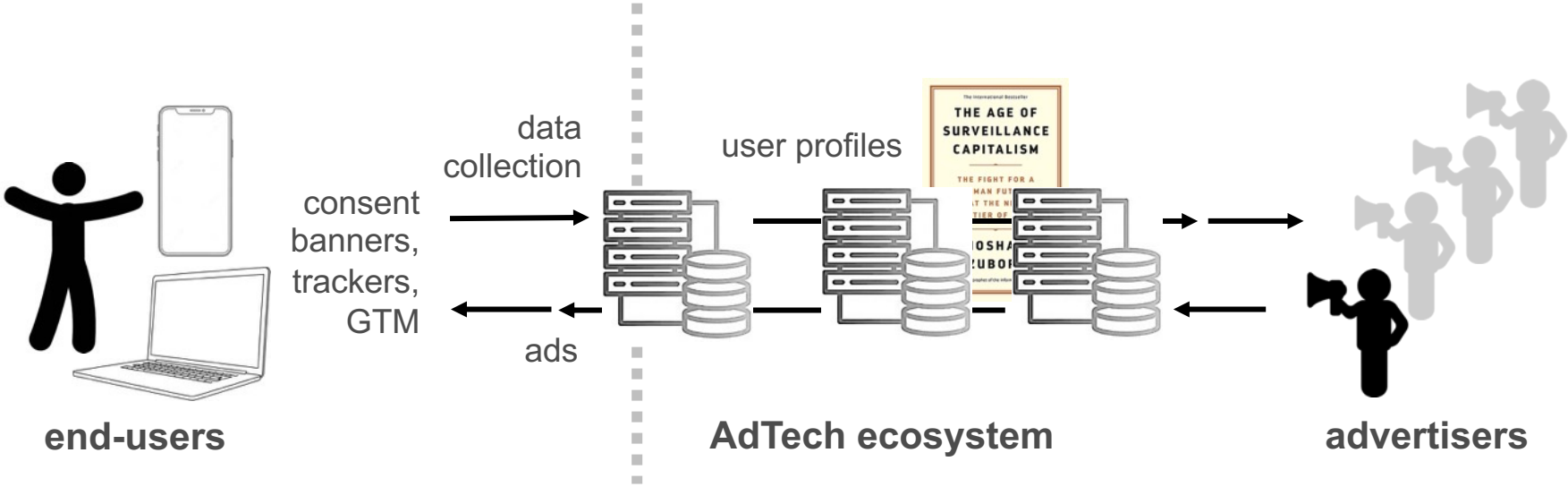
- many technics in use for tracking
- having IDs (pseudonyms) stable across time and space is essential
  - it's the goal of cookies
  - it's the goal of browser fingerprinting
- the end of 3rd party cookies
  - seems benefic at first glance… but it can be replaced by techniques that leave less control and visibility to users ☹
  - the AdTech will find alternatives, promoting "logged environments" is one of them

Part 5: ⇒ Is it compliant? ⇒ Is it desirable?

⇒ Is it sustainable? ⇒ Is it safe?

It sucks…

5.1 ⇒ Is it compliant?



compliance at periphery
(easier – accessible artifacts)

compliance of the core system
(very hard – behind the scene)

Compliance at periphery (e.g., browser)

