The Past, Present and Future of Online Tracking

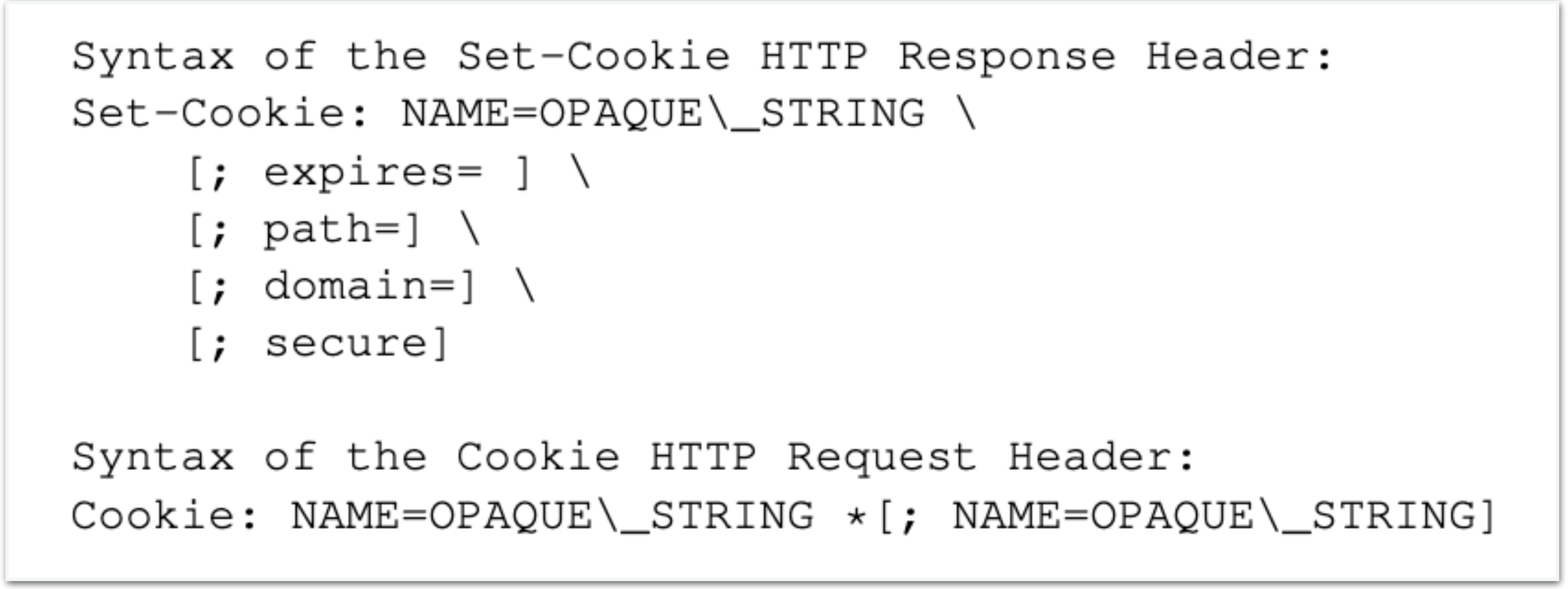
Dr Michael Veale

Faculty of Laws, University College London

click
click
click
By continuing using this site you agree to share your cookies
Yeah sure whatever.
click
Fool

A short history of Web tracking

- In the early 90s, the Web was ‘stateless’ — it had no *memory of its visitors*.
- **Cookies** were invented to solve this problem: they are simply **text placed on your browser by a web server that a server can look at later**.



```
Syntax of the Set-Cookie HTTP Response Header:
Set-Cookie: NAME=OPAQUE\_STRING \
    [; expires= ] \
    [; path=] \
    [; domain=] \
    [; secure]

Syntax of the Cookie HTTP Request Header:
Cookie: NAME=OPAQUE\_STRING *[; NAME=OPAQUE\_STRING]
```

First proposal for state management on the web (Apr. 18, 1995)

Webpage complexity grows

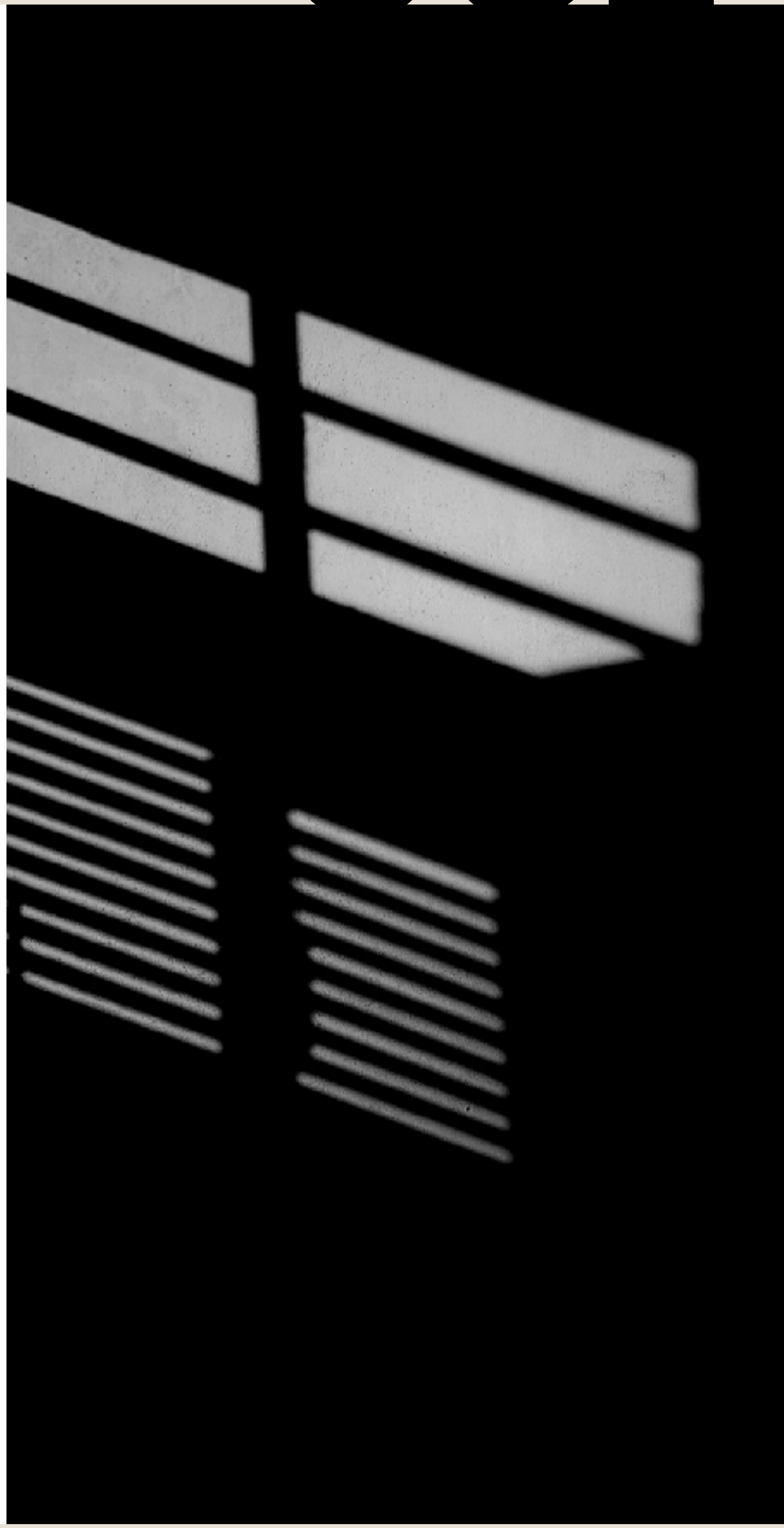
- In the early days of the Web, all content on a webpage came from the same **server**.
- An early, popular browser, **Netscape Navigator**, introduced the function of rendering two webpages in a single browsing window in 1996 (frames).
- This created a problem: could the second website access the cookies the first had laid?

The same origin policy

- The solution — the Same Origin Policy.
- Cookies only accessible by servers that share features (particularly the domain) of the one that laid them.
- A user visiting ucl.ac.uk should expect only ucl.ac.uk cookies to be read — not kcl.ac.uk cookies.

Crafty workarounds

- Didn’t fix the problem for long:
  - Websites started calling many distinct servers. Used to be 1, now 100s — because a website would instruct your computer to query many domains.
  - These many domains collaborate to share information about users’ Web usage and more — called Cookie Syncing.
- Google calls home with unique identifiers for at least 28% of all web page loads, while Facebook does the same for approximately 15%. The proportion is significantly higher in certain sectors, such as news, compared to others, such as banking.*
- Collaboration between trackers means that even under conservative estimates, 53 firms observe more than 91% of users’ browsing behaviour.**



*Arjaldo Karaj and others, ‘WhoTracks.Me: Shedding Light on the Opaque World of Online Tracking’ [2018] arXiv:180408959, 8;
** Muhammad Ahmad Bashir and Christo Wilson, ‘Diffusion of User Tracking Data in the Online Advertising Ecosystem’ (2018) 2018 Proceedings on Privacy Enhancing Technologies 85.

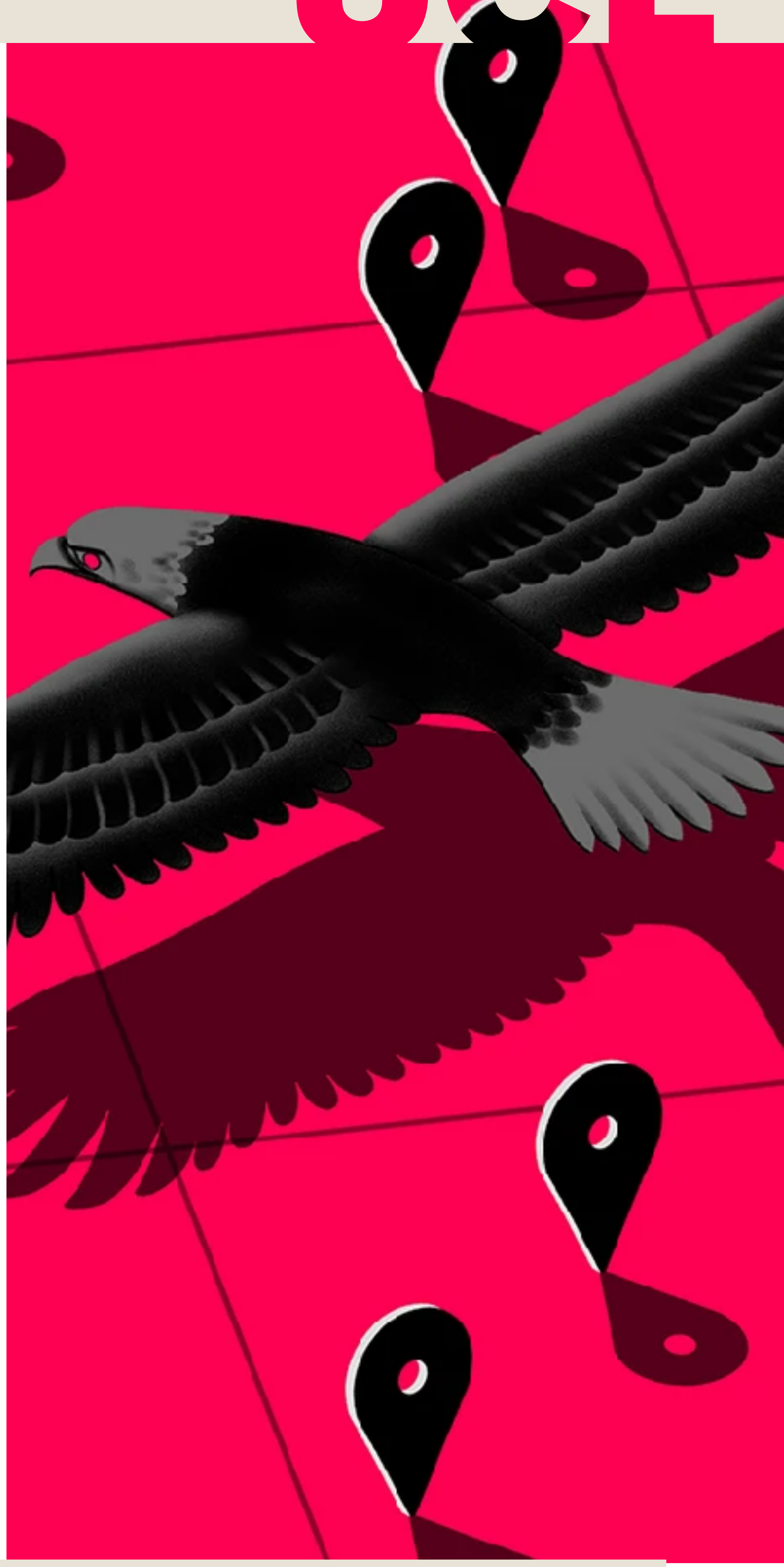
Apps are pretty bad

- Users have more ability to control the Web, through browsers. For apps, they have almost none.
- One recent study identified 2,121 separate advertising tracking services in apps in the Android ecosystem, which can be grouped by ownership into approximately 292 parent organisations.*
- Another study found that 88.4% of apps contained a tracker owned by Alphabet (Google), 42.6% by Facebook, 33.9% by Twitter, 26.3% by Verizon and 22.2% by Microsoft. 30% of News apps, 28% of Family apps, and 25% of Gaming & Entertainment apps contain trackers from more than ten distinct tracker companies.**

