



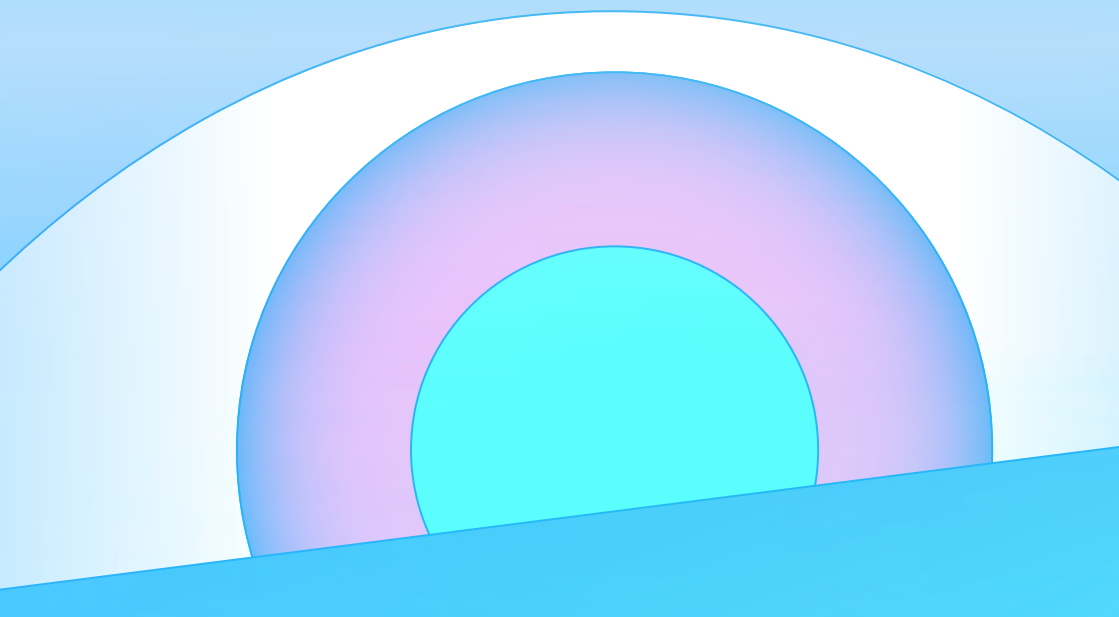
EDRi

EUROPEAN DIGITAL RIGHTS

Targeted Online

—

An industry broken by design and by default



Distributed under a Creative Commons Attribution 4.0 International (CC BY 4.0) license.

Booklet written by **Laureline Lemoine**, **Ella Jakubowska**, **Andreea Belu** and **Diego Naranjo**.

Reviewed and edited by **Sarah Chander**, **Chloé Berthelemy**, **Frederike Kaltheuner**, **Jan Penfrat** and **Gail Rego**.

This booklet was drafted based on the work of European Digital Rights' members and other partners, and it would have been impossible without their thorough revisions, comments and edits:

Access Now Europe

Open Rights Group

Panoptikon Foundation & Karolina Iwańska, Mozilla Fellow 2019-2020

Privacy International

Norwegian Consumer Council

Rigo Wenning

Vrijschrift

“We don’t need to own everything. Using the data we already have, there is a good chance that we know you are moving, changing jobs, having a baby, getting married, etc. — and we can really help you with the queries that you should have asked but didn’t. We have a value proposition that nobody else has.”

‘Ad tech’ is a catch-all term used to describe the industry of buying and selling the attention of internet users via targeted advertising or promoted content.

¹ <https://globaldatareview.com/competitionantitrust/googles-early-data-strategy-revealed>

Introduction

Targeted online ads can be confusing. Sometimes it can seem as if advertisers know us intimately. Other times, advertising is so wrong as to become annoying. What all targeted ads have in common is that it is often impossible to understand why we are being targeted. How much of your data is being collected and how it is being shared? In short, why are you really seeing this ad?

When the CEO of Netflix, Reed Hastings, was asked about his business's main competitor, he replied: "We're competing with sleep."² Likewise, Facebook, or any ad-supported platform, is competing for your free time. These platforms do whatever they can to occupy a maximum amount of your attention. Why? **Because having your attention means making money.**

This handbook is intended for curious internet users who want to understand the internet's dominant business model, how tech companies use (and abuse) data, why some ads are eerily creepy and others so foolishly wrong. This handbook explains how online advertising works, and why a reform of the entire online advertising industry is urgently needed.

'Ad tech'³ is a catch-all term used to describe the industry of buying and selling the attention of internet users via targeted advertising or promoted content.

In the earlier years of the web, ads were mostly contextual, meaning they were geared towards the context in

² Alex Hern, 'Netflix's biggest competitor? Sleep' (The Guardian, 18 April 2017) <https://www.theguardian.com/technology/2017/apr/18/netflix-competitor-sleep-uber-facebook>

³ Throughout this handbook we use terms such as ad tech, online advertising industry and online tracking industry to refer to the different actors from the same industry. However, companies may play different roles and follow different practices that vary in their impact on privacy, their power over citizens and their role (or not) as gatekeepers.

which they appeared, similar to the ways in which printed newspapers or magazines sell advertising space next to their articles, opinion pieces or fashion shoots.

Contextual ads were typically sold by website owners directly to advertisers. Ads on a website about vintage cars, for instance, would typically appeal to vintage car enthusiasts. Placing such an ad does not require specific knowledge about the people who are viewing the ad. Everyone who visits that website sees the same ads – much like billboards next to a highway, or car ads in a motor magazine.

Much has changed since then. The vast majority of ads or promoted content that appear on apps, websites, online news sites, on video platforms or social media are heavily personalised and targeted.

Behavioural advertising or behavioural targeting is an online marketing practice used to target individuals based on large, and growing, troves of data, which can include anything from a person's web browsing history, to online searches, product searches, someone's location history and even

purchases that have occurred in retail shops offline. The narrative, which is often used to justify the collection of all this personal data is that it helps advertising to be more “relevant” and “engaging” to internet users.

However, the amount of data that is collected, shared and processed to target ads at this level of granularity – as well as the invasiveness of the techniques used to target ads and promote content – come with significant risks and harms, for individuals and societies alike.

From targeted political ads, to filter bubbles and radicalisation, behavioural advertising and personalised online spaces more broadly have a profound impact on societies and are thus under scrutiny in this booklet.