end-users

consent banners, trackers, GTM

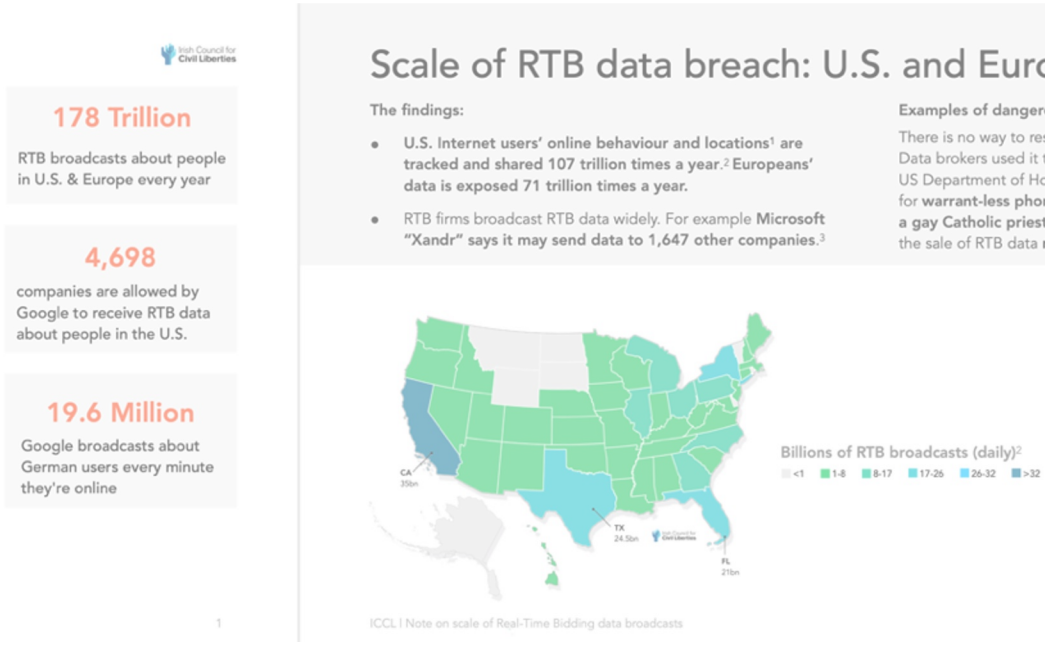
- Is user consent valid (e.g., illegal use of **dark patterns**)
- User consent **effectiveness**
- Legal compliance of **tag management systems**
- Finding hidden, unlawful, tracking

most of the time, transdisciplinary work with legal scholars!

5.2 ⇒ Is it desirable and sustainable?

- how much personal data is collected for user profiling?
- how much personal data is shared by AdTech companies?
- how many RTB broadcasts?
- what data is actually broadcast during RTB? How privacy intrusive is it?