*Abbas Razaghpanah and others, 'Apps, Trackers, Privacy, and Regulators: A Global Study of the Mobile Tracking Ecosystem' (2018) 13–14 <http://eprints.networks.imdea.org/1744/>; **Reuben Binns and others, 'Third Party Tracking in the Mobile Ecosystem', Proceedings of the 10th ACM Conference on Web Science (ACM 2018) 27

This data isn't just used for advertising

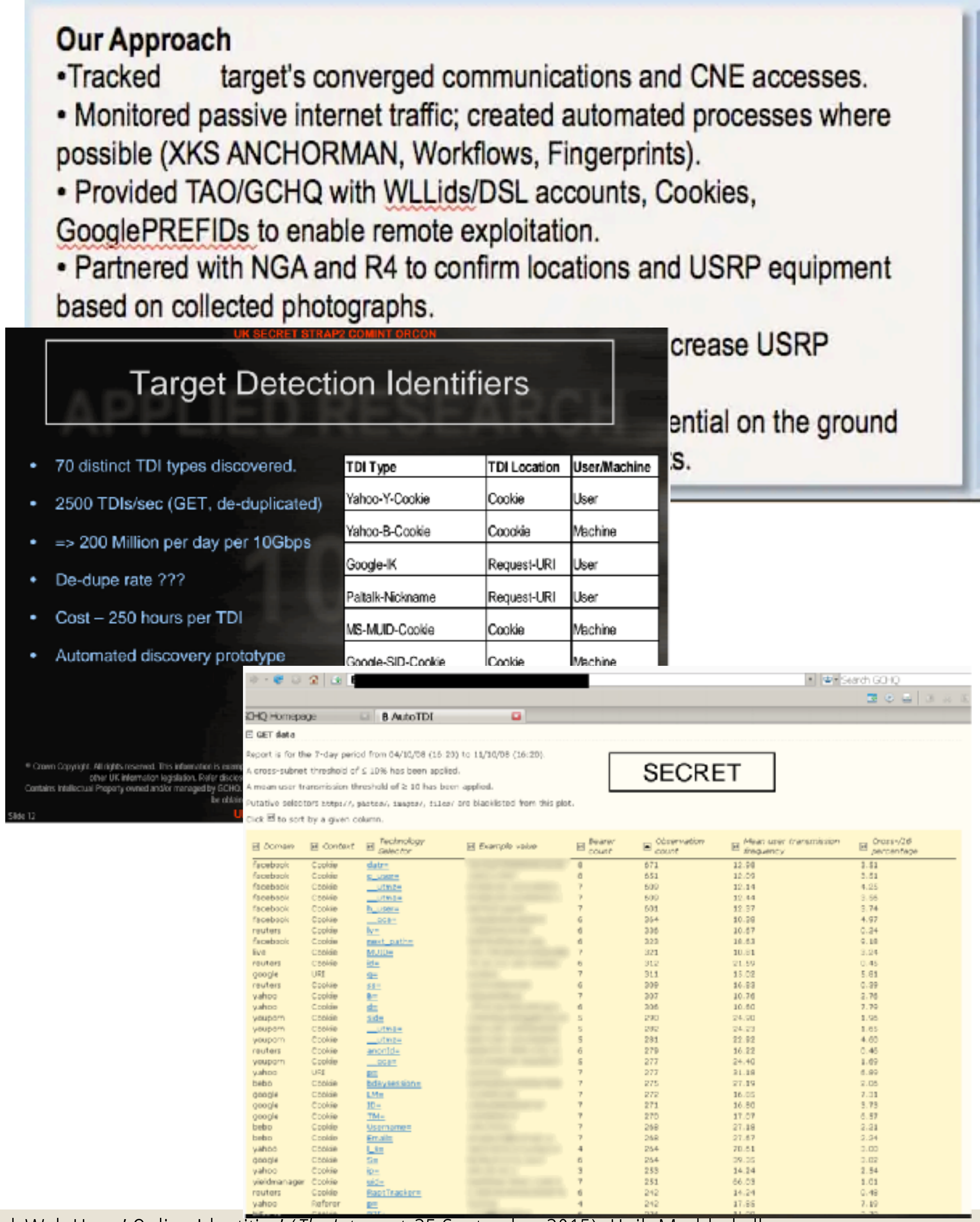
- The US military, Customs and Border Protection, the Secret Service and Homeland Security buy location data from adtech firms as a way of avoiding obtaining warrants.
  - 'X-Mode' trackers in apps: e.g. a Quar'an/prayer time app downloaded by 98m Muslims around the world; a Craigslist searching app and a spirit level app.
  - Bidstream data from real-time bidding (Venntel, Babel Street)
- Many vendors found selling data that can specifically be used to locate women who have visited abortion clinics (Kochava, SafeGraph, Placer.ai)



https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x, https://www.vice.com/en/article/jgxk3g/secret-service-phone-location-data-babel-street, https://www.vice.com/en/article/5d3gmb/documents-show-dhs-tracks-smartphones-across-the-country, https://www.vice.com/en/article/z343kw/ftc-sues-data-broker-kochava-selling-location-data-abortion-clinics

This infrastructure isn’t just used for advertising

- NSA and GCHQ utilise the uniquely identifying Google “PREF” cookies to single out a user’s computer and allow it to be remotely exploited using hacking tools developed by these state actors.
- DoubleClick cookies to reidentify Tor Browser users
- Major Belgacom hack achieved by GCHQ and CSEC through MUTANT BROTH, a system bulk-storing a range of cookies laid on popular websites, including those from Google and Facebook, in order to both identify users and build up a pattern of their daily habits and routines.



Our Approach
- Tracked   target's converged communications and CNE accesses.
- Monitored passive internet traffic; created automated processes where possible (XKS ANCHORMAN, Workflows, Fingerprints).
- Provided TAO/GCHQ with WLLids/DSL accounts, Cookies, GooglePREFIDs to enable remote exploitation.
- Partnered with NGA and R4 to confirm locations and USRP equipment based on collected photographs.

crease USRP

ential on the ground

s.

UK SECRET STRAP2 COMINT ORCON

Target Detection Identifiers

- 70 distinct TDI types discovered.
- 2500 TDIs/sec (GET, de-duplicated)
- => 200 Million per day per 10Gbps
- De-dupe rate ???
- Cost – 250 hours per TDI
- Automated discovery prototype

TDI Type	TDI Location	User/Machine
Yahoo-Y-Cookie	Cookie	User
Yahoo-B-Cookie	Coookie	Machine
Google-IK	Request-URI	User
Paltalk-Nickname	Request-URI	User
MS-MUID-Cookie	Cookie	Machine
Google-SID-Cookie	Cookie	Machine

© Crown Copyright. All rights reserved. This information is exem
other UK information legislation. Refer disc
Contains Intellectual Property owned and/or managed by GCHQ
be obtain

Slide 12

[redacted]

GET data

Report is for the 7-day period from 04/10/08 (15:20) to 11/10/08 (16:20).

A cross-subnet threshold of ≤ 10% has been applied.

A mean user transmission threshold of ≥ 10 has been applied.

Putative selectors http://, pastes/, images/, files/ are blacklisted from this plot.

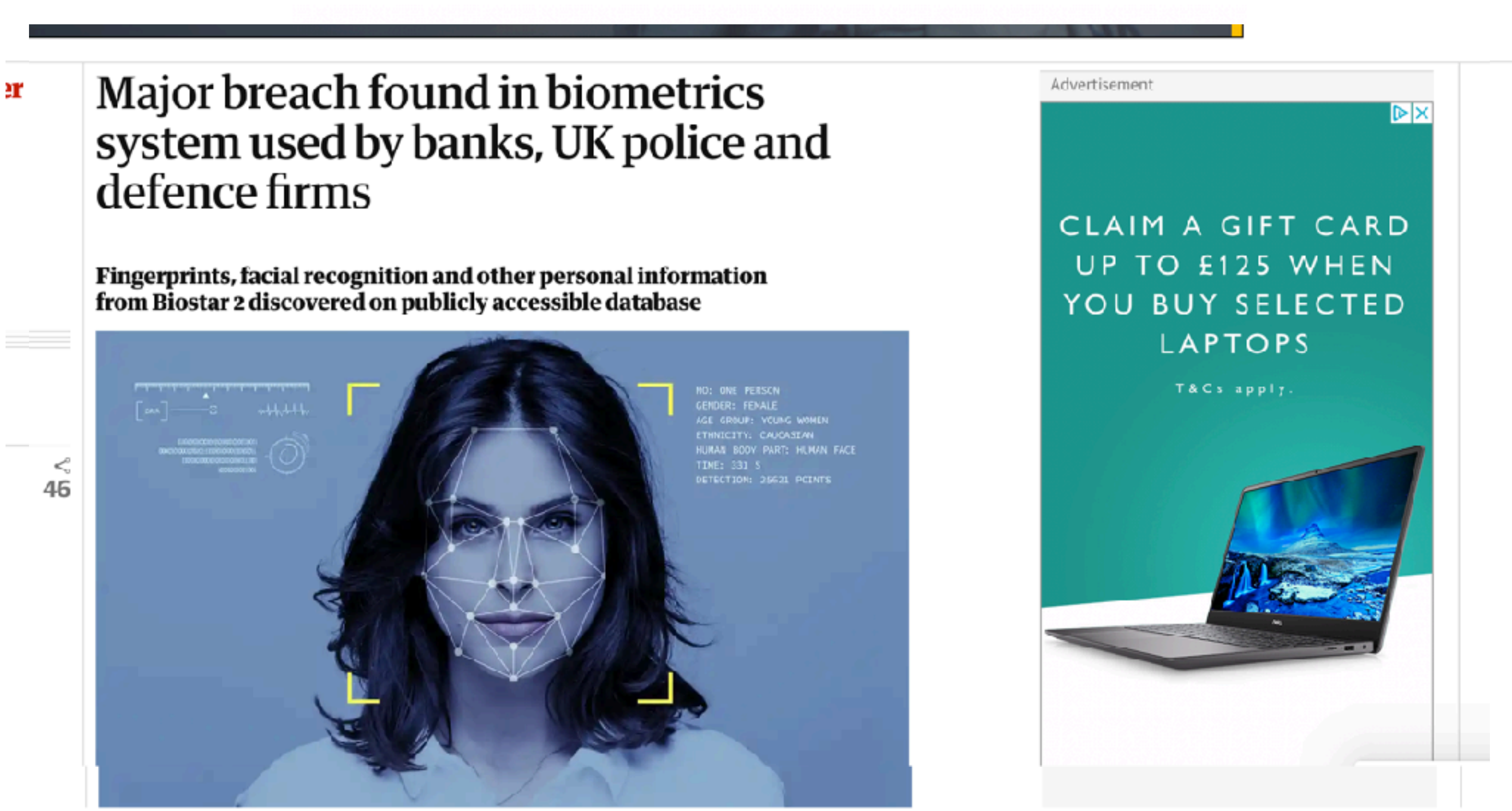
Click ⊞ to sort by a given column.