The opacity and unaccountability of the online advertising industry and the disproportionate power held by some of the world's largest tech companies within this industry are at the core of the most pressing tech policy issues today.

In the following pages we will outline key problems and possible solutions to some of the biggest concerns around the techniques used in online advertising, as well as by the industry as a whole.

Combined, these two are often referred to as “surveillance capitalism” – an economic system centred around the commodification of personal data with the purpose of making profit.⁴

The **first short chapter** of the booklet will look at digital advertising as an industry and explain the role of platforms and the lesser known ad tech companies, and how the logic of surveillance capitalism has become a dominant paradigm in many industries around the world.

The **second chapter** will explain the **workings** of some common techniques used in targeted advertising and personalisation.

Chapter 3 outlines the **societal impact** of both. Finally, in **Chapter 4** we will outline **our suggestions for systemic change** using existing or upcoming legislation, or enabling alternatives via, for example, public funding or other measures.

⁴ The term “surveillance capitalism” was popularised by Harvard professor Shoshana Zuboff.

TABLE OF CONTENTS


- ▾ Introduction _____ 05
- ▾ 01. Power dynamics and imbalances
in the digital advertising industry _____ 10
 - ▾ 1.1 An offer you cannot refuse –
consent and cookies in online
targeted advertising _____ 16
- ▾ 02: When the web watches you back: _____ 20
how most online advertising works
 - ▾ 2.1 Step 1: Tracking _____ 21
 - ▾ 2.2 Step 2: Profiling _____ 23
 - ▾ 2.3 Step 3: Targeting _____ 26
- ▾ 03. Harms to fundamental rights _____ 32
 - ▾ 3.1 Consequences for society _____ 33
 - ▾ 3.2 Consequences for people _____ 38

▼ 04. The changes we want to see	42
▼ Step 1: End current exploitative practices	44
▼ Step 2: Put humans at the centre	46
▼ Step 3: Breaking the digital Stockholm Syndrome: enable alternatives	52
▼ Sources:	56
▼ News articles	56
▼ Blog posts and websites	58
▼ Reports	61
▼ Academic articles	62
▼ Others	63

01

Power dynamics & imbalances in the digital advertising industry

Before we explain how online ads are targeted and where all the data that is used in targeting comes from, let us take a step back. First, we will look at the digital advertising market, and the different companies that make up what can only be described as the dominant business model of the web as we know it today.



The online advertising ecosystem is made up of a large number of companies that each fulfil various functions. This is where power imbalances first enter the picture.

Most users of the internet do not – and often cannot possibly – understand how content is monetised and how ads are served to them, simply because the techniques used and the sheer number of companies involved are so complex.

A first step to reducing this imbalance is to understand the roles of the different actors involved. Ad tech is an umbrella term for advertising technology and is typically used to refer to the software and tools used by advertisers, ad agencies, publishers, and other companies in the industry.

The ad tech industry has two major entities: the advertiser (the demand-side) and the publisher (the supply side).

Most ad tech companies are not household names, even though they play a crucial role in the industry and perform a variety of tasks. They serve ads, collect data from apps and websites, merge and aggregate data from different devices, combine offline and online data, and are also the marketplaces where ads are auctioned.

Data is also enriched using profiling techniques that place users in various categories, from the seemingly innocuous (like what brand of car they like), to sensitive or conjectured categories (like their personality).

What ad tech companies have in common is that they seek to create a picture of an individual user that is as comprehensive and complete as possible.

Even though this is the declared goal, it does not mean that the data that is collected, aggregated and inferred through profiling is necessarily accurate.

Another key – if not the key – group of players in the industry are the large tech companies. While it is common to refer to them as platforms, companies like Google, Amazon and Facebook operate at nearly all levels of the advertising industry.

For instance, they allow advertisers to purchase and display ads on their apps and websites, within videos and social media stories, but they also display ads on other apps and websites, and track users on these apps and websites.

Major tech companies already have access to troves of user data, simply because of the amount of information they can directly collect from their users.

This is either derived from their behaviour while on these platforms, or the things they do online whenever they are logged into their accounts (for example, searches and websites visited when logged into a Google account fall into this category).

It is impossible to overstate the number of websites and apps from which major tech companies are also able to collect additional data about the people who use their services – and about people who do not.

A 2018 study has shown that Facebook trackers are embedded in almost half of all free apps for Android.⁵

Trackers from Google's parent company Alphabet are embedded in nearly 90 percent of all free Android apps, followed by trackers from Twitter (almost 34 percent), Verizon and its companies (26 percent), Microsoft (almost 23 percent) and Amazon (almost 18 percent).

⁵ Reuben Binns, Ulrik Lyngs, Max Van Kleek, Jun Zhao, Timothy Libert, Nigel Shadbolt, 'Third Party Tracking in the Mobile Ecosystem' (2018) <https://arxiv.org/pdf/1804.03603.pdf>

Third Party Tracking in the Mobile Ecosystem

Root parent	% apps	Subsidiary	% apps	Country
Alphabet	88.44	Google	87.57	US
		Google APIs	67.51	US
		DoubleClick	60.85	US
		Google Analytics	39.42	US
		Google Tag Manager	33.88	US
		Adsense	30,12	US
		Firebase	19.20	US
		Admob	14.67	US
		Youtube	9.51	US
		Blogger	0.46	US
Facebook	42.55	Facebook	42.54	US
		Liverail	1.03	US
		Lifestreet	<0.01	US
Twitter	33.88	Twitter	30.94	US
		Crashlytics	5.10	US
		Mopub	2.51	US
Verizon	26.27	Yahoo	20.82	US
		Flurry	6.28	US
		Flickr	1.37	US
		Tumblr	1.22	US
		Millennialmedia	0.71	US
		Verizon	0.11	US
		AOL	0.06	US
		Intowow	<0.01	US
		One By AOL	<0.01	US
		Brightroll	<0.01	US
		Gravity Insights	<0.01	US

Root parent	% apps	Subsidiary	% apps	Country
Microsoft	22.75	Microsoft	22.11	US
		Amazon	7.72	US
		Amazon Marketing Services	1.73	US
		Bing	0.12	US
		Alexa	<0.01	US
Unitytechnologies	5.78	Unitytechnologies	5.78	US
Chartboost	5.45	Chartboost	5.45	US
Applovin	3.95	Applovin	3.95	US
Cloudflare	3.85	Cloudflare	3.85	US
Opera	3.20	Adcolony	3.12	US
		Admarvel	0.09	US

Lesser-known ad tech companies also track users on millions of apps and websites, but generally speaking, the most common trackers belong to the major tech companies.