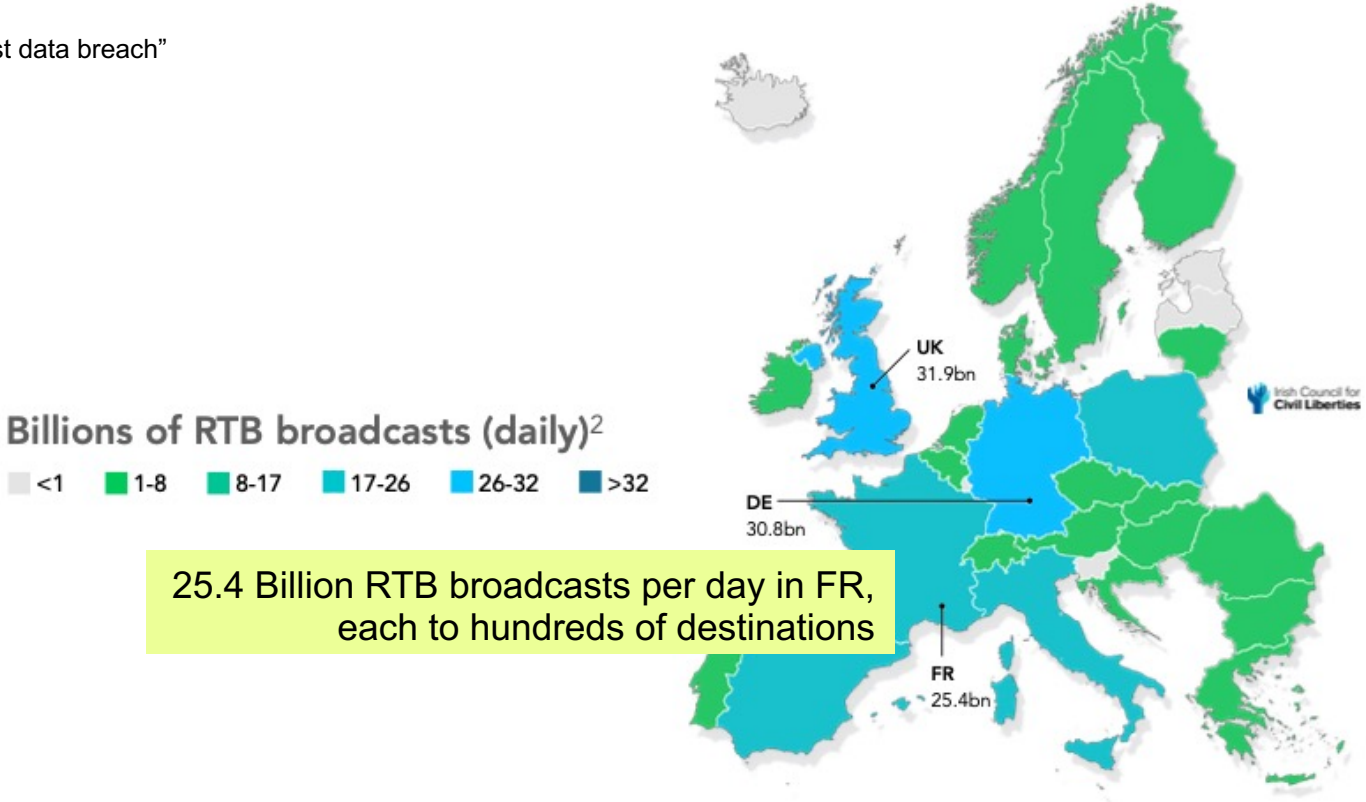
A ”must read” report



Johnny Ryan (ICCL) https://www.iccl.ie/digital-data/iccl-report-on-the-scale-of-real-time-bidding-data-broadcasts-in-the-u-s-and-europe/

Brave report on RTB https://brave.com/static-assets/files/Scale-billions-of-bid-requests-per-day-RAN2019061811075588.pdf

source: Jonnhy Ryan (ICCL) “The biggest data breach”



25.4 Billion RTB broadcasts per day in FR, each to hundreds of destinations

- On average, **a person in the U.S. has their online activity and location exposed 747 times every day** by the RTB industry.
- **In Europe, RTB exposes people’s data 376 times a day.**

GDPR benefits ☺

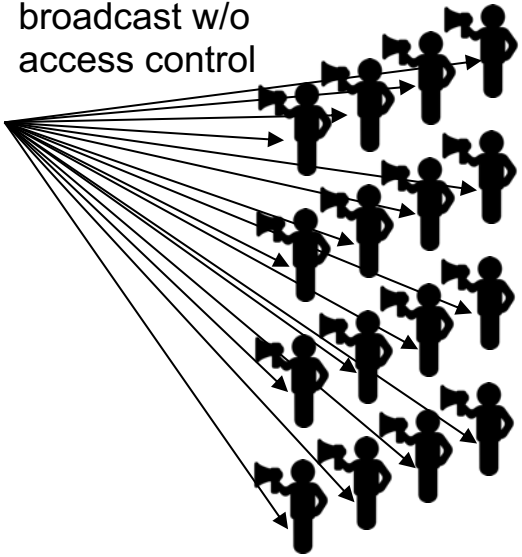
ad request

bid request: can include site, content, user, device, location, segment, …

SSP

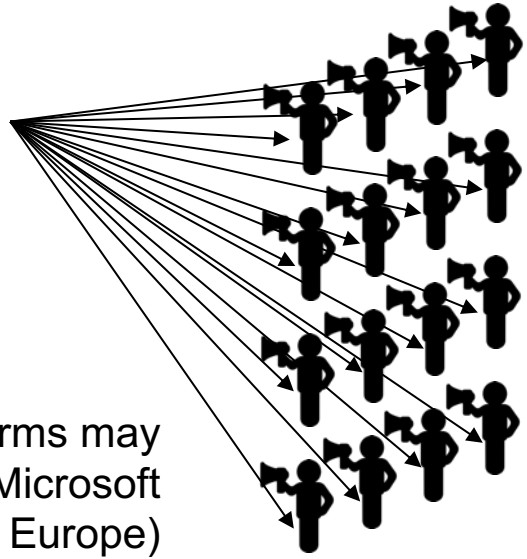
ad eXchange

broadcast w/o access control



“inventory” (space for ad in website/app)

ad eXchange



bidders (1,647 firms may receive data from Microsoft auctions in Europe)

bidders (1,102 firms may receive data from Google auctions in Europe)