SECRET

Domain	Context	Technology Selector	Example value	Bearer count	Observation count	Mean user transmission frequency	Cross-/16 percentage
facebook	Cookie	datr=	[illegible]	8	671	12.98	3.51
facebook	Cookie	c_user=	[illegible]	8	651	12.09	5.51
facebook	Cookie	__utmz=	[illegible]	7	609	12.14	4.25
facebook	Cookie	__utma=	[illegible]	7	609	12.44	3.56
facebook	Cookie	h_user=	[illegible]	7	601	12.37	3.74
facebook	Cookie	__qca=	[illegible]	6	364	10.39	4.97
reuters	Cookie	lv=	[illegible]	6	336	10.87	0.24
facebook	Cookie	next_path=	[illegible]	6	323	16.83	9.18
live	Cookie	MUID=	[illegible]	7	321	10.81	3.24
reuters	Cookie	id=	[illegible]	6	312	21.59	0.45
google	URI	q=	[illegible]	7	311	15.02	5.61
reuters	Cookie	ss=	[illegible]	6	309	16.83	0.39
yahoo	Cookie	B=	[illegible]	7	307	10.76	2.76
yahoo	Cookie	d=	[illegible]	6	306	10.60	7.79
youporn	Cookie	sid=	[illegible]	5	290	24.90	1.96
youporn	Cookie	__utma=	[illegible]	5	282	24.23	1.65
youporn	Cookie	__utmz=	[illegible]	5	281	22.92	4.60
reuters	Cookie	anonId=	[illegible]	6	279	16.22	0.46
youporn	Cookie	__qca=	[illegible]	5	277	24.40	1.69
yahoo	URI	p=	[illegible]	7	273	31.18	6.89
bebo	Cookie	bdaysession=	[illegible]	7	275	27.19	2.06
google	Cookie	LM=	[illegible]	7	272	16.05	7.31
google	Cookie	ID=	[illegible]	7	271	16.50	3.73
google	Cookie	TM=	[illegible]	7	270	17.07	6.57
bebo	Cookie	Username=	[illegible]	7	268	27.18	2.21
bebo	Cookie	Email=	[illegible]	7	268	27.67	2.34
yahoo	Cookie	L_id=	[illegible]	4	264	70.51	3.00
google	Cookie	S=	[illegible]	6	264	39.35	3.02
yahoo	Cookie	ip=	[illegible]	3	253	14.24	2.54
yieldmanager	Cookie	uid=	[illegible]	7	251	66.03	1.01
reuters	Cookie	RaptTracker=	[illegible]	6	242	14.24	0.48
yahoo	Referer	p=	[illegible]	4	242	17.66	7.19

Ashkan Soltani and others, ‘NSA Uses Google Cookies to Pinpoint Targets for Hacking’, *Washington Post* (11 December 2013); Ryan Gallagher, ‘Profiled: From Radio to Porn, British Spies Track Web Users’ Online Identities’ (*The Intercept*, 25 September 2015); Huib Modderkolk, ‘Waarom kwam de Britse geheime dienst zo makkelijk weg met het hacken van Belgacom?’ (*de Volkskrant*, 17 February 2018)

But when they are used for ads, it’s pretty bad too.



Major breach found in biometrics system used by banks, UK police and defence firms

Fingerprints, facial recognition and other personal information from Biostar 2 discovered on publicly accessible database

Advertisement

CLAIM A GIFT CARD UP TO £125 WHEN YOU BUY SELECTED LAPTOPS

T&Cs apply.

Real-Time Bidding

From about 2010, automated auctions for your eyeballs.

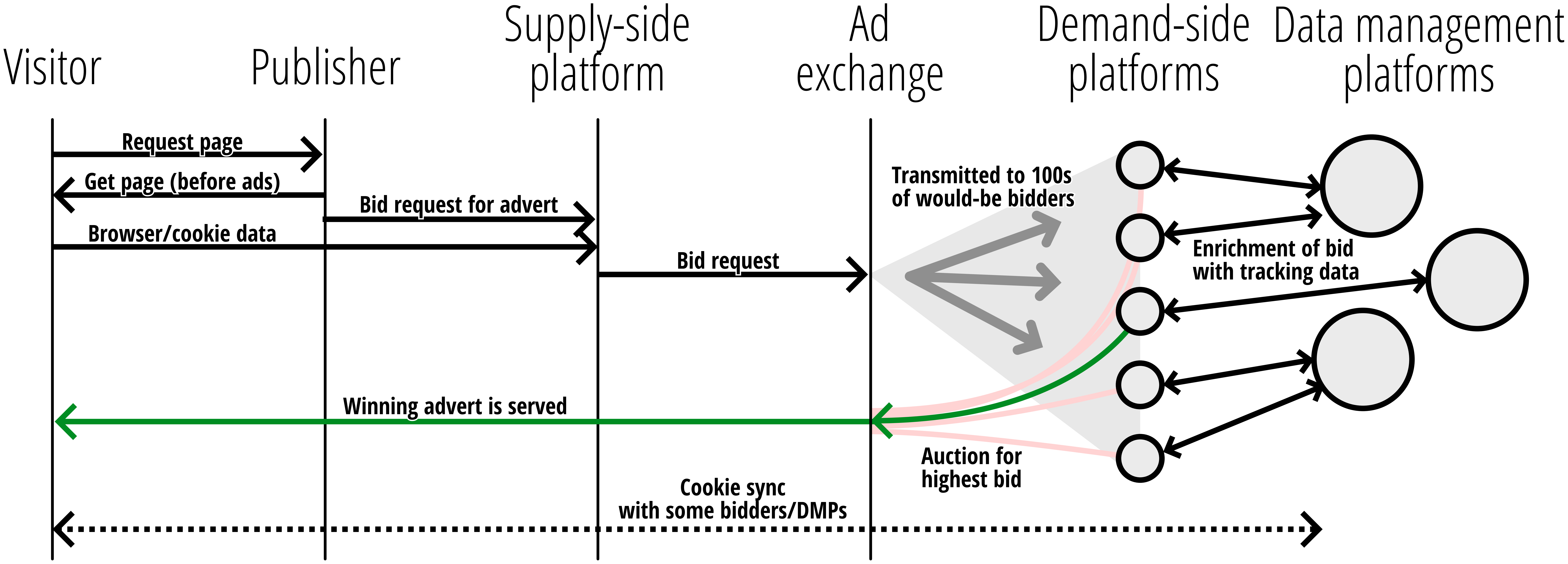
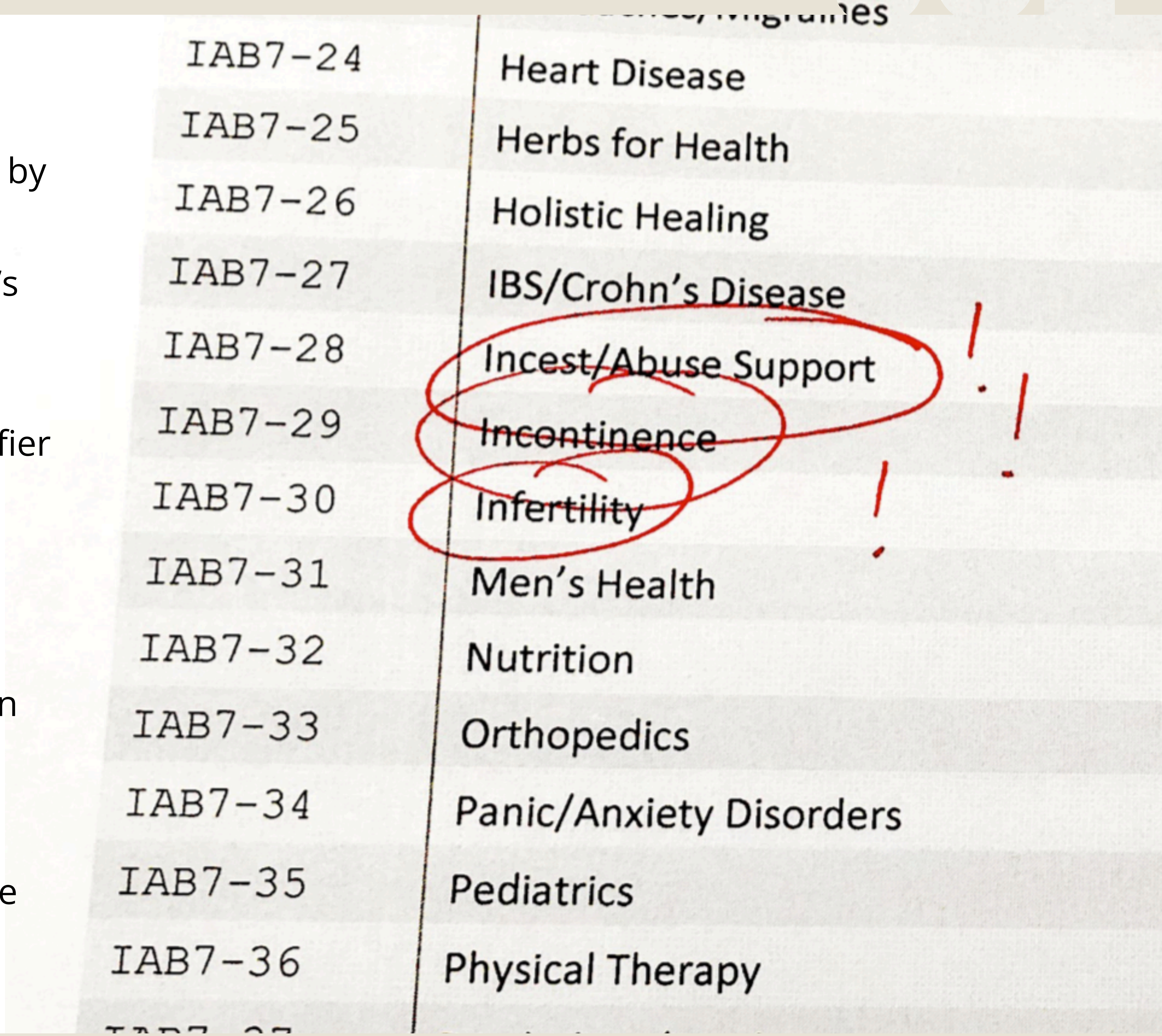


Diagram: Michael Veale and Frederik Zuiderveen Borgesius, 'Adtech and Real-Time Bidding under European Data Protection Law' (2022) 23 German Law Journal 226.