Having so much access to user data gives large tech companies many advantages. It allows them to target people at a level of granularity that few competitors can match.

It also allows businesses that have included Facebook, Google or Amazon trackers on their apps and websites to target people who have previously visited their site or app on the platform (depending on the user's privacy settings).

Typically, advertisers can also upload their own data to target people on a platform like Facebook.

This can include data that has been purchased from data brokers or collected through subscriptions, locality cards or mailing lists.

Finally, tech platforms allow advertisers to automatically find audiences that match the people they already know. Once an ad runs on a platform, often the targeting is continuously optimised, so that it is shown to the people who are most likely to engage with it.

Another group of important players in the online advertising industry are publishers and content creators who often rely on advertising to monetise their content. Some of them use platforms like YouTube and TikTok for this.

Most publishers and content creators also depend heavily on social media platforms to get views and reach audiences outside of their own apps and homepages. Publishers like news sites and smaller blogs display ads to support their business – positioning ads can be done at various levels of granularity.

Large publishers usually have their own troves of data, even though they do not match those of large tech platforms. Smaller blogs and websites typically rely on advertising networks, for instance Google ads, to automatically display ads.

Depending on the invasiveness of the advertising techniques allowed on their sites, this means that smaller sites are allowing third parties (from larger tech companies, to smaller, lesser-known ad tech companies) to track users on their sites and apps.

As you can see, the online advertising industry is complex and made up of a large number of companies, many of which are not household names. All of this results in a system that is incredibly opaque.

As a result, merely using an app or visiting a websites can mean that user data is shared with hundreds of companies.

1.1 An offer you cannot refuse – consent and cookies in online targeted advertising

Whether you are visiting a website, using an app on your phone or signing into a social media account, privacy and data protection laws in the European Union mandate that users' consent is needed to process personal data and install tracking technologies like cookies on devices. But through nudges and dark patterns,⁶ "consent" is often falsely extracted from users who do not have a real option to reject the "deal" that publishers and platforms offer.

Most cookie banners, for instance, do not clearly offer users the option to refuse, or will nudge users towards consenting (it often takes more than three clicks to refuse cookies when only one is enough to accept them).⁷ Similarly, it is not possible to use Google and Facebook's

services without accepting their privacy policies that include intensive tracking. Some websites place tracking cookies even after users clearly object.⁸

Most cookie banners do not mention the specific purpose of grabbing and using users' personal information or who can access it.

Likewise, privacy policies are dauntingly long and written in legalese, yet do not go into the detail needed to actually understand the purposes for which user data is being used.

The consent a user "gives" when agreeing to the privacy policies or terms and conditions of apps and online platforms is often equally problematic.

“Some websites place tracking cookies even after users clearly object.”

This is either because users do not fully understand how data is used and collected, or because they do not have the option of using the services without giving consent. This is not valid under current European data protection laws.⁹

The incorrect implementation of data protection and privacy legislation has led to a plague of pop-ups on websites that “ask” visitors to “accept” cookies, because otherwise they are prevented from using the site’s services. EDRI has long advocated against the existence of these “cookie walls”.¹⁰

The official group of data regulators in Europe, the European Data Protection Board (EDPB), also confirmed that this “does not constitute valid consent”.¹¹

Consent is one of the key legal bases that allow data processors to lawfully collect and process personal data, and it is the main legal basis for the processing of “sensitive data” such as actual or inferred data about race, political opinion, religious belief, health, sex life, sexual orientation, and genetic and biometric data.

⁶ Dark patterns are techniques and features of interface design meant to manipulate users with the aim of nudging users towards privacy intrusive options. See the report on dark patterns by the Norwegian Consumer Council: <https://www.forbrukerradet.no/dark-patterns/>

⁷ Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz, ‘(Un)informed Consent: Studying GDPR Consent Notices in the Field’ (ACM SIGSAC Conference on Computer and Communications Security, 2019). <https://arxiv.org/pdf/1909.02638.pdf>

⁸ NOYB, ‘Say “NO” to cookies – yet see your privacy crumble?’ (NOYB, 10 December 2019). <https://noyb.eu/en/say-no-cookies-yet-see-your-privacy-crumble>

⁹ See our one-pager on consent in the context of online tracking here: https://edri.org/files/eprivacy/e-privacy-onepager_consent.pdf

¹⁰ EDRI, ‘Tear Down the Tracking Wall’ (2017) <https://edri.org/tear-down-the-tracking-wall>

¹¹ European Data Protection Board (EDPB), Guidelines 05/2020 on consent under Regulation 2016/679 (2020), p.12. See: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

Yet, the opacity and complexity of the online advertising system makes it difficult for users to enjoy their fundamental right to data protection and privacy. Users cannot identify all the companies that will receive and process personal data, which makes informed consent impossible.

However, individuals are shown "options" to accept or deny (in some cases granularly, in some cases not) tracking of their behaviour which lends a feeling of powerlessness and "consent fatigue" (or rather "cookie banner fatigue").¹²

¹² (Un)informed Consent: Studying GDPR Consent Notices in the Field. <https://arxiv.org/pdf/1909.02638.pdf>

The business practices of dominant online platforms and the ad tech industry are complex and opaque by design, because the industry benefits from the fact that most people don't fully understand and cannot meaningfully control how their data is used and collected.

The lack of strong enforcement of existing laws and a lack of interest in (if not deliberate blocking of) additional regulatory initiatives creates the ideal conditions for harmful and illegal activities.

The industry is seldom held to account. This affects both individuals and society as a whole.

Example of a cookie banner that gives no real choice

Accept cookies from Instagram on this browser? ...

We use cookies to help personalize content, serve relevant ads and provide a safer experience. Learn more about cookie uses and controls in our [Cookie Policy](#). You can review your controls at any time.

Accept

Learn More

02

When the web watches you back: how most online advertising works

Before diving further into the different roles and functions of each actor involved, let us explore what you do and don't see on your screen when you visit a website, and what techniques are used to collect and process data about you to deliver targeted ads.

2.1 Tracking

To target users and predict behaviour with detail, ad tech companies and tech platforms want to know as much about each individual user as possible.

What are tracking tools and how do they work?

We have already discussed above how websites and apps contain trackers that collect data about users.