- IAB OpenRTB standard enables precise personal data to be carried in bid requests

- Example of info in a Bid request
  - source: IAB OpenRTB 2.6 doc.

3.2.20 Object: User

This object contains information known or derived about the human user of the device (i.e., the audience for advertising). The user `id` is an exchange artifact and may be subject to rotation or other privacy policies. However, when present, this user ID should be stable long enough to serve reasonably as the basis for frequency capping and retargeting.

Attribute	Type	Description
`id`	string	Exchange-specific ID for the user.
`buyeruid`	string	Buyer-specific ID for the user as mapped by the exchange for the buyer.
`yob`	integer; DEPRECATED	Year of birth as a 4-digit integer.
`gender`	string; DEPRECATED	Gender, where "M" = male, "F" = female, "O" = known to be other (i.e., omitted is unknown).
`keywords`	string	Comma separated list of keywords, interests, or intent. Only one of 'keywords' or 'kwarray' may be present.
`kwarray`	string array	Array of keywords about the user. Only one of 'keywords' or 'kwarray' may be present.

3.2.18 Object: Device

This object provides information pertaining to the device through which the user is interacting. Device information includes its hardware, platform, location, and carrier data. The device can refer to a mobile handset, a desktop computer, set top box, or other digital device.

`sua`	UserAgent object	Structured user agent information defined by a UserAgent object (see Section 3.2.29). If both 'ua' and 'sua' are present in the bid request, 'sua' should be considered the more accurate representation of the device attributes. This is because the 'ua' may contain a frozen or reduced user agent string.
`devicetype`	integer	The general type of device. Refer to List: Device Types in AdCOM 1.0.
`make`	string	Device make (e.g., "Apple").
`model`	string	Device model (e.g., "iPhone").
`os`	string	Device operating system (e.g., "iOS").
`osv`	string	Device operating system version (e.g., "3.1.2").
`hwv`	string	Hardware version of the device (e.g., "5S" for iPhone 5S).
`h`	integer	Physical height of the screen in pixels.
`w`	integer	Physical width of the screen in pixels.

3.2.19 Object: Geo

This object encapsulates various methods for specifying a geographic location. When subordinate to a `Device` object, it indicates the location of the device which can also be interpreted as the user's current location. When subordinate to a `User` object, it indicates the location of the user's home base (i.e., not necessarily their current location).

The `lat/lon` attributes should only be passed if they conform to the accuracy depicted in the `type` attribute. For example, the centroid of a geographic region such as postal code should not be passed.

Attribute	Type	Description
`lat`	float	Latitude from -90.0 to +90.0, where negative is south.
`lon`	float	Longitude from -180.0 to +180.0, where negative is west.
`type`	integer	Source of location data; recommended when passing `lat/lon`. Refer to List: Location Types in AdCOM 1.0.

Well…

- RTB figures are a **nightmare**
  - and it does not consider data collection/processing/storage/sharing!
- Do we really want to see such practices continue to **increase**?
- What are the associated energy/resource **costs**?
- answer of the profession: No problem, “we’re engaged in CO_2 compensation ☺”

research ⇒ find techniques to enter the AdTech ecosystem, collect data, establish scientific methods to assess their environmental footprint, provide insights and facts

5.4 ⇒ Is it safe?
Does surveillance capitalism put citizens at risk?