Data sent to bidders each time this happens

- Site
  - URL of the site being visited
  - Site category or topic
- Device
  - Operating system
  - Browser software and version
  - Device manufacturer, model
  - Mobile provider
  - Screen dimensions

- User
  - Unique identifiers set by vendor and/or buyer.
  - Advertising exchange's cookie ID.
  - A demand-side platform's user identifier
  - Year of Birth
  - Gender
  - Interests
  - Metadata reporting on consent provided
- Geography
  - Longitude and latitude
  - Postal/ZIP code

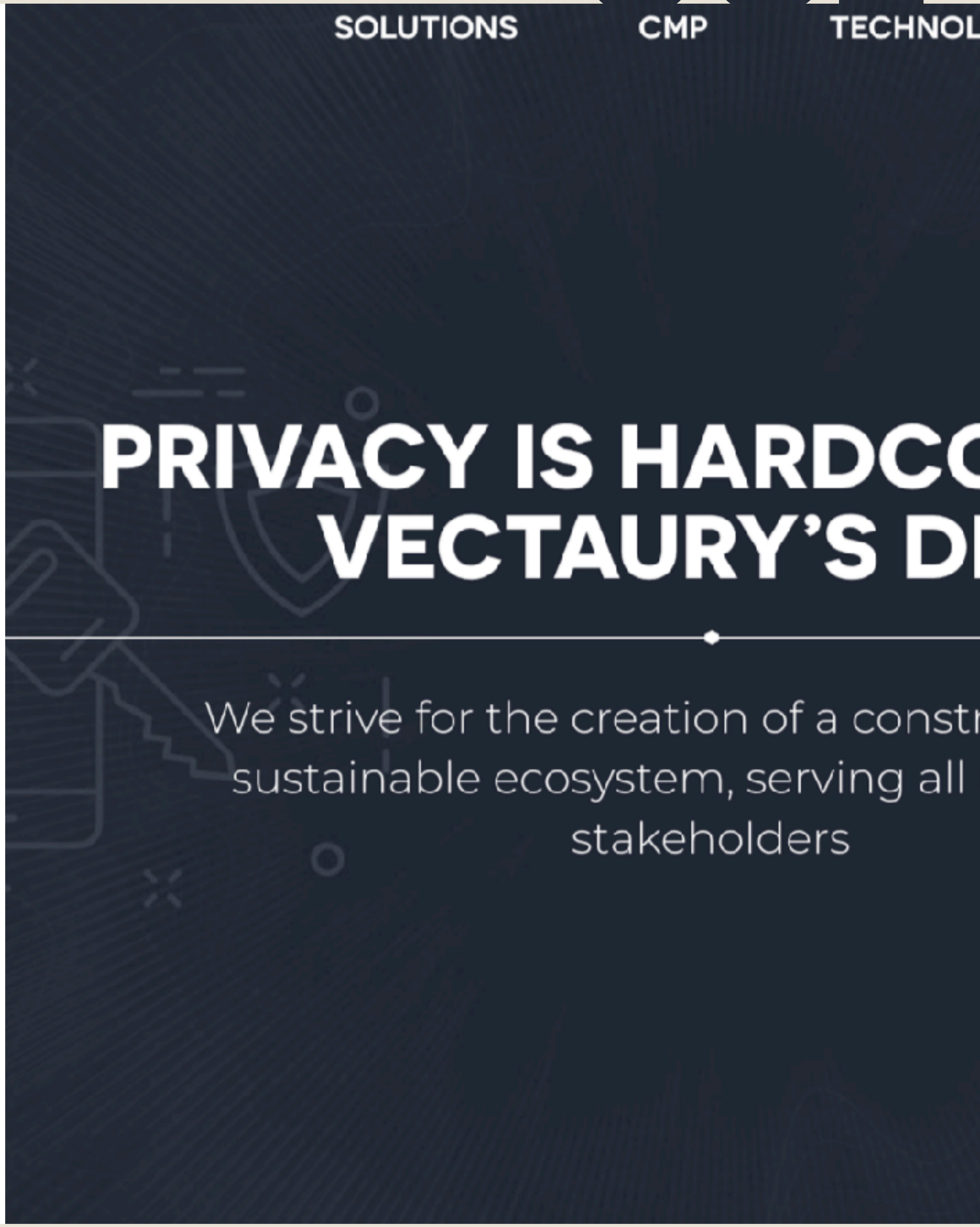


	aches/Migraines
IAB7-24	Heart Disease
IAB7-25	Herbs for Health
IAB7-26	Holistic Healing
IAB7-27	IBS/Crohn's Disease
IAB7-28	Incest/Abuse Support
IAB7-29	Incontinence
IAB7-30	Infertility
IAB7-31	Men's Health
IAB7-32	Nutrition
IAB7-33	Orthopedics
IAB7-34	Panic/Anxiety Disorders
IAB7-35	Pediatrics
IAB7-36	Physical Therapy
IAB7-37	

! ! !

… and retained

- Bid requests go to hundreds or thousands of companies; little oversight.
- **Vectaury** in France — small company ,with only 3.5m€ annual turnover — retained 68m bid request records (and fined by the French data regulator, CNIL) in 2018.
- Their website even claimed that they discarded 70% of all data, and only kept any of it for 12 months meaning that this small company was possibly sent 1/4 billion bid requests in just a single year.



PRIVACY IS HARDCO
VECTAURY'S DI

We strive for the creation of a constr
sustainable ecosystem, serving all
stakeholders

Data at scale for real-time bidding (RTB)

Leading RTB exchanges, daily bid request estimates

Index Exchange	50 billion[ii]
OpenX	60 billion+[i]
Rubicon Project	Unknown. Claims to reach 1 billion people's devices.[iii]
PubMatic	70 billion+[iv]
Oath/AOL	90 billion[v]
AppNexus	131 billion[vi]
Smaato	214 billion[vii]
Google DoubleClick	Unknown. DoubleClick is the dominant exchange.

[i] "Tour IX's Amsterdam and Frankfurt Data Centers", Index Exchange, 2 July 2018 (URL: https://www.indexexchange.com/tour-ix-amsterdam-frankfurt-data-centers/).

[ii] "OpenX Ad Exchange", OpenX (URL: https://www.openx.com/uk_en/products/ad-exchange/).

[iii] "Buyers", Rubicon Project, (URL: https://rubiconproject.com/buyers/).

[iv] "How PubMatic Is Learning Machine Learning", PubMatic, 25 January 2019 (URL: https://pubmatic.com/blog/learning-machine-learning/)

[v] "Maximize yield with Oath's publisher offerings", Oath, 3 April 2018 (URL: https://www.oath.com/insights/maximize-yield-with-oath-s-publisher-offerings/)

[vi] 500 Billion / 29.6 = 18.6 billion impressions per day. Using AppNexus 1:11.5 ratio, this is 214 auctions per day. 500+ impressions figure cited in "Optimize your mobile strategy", Smaato, (URL: https://www.smaato.com/).

[vii] "Transacting at a peak of 11.4 billion daily impressions, our marketplace handles more traffic each day than Visa, Nasdaq, and the NYSE combined" at https://www.appnexus.com/sell. Note that in 2017, AppNexus said in "AppNexus Scales with DriveScale", 2017, (URL: http://go.drivescale.com/rs/451-ESR-800/images/DRV_Case_Study_AppNexus-final.v1.pdf) that 10.7 billion "impressions transacted" came as a result of running 123 billion auctions. The impressions transacted to auctions ratio appears to be roughly 1:11.5. Therefore, the 11.4 daily impressions reported in 2018 equates to 131 billion auctions per day.

“Nanotargeting”

- Some ad infrastructures facilitate messages to be targeted to the level of specific individuals.
- Studies on Facebook’s ad infrastructure have modelled that this “nanotargeting” is possible using either the 4 rarest interests of an individual or the 22 random interests from the interests set Facebook assigns — both options make users unique on Facebook with a 90% probability (González-Cabañas et al., 2021).
- Various “war stories” of this occurring, from intimate partner abuse to Labour Party HQ targeting Jeremy Corbyn.

José González-Cabañas and others, ‘Unique on Facebook: Formulation and Evidence of (Nano)Targeting Individual Users with Non-PII Data’ in (ACM 11 February 2021) Proceedings of the 21st ACM Internet Measurement Conference 464.

‘Cookie Banners’

No cookie banner??

SIGN UP TO NEWSLETTER

SEARCH

NEWS ACT CAMPAIGNS LEARN IMPACT ABOUT DONATE

LONG READ

We asked five menstruation apps for our data and here is what we found...

We asked five menstruation apps to give us access to our data. We got a dizzying dive into the most intimate information about us.

FR

For a world where technology

- Personal data in data protection law: information relating to an identified or identifiable natural person.
- Data protection law (e.g. the GDPR) requires a ‘lawful basis’ for all personal data processing
  - **Not a consent-first law**: If you are doing something aligned with the user, not using sensitive categories of data like ethnicity or health, you typically won’t need consent.
- However, ePrivacy Directive: consent for storing or retrieving data for terminal devices (history of rootkits, tracking) if not necessary for the requested service.

Sources of law for consent

GDPR (operative provisions)

Article 4

Definitions

11. ‘consent’ of the data subject means any **freely given, specific, informed and unambiguous indication** of the data subject's wishes by which he or she, **by a statement or by a clear affirmative action**, signifies agreement to the processing of personal data relating to him or her;

Article 7

Conditions for consent

1. Where processing is based on consent, the controller shall be able to **demonstrate** that the data subject has consented to processing of his or her personal data.

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is **clearly distinguishable from the other matters**, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. The data subject shall have the **right to withdraw his or her consent at any time**. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. **It shall be as easy to withdraw as to give consent.**

4. **When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.**

Sources of law for consent

GDPR (recitals)

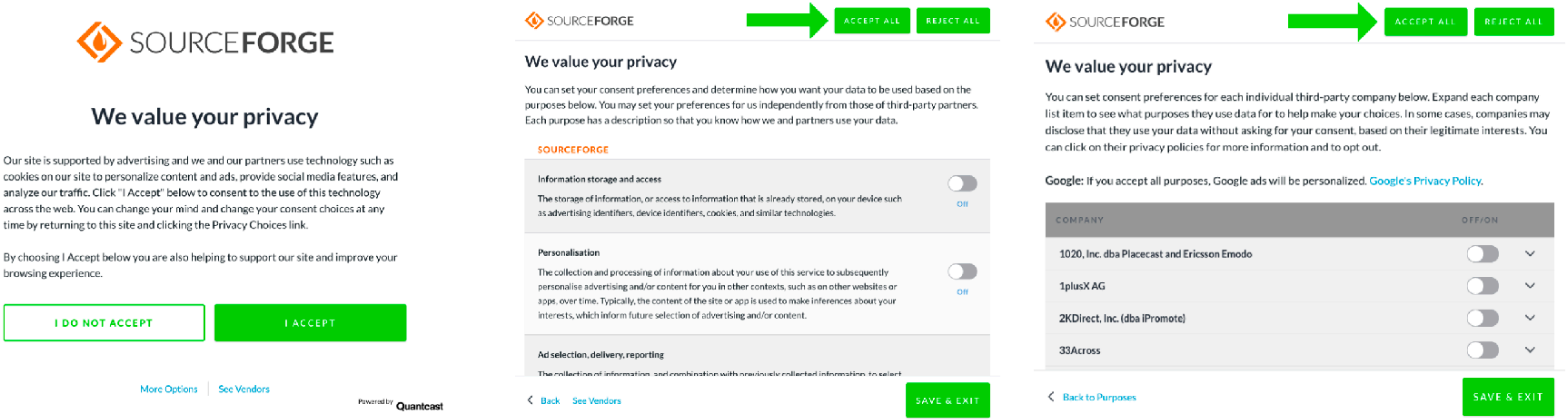
Recital 32

Consent should be given by a **clear affirmative act** establishing a **freely given, specific, informed and unambiguous indication** of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include **ticking a box when visiting an internet website**, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. **Silence, pre-ticked boxes or inactivity should not therefore constitute consent.** Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. **If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.**

With hundreds of trackers… how?

Consent management platforms emerge

Legal entrepreneurship of an unsavoury kind



We value your privacy

Our site is supported by advertising and we and our partners use technology such as cookies on our site to personalize content and ads, provide social media features, and analyze our traffic. Click "I Accept" below to consent to the use of this technology across the web. You can change your mind and change your consent choices at any time by returning to this site and clicking the Privacy Choices link.

By choosing I Accept below you are also helping to support our site and improve your browsing experience.

(a) First page

We value your privacy

You can set your consent preferences and determine how you want your data to be used based on the purposes below. You may set your preferences for us independently from those of third-party partners. Each purpose has a description so that you know how we and partners use your data.

Information storage and access

The storage of information, or access to information that is already stored, on your device such as advertising identifiers, device identifiers, cookies, and similar technologies.

Personalisation

The collection and processing of information about your use of this service to subsequently personalise advertising and/or content for you in other contexts, such as on other websites or apps, over time. Typically, the content of the site or app is used to make inferences about your interests, which inform future selection of advertising and/or content.