These tracking tools (which include cookies, beacons and browser fingerprinting among others) are used to collect and, more importantly, combine data about people from across the web, different apps and even different devices. These are then used to make guesses about individuals' interests and preferences. Trackers constantly observe users and their behaviour online.

This can mean knowing the screen size of a particular user's device and the software installed on it (which can in some cases be enough to identify individuals).

It can also mean a user's physical location, the apps installed on their device, browser settings, IP addresses, their topics of interest (politics, hobbies, sexual preferences, culture etc), how much time they spend on the website or platforms, the way they move their mouse, who they hang out with offline, the state of their mental health and much more.¹³

What is more, websites and app developers integrate those technologies from "third parties" in their website or mobile applications source code, often for convenience and to increase commercial profit.

Third party tracking is particularly problematic, because people aren't aware of it and have little control over how their interactions with an app or a website are shared with those third parties. In particular, third parties whose code is embedded in a large number of different apps and websites receive data about users that can be linked and combined into an incredibly detailed profile.

This results in companies having access to a large share of individual users' browsing history.¹⁴

While users can delete some of these trackers, such as cookies, from their browser, other tracking tools have been developed that are less easily controlled. Fingerprinting, for example, uses information about a user's device, browser, or IP address to uniquely identify and recognise their device without the need to place a cookie.

Other techniques, like beacons, can track everything a user does on a web page including what they type or where their mouse moves.¹⁵

Since online tracking has become ubiquitous, data about a large portion of users' online experience (searches, likes, lists, subscriptions, time spent on each piece of content, etc.) is used to profile them for advertising purposes. This is then used to direct more of the same content that they may be interested in, according to the data users have handed over and data that has been inferred. This creates a feedback loop of micro-targeted content and ads.

So what? Next, we'll look at why this is harmful.

¹³ Find more information about how tracking impacts fundamental rights at: <https://edri.org/privacy-security-freedom>

¹⁴ Privacy International, 'I asked an online tracking company for all of my data and here's what I found' (7 November 2018): <https://privacyinternational.org/long-read/2433/i-asked-online-tracking-company-all-my-data-and-heres-what-i-found>

2.2 Profiling

We know that content on a website can change, according to who is visiting. Social media feeds and recommendations look radically different, not just based on who individuals follow. The same is true for the ads that we see.

▸ What makes a user unique for advertisers?

The data and information gathered through tracking can end up in detailed user profiles. For example, when a user is using their phone to visit a website online, that website automatically places cookies and embeds beacons and/or other tracking software.

Trackers don't necessarily know an individual's legal name, but they are able to uniquely identify a user's device or browser, and merge data that has been collected on different browsers and on different devices into a single profile.

Unique identifiers¹⁶ such as device or browser fingerprints¹⁷ or a mobile phone's unique Advertising ID make profiling possible and further turn a user's profile into a unique person identifier. The techniques used to do that are far from perfect, for instance when several people share the same device, but they are good enough to provide deep insights into people's most intimate personal lives.

▸ Inferred data: guessing stuff about users and enriching data

The more data companies collect about individual users, the more additional insights they can infer and derive from that information.

Inferred data means ad tech companies can know things about people that those people never actually shared with anybody. That can range from gender, age or general interests to highly intimate information such as predicted sexual orientation, psychometric profile, IQ level, family situation, addictions, illnesses or the menstrual cycle.¹⁸

Often apps will have access to even more sensitive information such as location data, personal calendars, the camera, personal contact lists and more.

A study at the Universities of Cambridge and Stanford found that, by analysing clicks on Facebook "like" buttons, it was possible to guess an individual's personality better than a work colleague (based on just 10 clicks), better than a parent or sibling (based on 150 clicks) and better than a spouse (based on 300 clicks). Researchers indicated that Facebook has records of 100 billion "likes".¹⁹

¹⁵ Epic.org, 'Online Tracking and Behavioural Profiling': <https://epic.org/privacy/consumer/online-tracking>

¹⁶ For more details on the different types of trackers see: Bennett Cyphers, 'Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance' (2 December 2019): <https://www.eff.org/wp/behind-the-one-way-mirror>

¹⁷ For more information on browser fingerprinting, see: <https://panopticklick.eff.org/about#browser-fingerprinting>

¹⁸ Privacy International, 'No Body's Business But Mine: How Menstruation Apps Are Sharing Your Data' (2019): <https://privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruations-apps-are-sharing-your-data>

¹⁹ Andrew Brown, 'Ever liked a film on Facebook? You've given the security services a key to your soul' (The Guardian, 13 January 2015): <https://www.theguardian.com/commentisfree/2015/jan/13/facebook-likes-security-services-psychological-profile-facebook-research>

²⁰ The Facebook-Cambridge Analytica scandal concerned the obtaining of the personal data of millions of Facebook users without their consent by British consulting firm Cambridge Analytica, predominantly to be used for influencing the outcome of political elections.

“By analysing clicks on Facebook “like” buttons, it was possible to guess an individual’s personality better than a work colleague, better than a parent or sibling and better than a spouse.”

2.3 Targeting

There are a variety of ways in which online ads can be targeted. Broadly speaking, these fall into four categories.

Targeting based on categories provided by online platforms

The easiest way to target ads is to buy advertising space on social media platforms or through their ad networks. These allow advertisers to target ads based on relatively broad categories, demographic information, such as age, location, and interests.

These options suggest that targeting is relatively broad, but in reality, these categories are based on all the data that tech platforms have aggregated.

This includes users' declared interests, the content they have shared, as well as who they are connected with, but also a platform's own data, such

as the ways in which users have interacted with content.

Depending on the privacy settings chosen by users, ads on platforms can also be targeted based on data that has been collected outside the platform, meaning ads on social media platforms can be targeted based on the websites a user has visited and the apps installed on their phone.

Until the Facebook-Cambridge Analytica scandal²⁰ caused some platforms to change their practices, advertisers could also target people on platforms based on data provided by data brokers and credit referencing agencies.

▾ Targeting based on custom data

Advertisers can also target users based on the data they have collected directly, for instance through trackers on their websites, apps, or online shops, or through email lists, shop data, location data and phone numbers they have either collected themselves or purchased elsewhere. That includes personal information collected through so-called loyalty cards, email newsletters for customers, and other types of promotional activity.

▾ Automated targeting

Most targeted ads are continuously optimised for engagement, meaning that no matter how an advertiser has chosen to target an ad, the ad delivery system constantly tests which kinds of users are most likely to click on an ad.