- Admittedly Apple (GAFA?) do their best to resist to external pressure
  - Ex. the "Apple–FBI encryption dispute" (help FBI unlock the iPhone 5C from one of the San Bernardino terrorists). Tim Cook refused FBI found another way and dropped the case

"The United States government has demanded that Apple take an unprecedented step which threatens the security of our customers. We oppose this order, which has implications far beyond the legal case at hand. This moment calls for public discussion, and we want our customers and people around the country to understand what is at stake."
Tim Cook, February 16, 2016. "A Message to Our Customers"

- ⇒ So far, so good? Our devices and personal data are safe ☺

- But there’s a major weak point: AdTech and RTB!

About the authors

Dr Johnny Ryan FRHistS is a Senior Fellow of the Irish Council for Civil Liberties and the Open Markets Institute, and previously held senior roles in the technology industry, including in the RTB industry. He has written for *The Economist*, *NATO Review*, and *Studies in Conflict & Terrorism*.

Wolfie Christl is the principal of Cracked Labs, an independent Austrian research institute. He is a regular speaker at government and research cyber security and data conferences, and his research is widely cited, including in *The Financial Times* and *The Wall Street Journal*.

Acknowledgements
Thanks to Olga Cronin and Dr Kris Shrishak of ICCL, Ryan Gallagher of Bloomberg, Byron Tau of The Wall Street Journal.

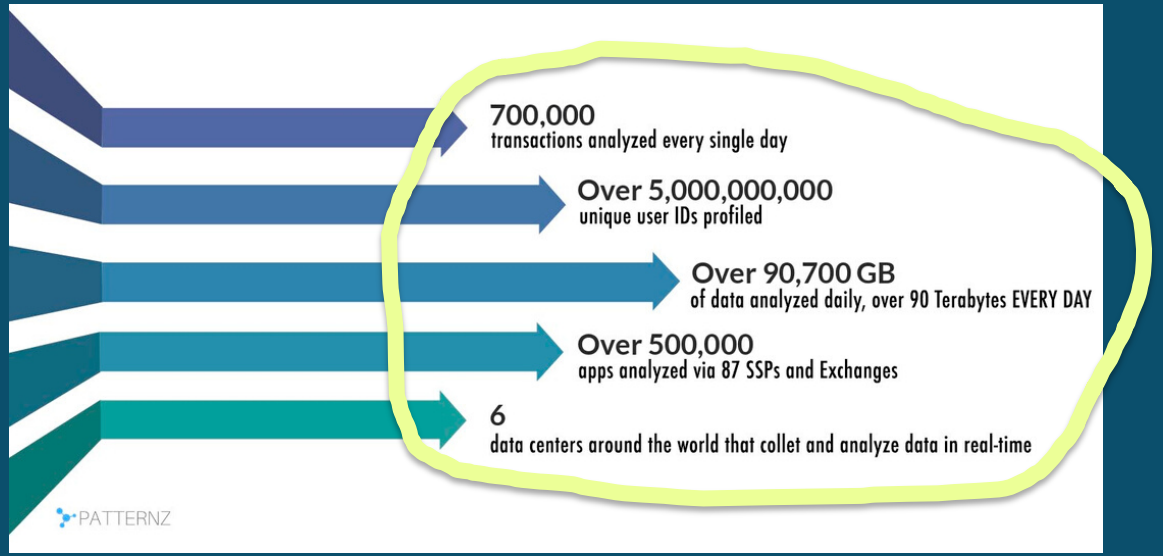
Cover photograph by Luca Morvillo.

A “MUST READ”: Johnny Ryan (ICCL): https://www.iccl.ie/wp-content/uploads/2023/11/Europes-hidden-security-crisis.pdf

Enforce

A unit of the Irish Council for Civil Liberties (ICCL). Learn more about our work on Real-Time Bidding’s security and data protection harms at https://www.iccl.ie/enforce/

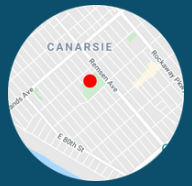
WE HELP NATIONAL SECURITY AGENCIES DETECT AUDIENCE PATTERNS AND USER BEHAVIOR USING DIGITAL ADVERTISING DATA MINING AND ANALYTICS



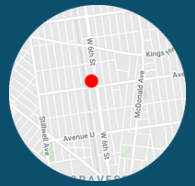
ADVERTISING BASED INTELLIGENCE PLATFORM

PATTERNZ allows national security agencies utilize real-time and historical user advertising generated data to detect, monitor and predict users actions, security threats and anomalies based on users' behavior, location patterns and mobile usage characteristics.