Ad selection, delivery, reporting

The collection of information, and combination with previously collected information, to select

(b) Categories and purposes

We value your privacy

You can set consent preferences for each individual third-party company below. Expand each company list item to see what purposes they use data for to help make your choices. In some cases, companies may disclose that they use your data without asking for your consent, based on their legitimate interests. You can click on their privacy policies for more information and to opt out.

Google: If you accept all purposes, Google ads will be personalized. Google's Privacy Policy.

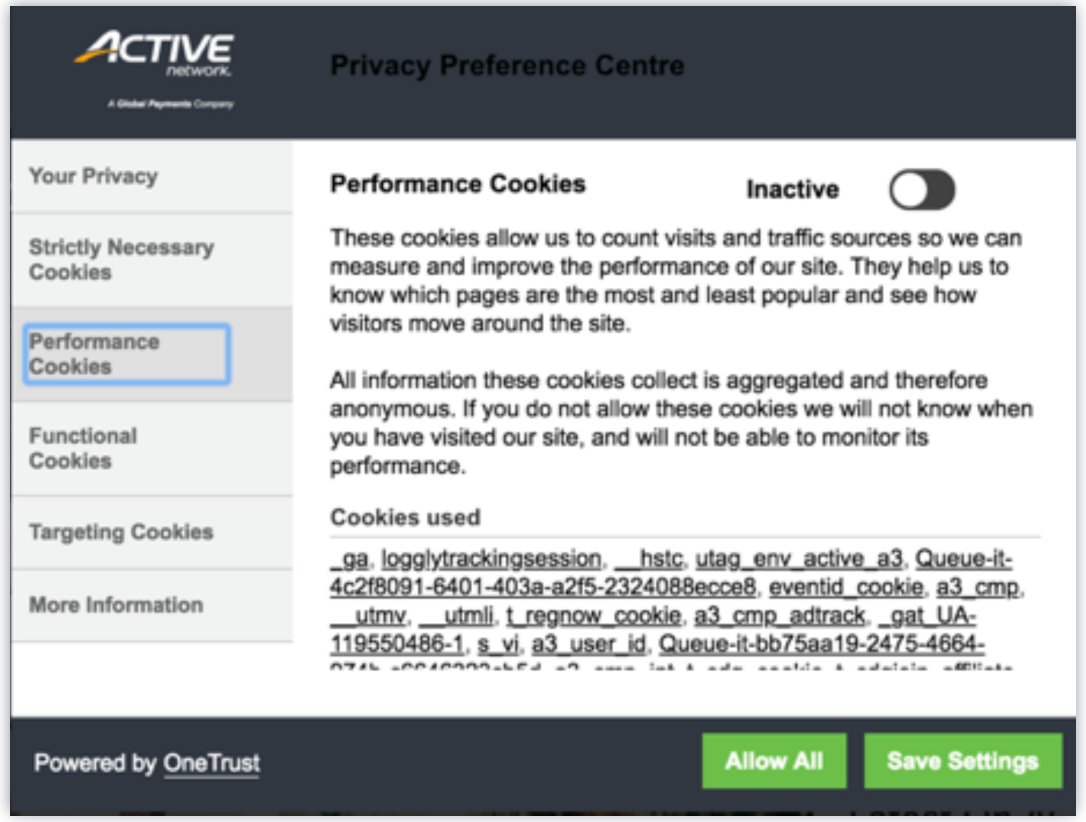
COMPANY	OFF/ON
1020, Inc. dba Placecast and Ericsson Emodo	○
1plusX AG	○
2KDirect, Inc. (dba iPromote)	○
33Across	○

(c) Vendors/third-parties

Figure 1. The three components of the QuantCast CMP on https://sourceforge.net as of September 2019.

Many vendors: but are they compliant with the law?

OneTrust



Privacy Preference Centre

- Your Privacy
- Strictly Necessary Cookies
- Performance Cookies
- Functional Cookies
- Targeting Cookies
- More Information

Performance Cookies Inactive

These cookies allow us to count visits and traffic sources so we can measure and improve the performance of our site. They help us to know which pages are the most and least popular and see how visitors move around the site.

All information these cookies collect is aggregated and therefore anonymous. If you do not allow these cookies we will not know when you have visited our site, and will not be able to monitor its performance.

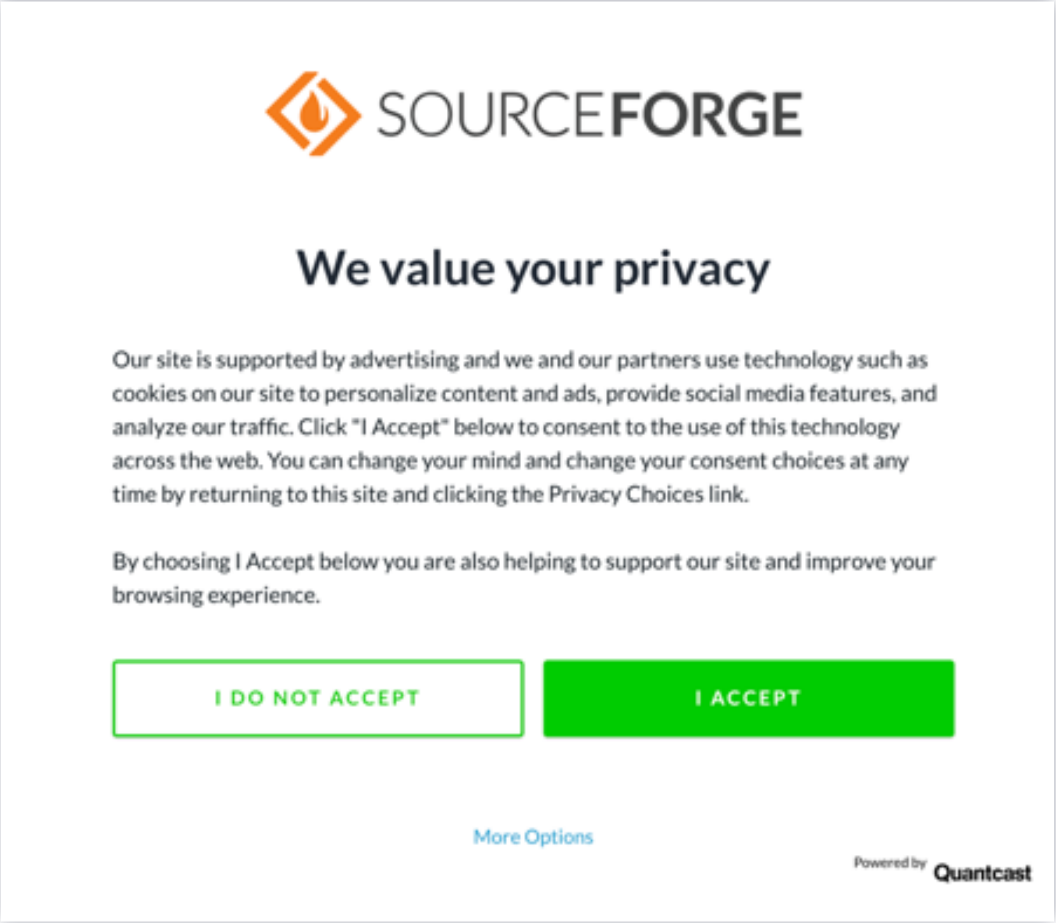
Cookies used

_ga, logglytrackingsession, __hstc, utag_env_active_a3, Queue-it-4c2f8091-6401-403a-a2f5-2324088ecce8, eventid_cookie, a3_cmp, __utmv, __utmli, t_regnow_cookie, a3_cmp_adtrack, _gat_UA-119550486-1, s_vi, a3_user_id, Queue-it-bb75aa19-2475-4664-

Powered by OneTrust

Allow All | Save Settings

Quantcast



We value your privacy

Our site is supported by advertising and we and our partners use technology such as cookies on our site to personalize content and ads, provide social media features, and analyze our traffic. Click "I Accept" below to consent to the use of this technology across the web. You can change your mind and change your consent choices at any time by returning to this site and clicking the Privacy Choices link.

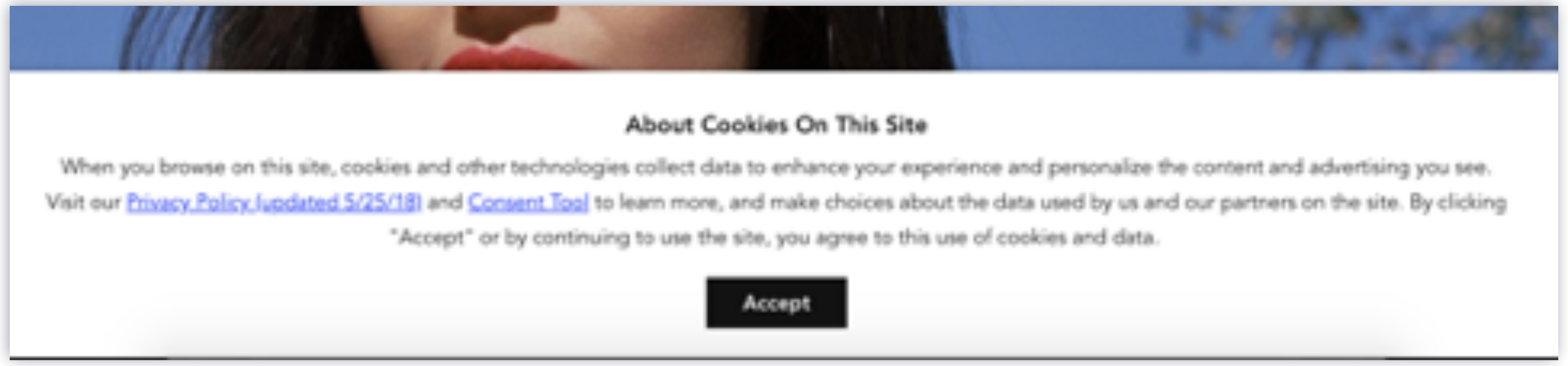
By choosing I Accept below you are also helping to support our site and improve your browsing experience.

I DO NOT ACCEPT | I ACCEPT

More Options

Powered by Quantcast

CrownPeak

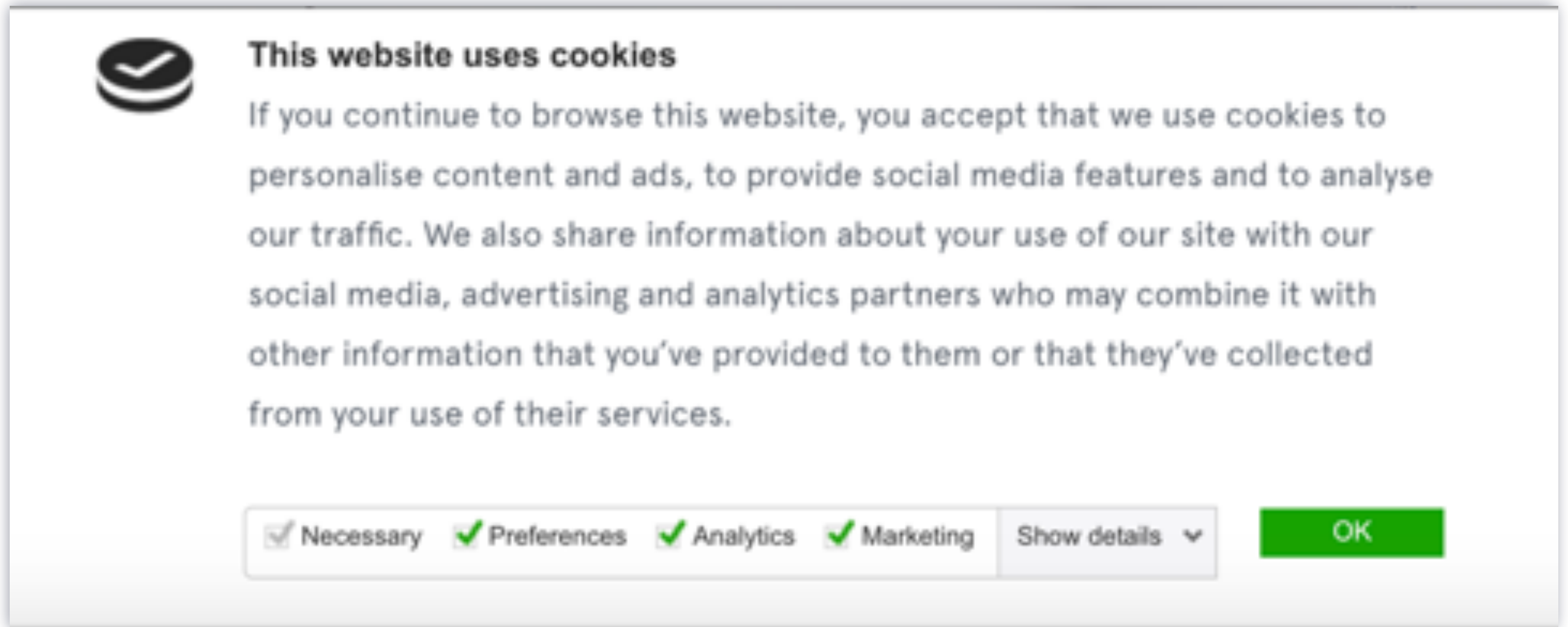


About Cookies On This Site

When you browse on this site, cookies and other technologies collect data to enhance your experience and personalize the content and advertising you see. Visit our Privacy Policy (updated 5/25/18) and Consent Tool to learn more, and make choices about the data used by us and our partners on the site. By clicking "Accept" or by continuing to use the site, you agree to this use of cookies and data.