Whenever a user clicks on an ad, similar users are more likely to be shown the same ad.

Advertisers can also leave the targeting of ads entirely to these automated systems. Facebook, for example, offers a tool called 'Lookalike Audience', that allows

advertisers to automatically find audiences that "look" similar to users they have already identified and targeted.

▾ Real time bidding (RTB)

RTB is an automated auction process that enables advertisers to target very specific groups of people on different websites, videos and apps without having to negotiate prices directly.

Imagine auctions, stock exchange, traders, big screens, noise, graphs, percentages. RTB systems similarly facilitate the auction of advertising space to the highest bidding advertiser. This technique is often used on websites and by publishers. Platforms like Facebook also use ad auctions to determine the best ad to show to a person at a given point in time.

How does it work? A website rents its advertising space to one (or many) ad exchanges. The moment a user visits the website, during the milliseconds in which it loads, the ad exchange creates a "bid request" that includes their personal information: what they are reading, watching or listening to, the website they are on, the categories

Example of a real-time bid request sent to hundreds of ad tech companies while the user waits for the website and its advertising to load.

```
"id": "1234",
"name": "Awesome Example Site",
"domain": "examplesitedomain.com",
"mobile": 1,
"amp": 0,
"pub": {
  "id": "9876",
  "name": "Example Publisher, Inc.",
  "domain": "examplepubdomain.com"
}
"user": {
  "id": "a0af45c77890045deec100acb8443baff57c",
  "buyeruid": "fcd4282456238256034abcdef220d9aa5892",
  "yob": 1990,
  "gender": "F",
  "device": {
    "type": 4,
    "ifa": "8846d6fa10008bceaaf322908dfcb221",
    "ip": "1.2.3.4",
    "ua": "...user agent string...",
    "make": "Apple",
    "model": "iPhone",
    "hvv": "6s",
    "os": 13,
    "osv": "11.4.1",
    "mccmnc": "310-005",
    "geo": {
      "type": 1,
      "lat": 42.3601,
      "lon": 71.0581,
      "country": "USA",
    }
  }
}
```

The website this specific person is currently viewing

Various ID codes that identify this specific person, and can tie them to existing profiles

Distinctive characteristics of this specific person

Distinctive information about this specific person's device

This specific person's IP address

Distinctive information about this specific person's device

This young woman's GPS coordinates!

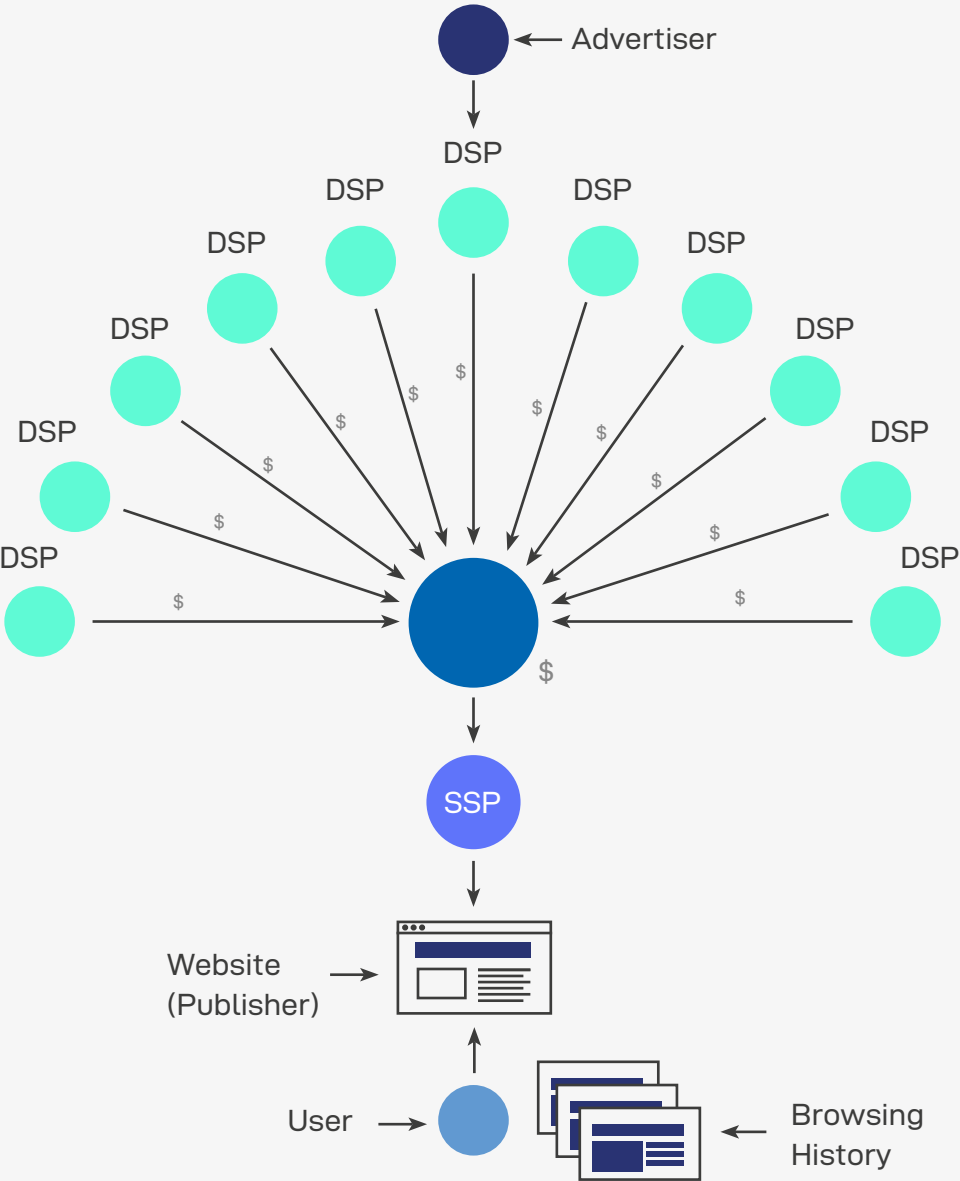
The moment a user visits the website, during the milliseconds in which it loads, the ad exchange creates a “bid request” that includes their personal information.

into which that content goes, their unique pseudonymous ID, their profile's ID from the ad buyer's system, their geographical location, device type (smartphone or laptop), operating system, browser, IP address, and so on.