Mobile Applications



Home Zone



Work Zone

Driving Path

Who's Nearby

BACKGROUND

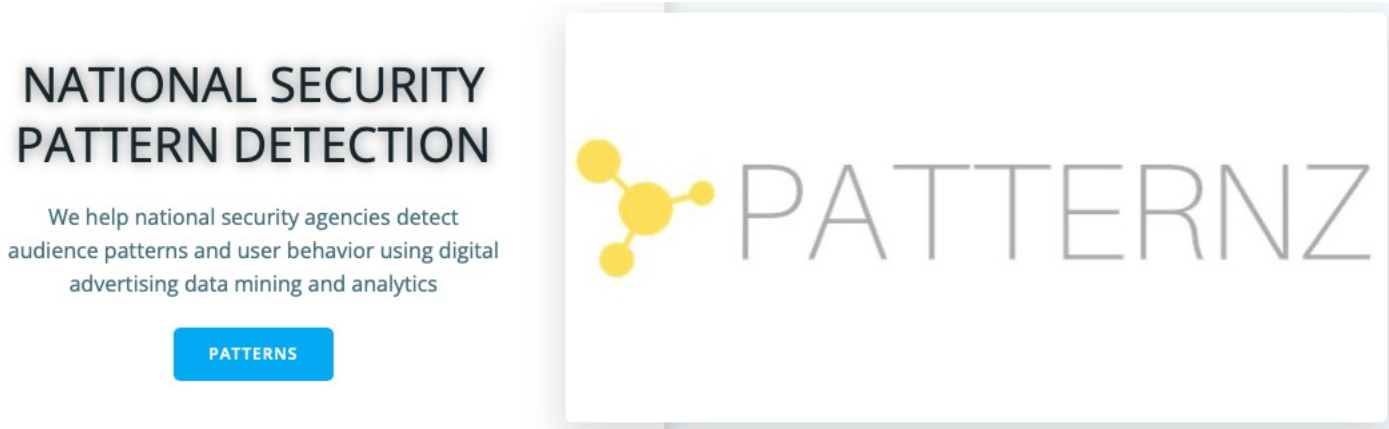
- Mobile Realtime bidding technologies have been the dominant advertising and personalization methods in the last 10 years
- In order to optimize and personalize the advertising experience, every advertising transaction includes various information about the user such as:
  - Unique device id
  - Mobile app
  - Longitude and latitude of the device
- Whatever information the app mange to ”sniff” from the mobile phone such as dates, contacts other installed apps, personal information sets.
- Built on the extensive knowhow of operating a Realtime bidding platform for the last 5 years analyzing and optimizing mobile advertising data
- During this period we gathered unparalleled database of users, their behavior patterns, locations, apps and more

Said differently: thank you, AdTech companies, who help our company to build a global surveillance tool, easily accessible, that targets >5 B unique IDs (humans?) worldwide, without any control!

I.S.A. The Israeli Security Academy
Training & Technology

http://isasecurity.org/technologies

- **I.S.A. the Israeli Security Academy** & technologies is an international organization that specializes in establish of security, intelligence Law Enforcement services and related equipment, as well as the development and implementation of advanced security systems and units, including Law Enforcement units, for governments and private entities around the globe.



Recap

- Is AdTech:
  - **compliant?** ⇒ complying with GDPR is not trivial, yet many do not comply. One can monitor artifacts at the periphery, quid of the core?
  - **desirable?** ⇒ the scale of personal data broadcast is frightening (and undoubtedly collection and exchange of personal data)
  - **sustainable?** ⇒ we need more research, yet the ecological impacts are probably significant (TBC)
  - **safe?** ⇒ who wants advertising-based intelligence platforms?