Accept

CookieBot

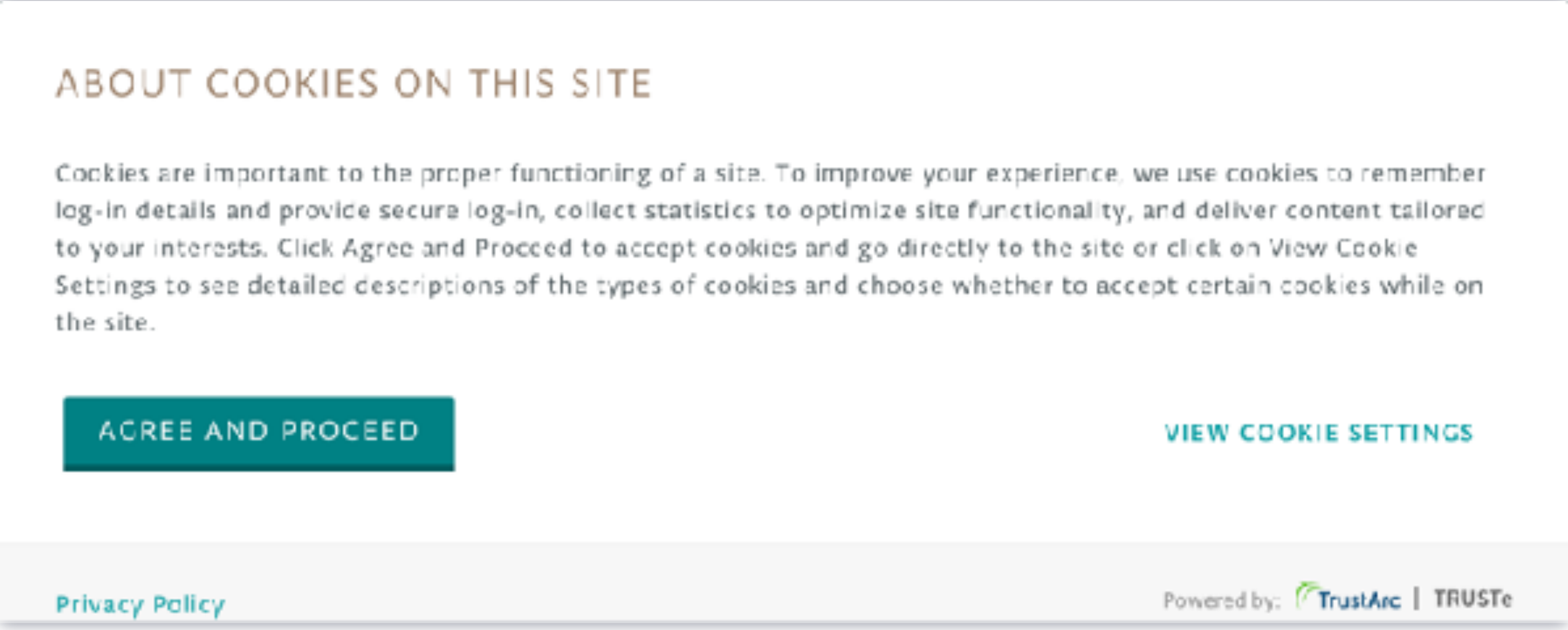


This website uses cookies

If you continue to browse this website, you accept that we use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

✓ Necessary ✓ Preferences ✓ Analytics ✓ Marketing | Show details | OK

TrustArc



ABOUT COOKIES ON THIS SITE

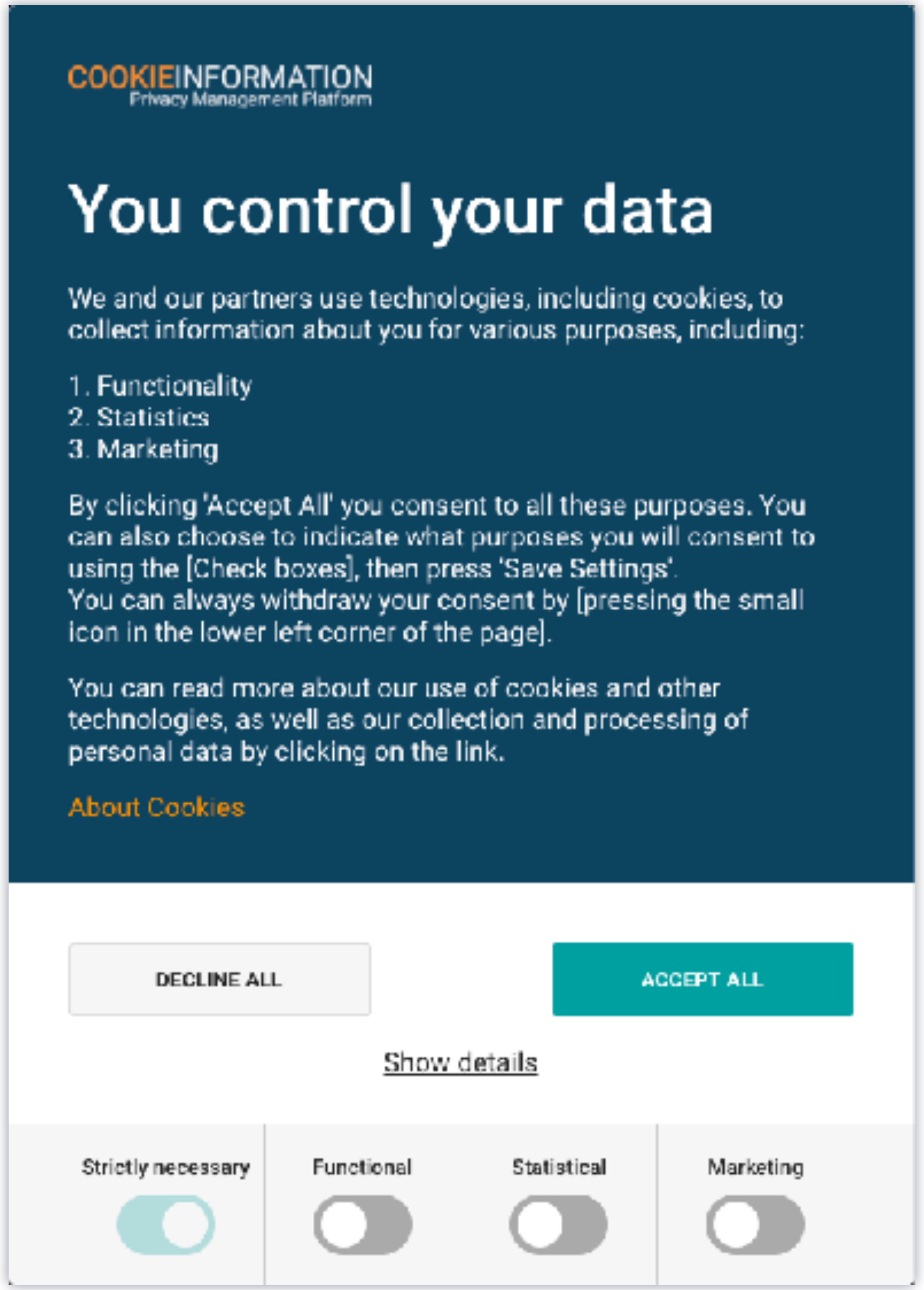
Cookies are important to the proper functioning of a site. To improve your experience, we use cookies to remember log-in details and provide secure log-in, collect statistics to optimize site functionality, and deliver content tailored to your interests. Click Agree and Proceed to accept cookies and go directly to the site or click on View Cookie Settings to see detailed descriptions of the types of cookies and choose whether to accept certain cookies while on the site.

AGREE AND PROCEED | VIEW COOKIE SETTINGS

Privacy Policy

Powered by: TrustArc | TRUSTe

Cookieinformation



COOKIEINFORMATION
Privacy Management Platform

You control your data

We and our partners use technologies, including cookies, to collect information about you for various purposes, including:

1. Functionality
2. Statistics
3. Marketing

By clicking 'Accept All' you consent to all these purposes. You can also choose to indicate what purposes you will consent to using the [Check boxes], then press 'Save Settings'.
You can always withdraw your consent by [pressing the small icon in the lower left corner of the page].

You can read more about our use of cookies and other technologies, as well as our collection and processing of personal data by clicking on the link.