Advertisers inform the ad exchange about who they want to show their advertisement to. Sometimes they provide detailed customer segments. These categories have been obtained by combining the advertisers' data about (potential) customers, and the personal profiles generated by data brokers such as Experian, Acxiom or Oracle.

The ad exchange now has a complex profile of an individual user, made of information from the website supplying the ad space, and information from the advertiser demanding the ad space.

When there is a match between a bid request and the advertiser's desired customer segment, a Demand Side Platform (DSP) acting on behalf of thousands of advertisers starts placing bids for the website's ad space. The bid winner makes the race and gets to place its advertisement in front of a particular website viewer, and the rest is history.



Some websites have as many as 400 external advertising partners with whom they share user data.²¹ And some mobile apps have been found to transmit user data to as many as 135 advertising third parties.²²

But what is the infrastructure they use to share all this data?

Two systems provide personalised advertising on websites through RTB: Google's "Authorized Buyers" and "OpenRTB" are used by almost every company in the online advertising industry.

The specification documents of these two systems reveal that every time a user visits a website that uses RTB, their personal data is publicly broadcast to sometimes thousands of companies waiting to target their ads.²³

What is more, all of the actors may receive an individual's personal data, regardless of whether they win the bid to show the ad or not.

If the user has attempted to opt out (for example through device settings for the advertising ID), in many cases the personal data will still be transmitted, just alongside a flag saying that they opted out.

In a nutshell, if the third party chooses not to respect a user's choice to opt out, they can keep harvesting their data without any consequences for themselves.

²¹ Karolina Iwańska, 'Behavioural Advertising 101' (Panoptikon Foundation, 9 January 2020): <https://en.panoptikon.org/online-advertising-is-broken>

²² Norwegian Consumer Council – Forbrukerrådet, 'Out Of Control: How consumers are exploited by the online advertising industry' (14 January 2020): <https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf>

²³ Complaint filed with the UK Information Commissioner's office by Mr James Killock and Mr Michael Veale: <https://brave.com/wp-content/uploads/2018/09/ICO-Complaint-.pdf>

03

Harms to fundamental rights

We have discussed how ads are targeted online, how the online advertising industry works and which power imbalances and dynamics are at play. In this chapter, we will look at some of the harms that online advertising causes in individuals and society at large.

3.1 Consequences for society

▸ The industry fails to meet basic standards of human dignity, liberty and respect for privacy

The most obvious and common harm of online advertising today is the widespread and routine exploitation of people's data. The sheer amount of data that is routinely collected is concerning in and of itself.

But tracking and profiling have also become virtually inescapable.

The industry for commercial data is so leaky and complex that it has become impossible for most people to understand where private information about them ends up, or to exert any agency over what data is collected and by whom. As a result, it is incredibly difficult – if not impossible – for people to exercise their data rights.

This is exactly why Amnesty International has warned that the way in which the industry's business model relies on exploiting people's data, and using it against them fails to meet the most basic standards of human dignity, liberty or respect for privacy.²⁴

Beyond inferring categories like an individual's age, race or gender, behavioural profiling can go a step further to profile their most sensitive characteristics.

²⁴ Amnesty International, 'Surveillance Giants; How the business model of Google and Facebook threatens human rights' (21 November 2019), <https://www.amnesty.org/en/documents/pol30/1404/2019/en>

Research has shown that tracking companies even use labels for identifying survivors of incest, rape and sexual abuse, people with mental health issues, impotence or infertility.²⁵

The use of such intrusive categories for the purpose of advertising harms the fundamental dignity to which each person is entitled.

▸ Lack of accountability means harmful ads are rampant

Even though most advertising networks have policies that ban certain kinds of ads, harmful ads such as scams remain widespread.

For instance, in a 2020 experiment the UK consumer organisation Which? was able to promote fake health advice and a brand that didn't exist to highly targeted audience online by using Facebook and Google advertising tools.²⁶

As most ads on websites and apps are delivered automatically, there is limited accountability as to whether these ads are harmful or violate the advertising standards of the network they run on.

Since ads are personalised, and since there are no ad libraries for non-political ads, it is incredibly difficult to understand the scope of harmful ads. Brands are not required to list all the ads they are running at any point in time. It is therefore incredibly difficult to track down and request the removal of harmful ads.

This constitutes a considerable risk for publishers too, who do not know what ads will run next to their content.

▸ Advertising funds hate and disinformation

Online advertising is a key funder of online hate and disinformation which can disrupt elections, incite violence, and is preventing us from effectively tackling climate change.

According to The Global Disinformation Index, at least \$235 million in revenue is generated annually from ads which run on extremist and disinformation websites – fuelled in part by the advertising budgets of well-known companies²⁷ and even political actors,²⁸ including \$25 million in 2020 which funded COVID-19 disinformation.

Online extremism, radicalisation, election meddling and disinformation are problems that pre-date the internet and online advertising platforms.²⁹ However, the race for our attention and advertising revenue risk further exacerbating, and intensifying these problems, while giving them a new and different dimension.³⁰

Studies from 2019³¹ and 2020³² by Avaaz also found that recommendation algorithms on advertising-funded platforms (such as YouTube and Facebook) prioritised disinformation in part because of its engagement rate and consequential attractiveness to advertisers.

The platforms themselves are often reactive and rely on fallible algorithms to police the content being uploaded and/or the content of the sites they are monetising.

▮ Threats to quality journalism

A free and independent press is an important cornerstone of every democratic society. It reports on news, holds elected officials to account, performs investigations and reveals corruption. Although much of the early press funded their work through

²⁵ Norwegian Consumer Council – Forbrukerrådet, 'Out Of Control: How consumers are exploited by the online advertising industry'.