Conclusions

- we’re almost done ☺

- Internet/web/devices have been **diverted** into massive surveillance tools on purpose
  - it's a cat a mouse game: no matter how high the barrier to prevent tracking, AdTech find ways to circumvent it

- what **business model**?
  - "free in exchange of advertising" is not the issue, targeted advertising is the issue
  - surveillance capitalism works incredibly well, but there's a price to pay

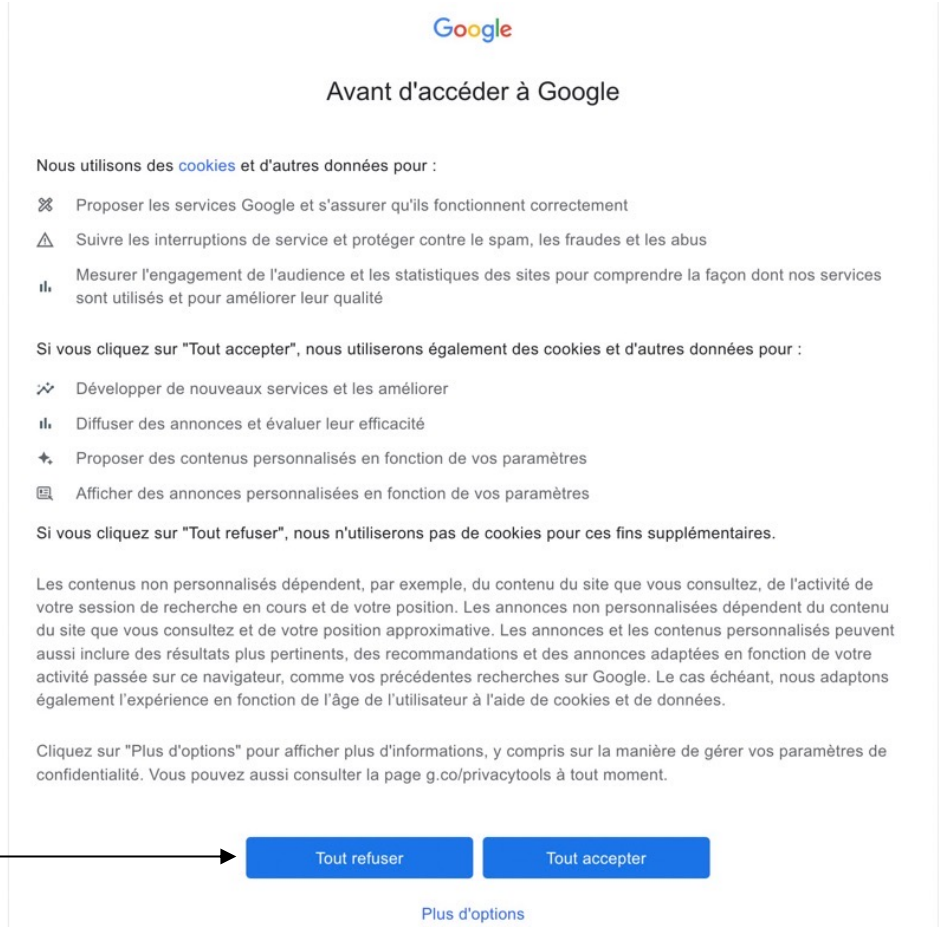
- the situation is **neither desirable, nor sustainable, nor safe**

- privacy **regulation** is essential to protect all of us
  - huge difference between US / EU
  - we are all **protected by default**, including citizens who do not feel the need
  - we can **object** to personal data collection otherwise

- we, PhDs, engineers, researchers, can contribute to make the world a little bit better ☺

- and we all have a super power…

Always click **“refuse all”**:
-it’s good for your **privacy**
-it’s good for your **security**
-it’s good for the **Planet**



"On the Internet, nobody knows you're a dog"

In 1993…

"Remember when, on the Internet, nobody knew who you were?"

In 2015…

Thank you!