About Cookies

DECLINE ALL | ACCEPT ALL

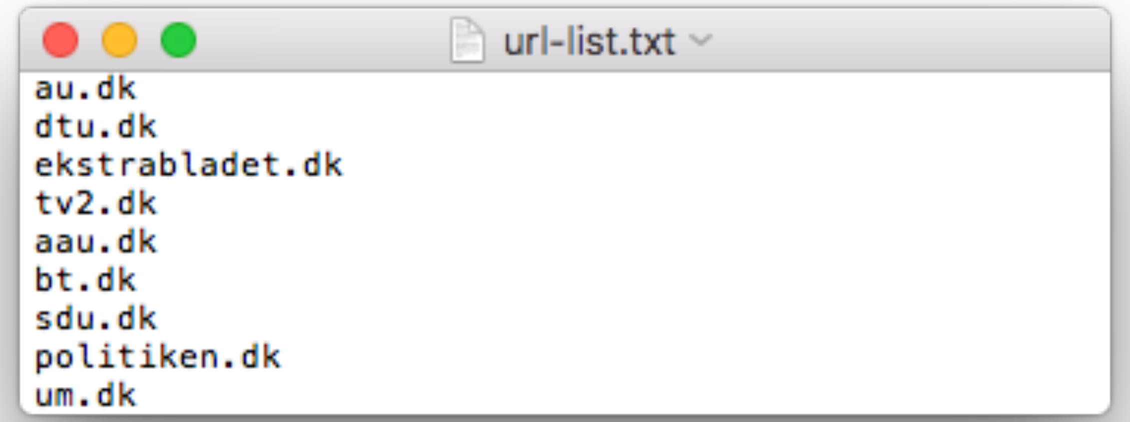
Show details

Strictly necessary ● | Functional ○ | Statistical ○ | Marketing ○

Empirical, computational legal analysis to find out

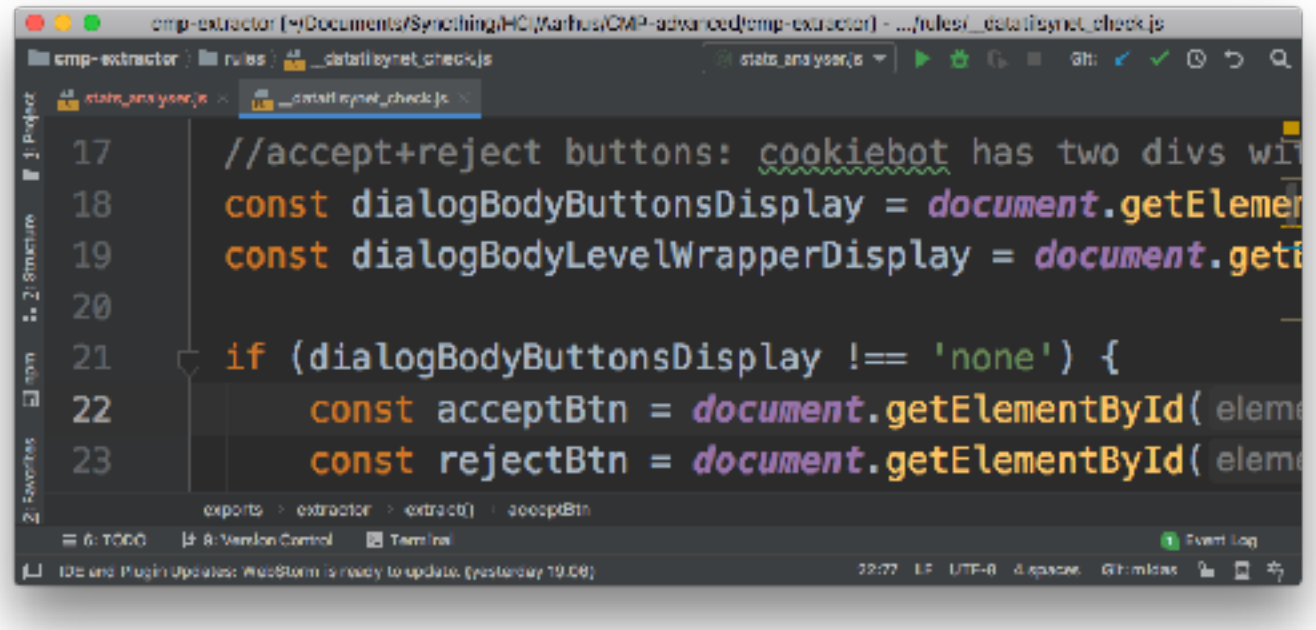
- Together with Aarhus University and MIT, we investigated whether these interfaces were providing valid consent under EU law.
- Built a bespoke *web scraper* and fed it the top 10K UK websites in 2019. We coded it to be able to analyse the top 5 CMPs to see how they were configured.

List of URLs to check



```
au.dk
dtu.dk
ekstrabladet.dk
tv2.dk
aau.dk
bt.dk
sdu.dk
politiken.dk
um.dk
```

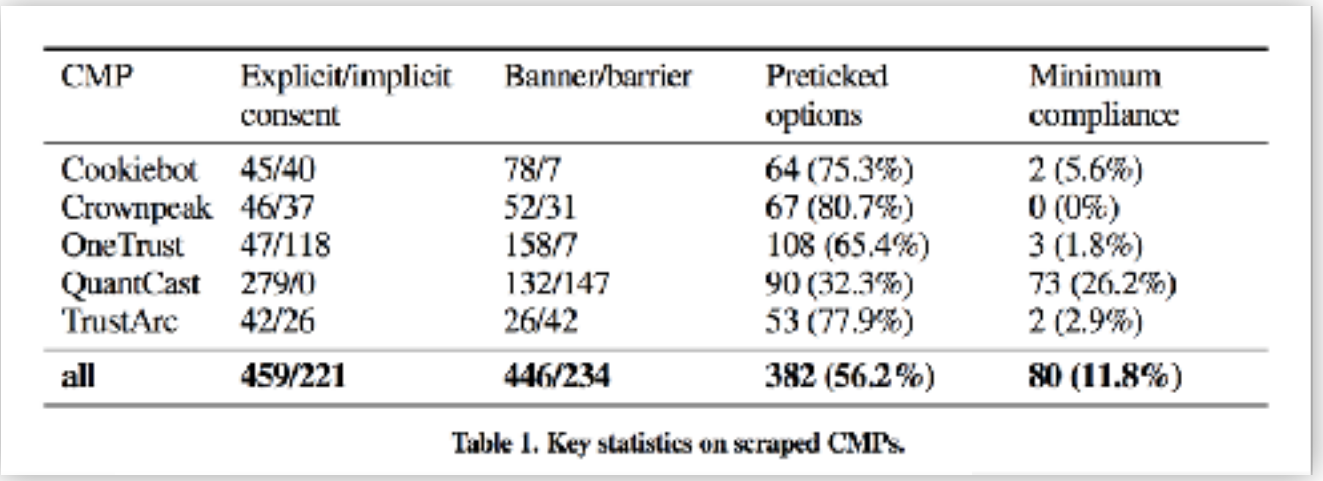
Software analyses pop-ups



```
//accept+reject buttons: cookiebot has two divs wi
const dialogBodyButtonsDisplay = document.getElemen
const dialogBodyLevelWrapperDisplay = document.getE

if (dialogBodyButtonsDisplay !== 'none') {
    const acceptBtn = document.getElementById( eleme
    const rejectBtn = document.getElementById( eleme
```

Returns data on compliance



CMP	Explicit/implicit consent	Banner/barrier	Preticked options	Minimum compliance
Cookiebot	45/40	78/7	64 (75.3%)	2 (5.6%)
Crownpeak	46/37	52/31	67 (80.7%)	0 (0%)
OneTrust	47/118	158/7	108 (65.4%)	3 (1.8%)
QuantCast	279/0	132/147	90 (32.3%)	73 (26.2%)
TrustArc	42/26	26/42	53 (77.9%)	2 (2.9%)
all	**459/221**	**446/234**	**382 (56.2%)**	**80 (11.8%)**

Table 1. Key statistics on scraped CMPs.

Midas Nouwens and others, 'Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence' in (ACM 2020) Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI 2020).

And what did we find?

Turned case law into three legal tests

1. No optional boxes preticked
2. Reject all as easy as Accept all
3. Consent is explicit

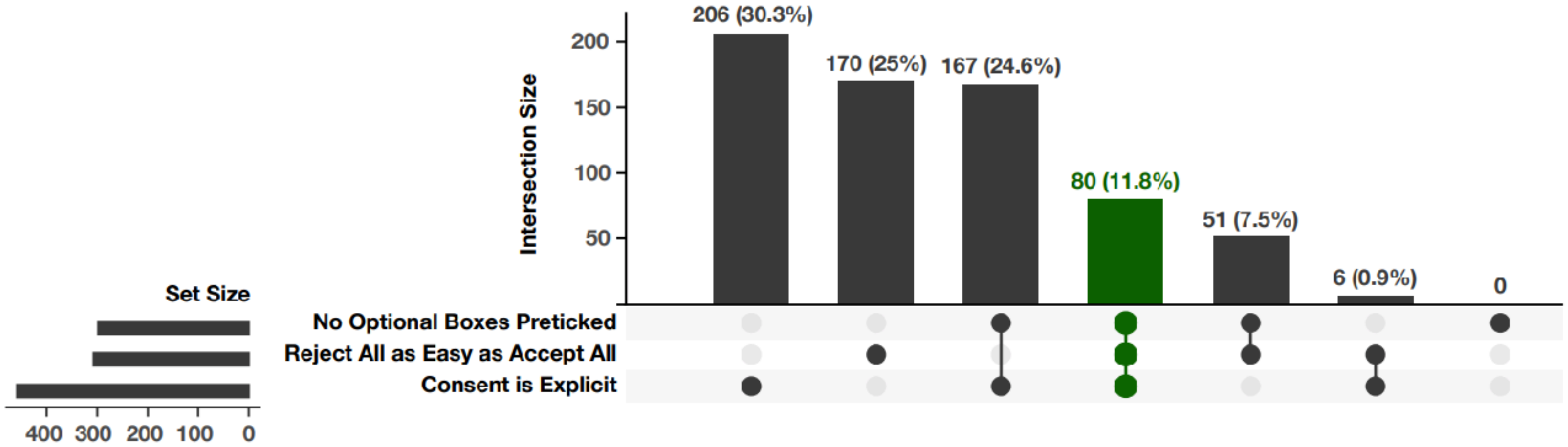
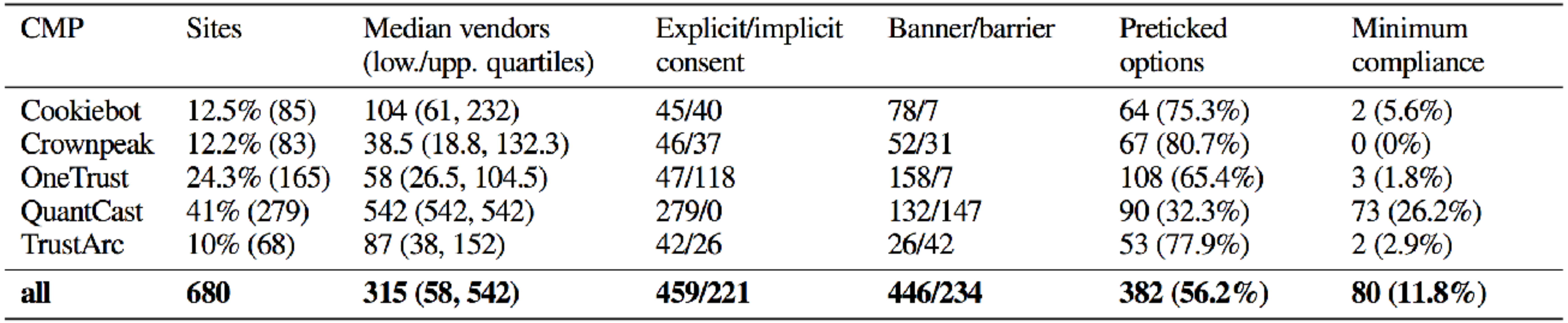


Figure 2. UpSet diagram [16, 36] of sites by adherence to three core conditions of EU law. Sites meeting all three in green.