²⁶ Andrew Laughlin, 'Fake ads; real problems: how easy is it to post scam adverts on Facebook and Google?' (Which? 6 July 2020): <https://www.which.co.uk/news/2020/07/fake-ads-real-problems-how-easy-is-it-to-post-scam-adverts-on-google-and-facebook>

²⁷ Global Disinformation Index, 'Ad-Funded COVID 19 Disinformation: Money, Brands & Tech' (8 July 2020): https://disinformationindex.org/wp-content/uploads/2020/07/GDI_Ad-funded-COVID-19-Disinformation-1.pdf

²⁸ Xnet, '#FakeYou – Fake News y Desinformación: Gobiernos, partidos políticos, mass media, corporaciones, grandes fortunas: monopolios de la manipulación informativa y recortes de la libertad de expresión' (29 October 2019): <https://xnet-x.net/informe-fake-news-desinformacion>

²⁹ Glenn Greenwald, 'The CIA's Murderous Practices, Disinformation Campaigns, and Interference in Other Countries Still Shape the World Order and U.S. Politics' (The Intercept, 21 May 2020): <https://theintercept.com/2020/05/21/the-cias-murderous-practices-disinformation-campaigns-and-interference-in-other-countries-still-shapes-the-world-order-and-u-s-politics>

³⁰ Nathalie Maréchal & Ellery Roberts Biddle, 'It's Not Just the Content, It's the Business Model: Democracy's Online Speech Challenge' (17 March 2020): https://d1y8sb8igg2f8e.cloudfront.net/documents/REAL_FINAL-Its_Not_Just_the_Content_Its_the_Business_Model.pdf

³¹ Avaaz 'Why is YouTube Broadcasting Climate Misinformation to Millions?' (6 January 2019): https://secure.avaaz.org/campaign/en/youtube_climate_misinformation

³² Avaaz, 'How Facebook Can Flatten the Curve of the Coronavirus Infodemic' (15 April 2020): https://avaazimages.avaaz.org/facebook_coronavirus_misinformation.pdf

³³ Andrew Marantz, Big Swinging Brains and fashy trolls: how the world fell into a clickbait death spiral (The Guardian, 7 February 2020) <https://www.theguardian.com/technology/2020/feb/07/big-swinging-brains-fashy-trolls-clickbait-death-spiral-internet-media> See also Harriet Kingaby and Frederike Kaltefleiter, 'Ad Break for Europe: The race to regulate digital advertising and fix online spaces', (September 2020): https://assets.mofoprod.net/network/documents/Ad_Break_for_Europe_FINAL_online.pdf

³⁴ European Parliamentary Research Service, 'Polarisation and the use of technology in political campaigns and communication' (7 March 2019): [https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU\(2019\)634414](https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2019)634414) See also Robert Gorwa and Timothy Barton Ash, Democratic transparency in the platform society. Social Media and Democracy: The State of the Field, Prospects for Reform, p.286, referenced by Kingaby and Kaltefleiter (2020).

³⁵ European Parliamentary Research Service, (2019)

revenue from subscriptions, today quality journalism increasingly relies on advertising revenue.

As the market for online advertising shifted towards targeted ads, online publishers have been caught in the web of ad networks that hold the data of billions of people as third party property. Instead of marketing their ad space directly to advertisers, and thereby keeping the value of their brand and the access to their readers' attention in-house, publishers have sold out those assets to ad networks like Google in exchange of convenience and the promise of more valuable ads.

In reality, the value of advertising space is decreasing and Google, as the data-owning middleman, grabs a larger and larger share of the advertising revenue that is supposed to fund quality journalism.

▸ Threats to the quality of public discourse

In the case of online media, the dependence on platform's recommender systems and behavioural advertising more broadly risks incentivising outrage and virality over quality.³³

The more extreme, provocative or divisive content is, the more attention it will gain – regardless of whether people interact with it because they agree with it, or because they want to challenge it – and the more money it makes for ad intermediaries and marketers. The European Parliamentary Research Service (EPRS) have called such trends in the online advertising industry “polarisation by design”.³⁴

These tendencies can make it increasingly difficult for respectable journalism to get the attention it deserves, resulting in a reduction in ad revenue for quality publishers.

When democratic societies lose these credible sources of news, there is a risk that misleading, provocative and spoof websites fill this news vacuum. When this happens, the important societal and democratic functions performed by quality journalism are lost.

Threats to democracy

Sometimes, online advertising and platforms are used by malicious actors keen to exploit this attention-driven industry to disrupt public and political discourse.³⁵ This abuse of personal data can result in serious impediments to democratic processes and the integrity of elections.

The Facebook-Cambridge Analytica scandal and the Brexit campaign³⁶ show that the trafficking of illegally obtained personal data can lead to its misuse for political gain, notably by micro-targeting citizens with political ads³⁷ and even targeting voters with disinformation.³⁸

Facebook in particular enables precision-targeted political messages, thanks to its access to behavioural data and sophisticated algorithms, both treated by the platform as its “property”.³⁹

³⁶ Caroline Cadwalladr, ‘The great British Brexit robbery: how our democracy was hijacked’ (The Guardian, 7 May 2017): <https://www.theguardian.com/technology/2017/may/07/the-great-british-brexite-robbery-hijacked-democracy>

3.2 Consequences for people

▸ People are unable to exercise their fundamental rights

The automated nature and complexity of the online advertising ecosystem makes it hard to audit, even for advertisers.⁴⁰ Just as it is now practically impossible to understand and control how companies collect data about users for advertising purposes, it is equally impossible for users to understand why and how ads and promoted content are targeted at them.

Facebook, Google and Twitter only provide limited information to users, and many ads run through ad networks on news sites and apps that provide no explanatory information at all.

As a result, it is difficult to know and prove whether an ad has been targeted based on sensitive data (i.e. sexual orientation, health indicators), whether the targeting is predatory (i.e. loans targeted at people with debt) or whether it is targeted in ways that are discriminatory.

▸ Chilling effects on freedom of information and expression

Rights to freedom of information and expression include the right to express and share thoughts and information, as well as the right to receive the information necessary for informed consent.

The Norwegian Consumer Council has described the chilling effects that could derive from the surveillance that is associated with the majority

of online advertising. For example, people might be concerned that their online search history could drive up their health insurance premiums, and this fear could lead them to abstain from getting necessary information about their medical conditions.⁴¹

▸ Increased mass surveillance

The ad tech industry's hunger for data means that anyone can buy access to potentially sensitive data,⁴² including oppressive governments and other nefarious actors.

By collecting unnecessary data, the online advertising industry creates the perfect conditions for unlawful mass surveillance and, because of the links between data brokers and the ad tech industry,⁴⁴ personal data can end up being abused even by law enforcement officers.

For example, cases have been reported of data obtained by the online advertising industry being sold to authorities for the purpose of tracking down and arresting undocumented migrants.⁴⁵

³⁷ Micro-targeted political ads are opposed by most citizens both in the U.S. and the EU, see for the EU: European Commission 'European Commission survey shows citizens worry about interference ahead of the European elections' (Press Release, 26 November 2018) https://ec.europa.eu/commission/presscorner/detail/en/IP_18_6522 and for the U.S.: Justin McCarthy, 'In U.S., most oppose micro-targeting in online politics; ads' (Knight Foundation, 2 March 2020): <https://knightfoundation.org/articles/in-us-most-oppose-micro-targeting-in-online-political-ads>.