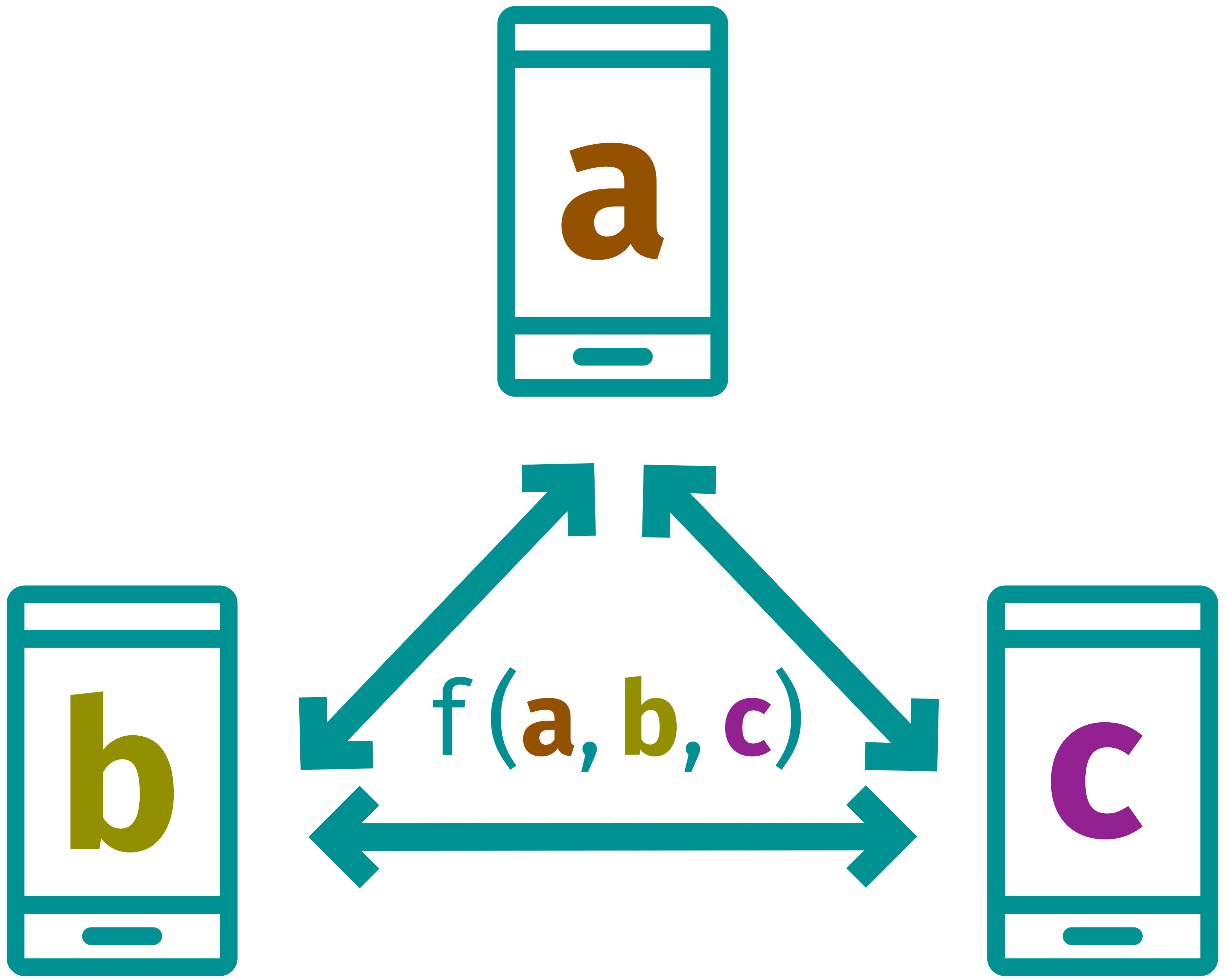
CMP	Sites	Median vendors (low./upp. quartiles)	Explicit/implicit consent	Banner/barrier	Preticked options	Minimum compliance
Cookiebot	12.5% (85)	104 (61, 232)	45/40	78/7	64 (75.3%)	2 (5.6%)
Crownpeak	12.2% (83)	38.5 (18.8, 132.3)	46/37	52/31	67 (80.7%)	0 (0%)
OneTrust	24.3% (165)	58 (26.5, 104.5)	47/118	158/7	108 (65.4%)	3 (1.8%)
QuantCast	41% (279)	542 (542, 542)	279/0	132/147	90 (32.3%)	73 (26.2%)
TrustArc	10% (68)	87 (38, 152)	42/26	26/42	53 (77.9%)	2 (2.9%)
all	**680**	**315 (58, 542)**	**459/221**	**446/234**	**382 (56.2%)**	**80 (11.8%)**

Table 1. Key statistics on scraped CMPs.

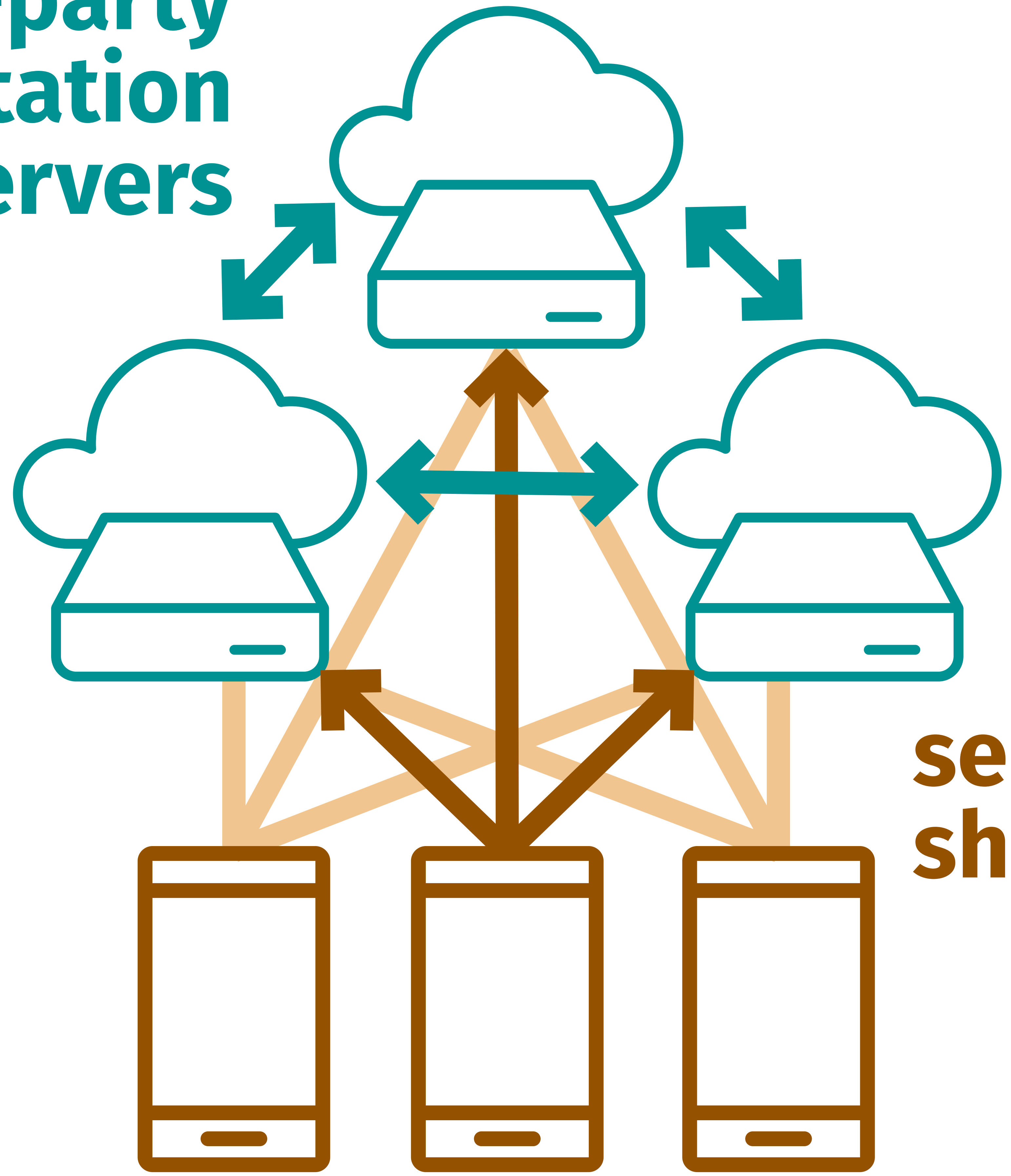
Midas Nouwens and others, 'Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence' in (ACM 2020) Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI 2020).

Future of Targeting

Example: Multi-party computation



multi-party computation among servers



secret sharing

On-device targeting

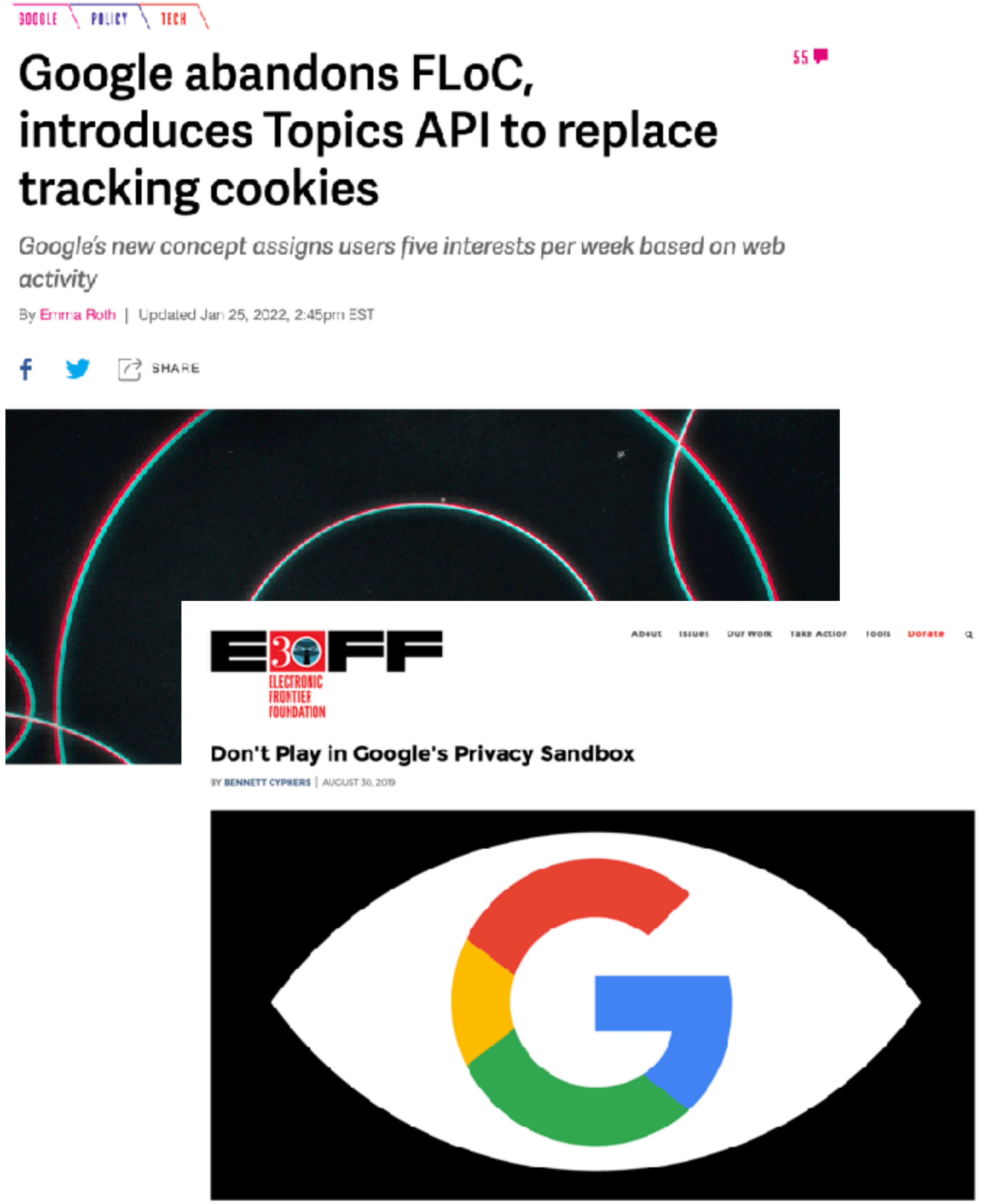
Let’s do it at my place instead

- Can we target users in as before, but without data leaving devices?
- Train shared models with privacy enhancing data analysis so tracking data never leaves the phone.
- Use other technologies such as ‘zero-knowledge proofs’ — or just locked down platforms — to check individuals are profiling themselves sufficiently, seeing the adverts.

Michael Veale, ‘Future of online advertising: Adtech’s new clothes might redefine privacy more than they reform profiling’ (netzpolitik.org, 25 February 2022) <https://netzpolitik.org/2022/future-of-online-advertising-adtechs-new-clothes-might-redefine-privacy-more-than-they-reform-profiling-cookies-meta-mozilla-apple-google/> accessed 14 March 2022.

Emerging moves

- Google's Privacy Sandbox
  - Investigation by UK competition and markets authority
- Others: Apple's hires in AdTech; Meta and Mozilla's proposals in the IETF.



Google abandons FLoC, introduces Topics API to replace tracking cookies

Google's new concept assigns users five interests per week based on web activity

By Emma Roth | Updated Jan 25, 2022, 2:45pm EST

Don't Play in Google's Privacy Sandbox

BY BENNETT CYPHERS | AUGUST 30, 2019

Questions for the future of online advertising

- **Interaction between input data and confidential computing**: what is the theoretical, ethical, and legal basis not to use e.g. blood pulse, eye-tracking, etc data when the output is confidential?
- **Is your device betraying you?** Rights for people facilitating computing, rather than just rights related to how data about you is used. Links to research ethics.