³⁸ European Parliamentary Research Service, (2019)

³⁹ Karolina Iwańska and Katarzyna Szymielewicz, 'Who (really) targets you? Facebook in Polish election campaigns' (Panoptikon Foundation, April 2020): <https://panoptikon.org/political-ads-report>

⁴⁰ Abi Gibbons, 'Time for change and transparency in programmatic advertising', (ISBA, 6 May 2020): <https://www.isba.org.uk/news/time-for-change-and-transparency-in-programmatic-advertising>

⁴¹ Norwegian Consumer Council, (2020), p.52.

⁴² For example, the Norwegian public broadcaster was able to buy the location data of almost 200,000 Norwegians from a data broker. The data was collected through apps/ad tech: <https://www.nrk.no/norge/xl/avslort-av-mobil-en-1.14911685>

⁴³ For more about data brokers, see Floris Kreiken, 'Transparent consumers – a report by Bits of Freedom' (EDRI, 24 February 2016): <https://edri.org/transparent-consumers-a-report-by-bits-of-freedom/>

⁴⁴ Sometimes the lines between data brokers and ad tech is mixed. See Norwegian Consumer Council (2020), pp.19-23.

In the U.S., various authorities have purchased geographical location data from data brokers that was originally collected by Muslim prayer apps, and thereby used personal data that specifically targets Muslim citizens.⁴⁶

▮ Discrimination

Targeted ads can also lead to discrimination. Research has shown that online job ads for Science, Technology, Engineering and Mathematics (STEM) jobs are disproportionately shown to men and hidden from women.⁴⁷

This perpetuates and reinforces harmful gender stereotypes and cuts in half the talent pool. In yet more examples, rental opportunities have deliberately not been shown to people of colour, which reinforces and perpetuates structural racism, inequality and could even encourage de facto segregation by neighbourhood.

In this context, the importance of inferred data (also called “proxy data”) cannot be understated. For example, Facebook have claimed that they do not target people based on “race”, but they instead offer a targeting criterion

called “ethnic affinity” which can be used as a proxy characteristic for race. Similarly, location data can be used to profile people based on low-income neighbourhoods, without directly targeting them based on their financial situation. Yet the associated discrimination risks are exactly the same.

⁴⁵ See Byron Tau and Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, (The Wall Street Journal, 7 February 2020) <https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600> and Rani Molla, ‘Law enforcement is now buying cellphone location data from marketers’ (Vox, 7 February 2020): <https://www.vox.com/recode/2020/2/7/21127911/ice-border-cellphone-data-tracking-department-homeland-security-immigration> More examples from Wolfie Christl can be seen here: <https://twitter.com/WolfieChristl/status/1230623624945643520>

⁴⁶ See Joseph Cox, *Leaked Location Data Shows Another Muslim Prayer App Tracking Users*, (Vice Magazine, 11 January 2021): <https://www.vice.com/en/article/xgz4n3/muslim-app-location-data-salaat-first>

⁴⁷ Karolina Iwańska, ‘10 Reasons Why Online Advertising is Broken’ (Panoptikon Foundation, 9 January 2020): <https://en.panoptikon.org/online-advertising-is-broken>

“Research has shown that online job ads for Science, Technology, Engineering and Mathematics (STEM) jobs are disproportionately shown to men and hidden from women.”

04

The changes we want to see

Changing the micro-targeted, advertisement-driven, invasive and centralised attention economy that occupies large parts of today's internet requires structural transformation.

We need regulation that drastically reforms the way online advertising works. That means phasing out⁴⁸ some key techniques and industry practices that define how ads are targeted, and how content is promoted and recommended.

Reforms of online advertising should help promote a healthy system that is respectful and protective of privacy among other fundamental rights.

The online advertising industry is already under investigation by several EU data protection authorities.⁴⁹

Now is the time to create the conditions to allow for a healthier internet industry. This includes formulating new rules and

strengthening the enforcement of existing rules that apply to advertising companies, social media platforms, search engines, email providers and news publishers.

We suggest the following steps to promote an open, human-centric internet environment that moves away from current surveillance-based practices:

⁴⁸ The EDPS Opinion on the Digital Services Act says, in relation to online targeted advertising, the following: “Such measures should include a phase-out leading to a prohibition of targeted advertising on the basis of pervasive tracking, as well as restrictions in relation to the categories of data that can be processed for targeting purposes and the categories of data that may be disclosed to advertisers or third parties to enable or facilitate targeted advertising. https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_services_act_en.pdf

4.1 End current exploitative practices

Privacy by design and by default are core principles that any new legislation needs to incorporate.⁵⁰

The practices of micro-targeting and using personal data for targeted advertising by default and without users' knowledge need to stop.

For example, the ways in which many websites and apps currently obtain user "consent" through cookie notices, do not meet the standard set by current data protection and privacy legislation. Where consent mechanisms fail to respect the legislation, there must be strong enforcement and redress.

Better enforcement alone would already help to reduce the overall amount of data in the system.

It would also mean that personal data could not be shared with advertising companies without the knowledge and informed consent of users.

By restricting the way targeted advertising currently works and phasing out some of the most invasive practices, companies would lose the incentive to collect excessive amounts of personal data in the first place.

Such limitations would contribute to a healthier, less polarised online environment while containing the risk of manipulation, for instance in the context of elections.

Without invasive cookies and similar tracking technologies users would have no more second thoughts about sharing their personal data with companies they otherwise trust.

Moreover, in-depth reform of online advertising practices could help decentralise power from tech giants.

Data is a source of market power and has led to some platforms and intermediaries becoming dominant and abusive, using their position to collect even more data and thereby creating a vicious circle for users and publishers.

Reform could give power and control back to individuals and liberate publishers and journalists from their dependence on the tech giants' data monopolies.

Making online advertising less invasive, for instance through contextual ads, or ads that are targeted according to simple criteria to which the user opts in, would still allow publishers and platforms to make money.

⁴⁹ Currently, complaints have been filed with the national data protection authorities of 14 European Member States, by several actors, including Panoptikon Foundation, Liberties and Brave. See more at: <https://brave.com/rtb-updates>

⁵⁰ At the time of writing (February 2021), the tracking-based part of ad tech is covered by the ePrivacy Directive, while we advocate for privacy by design and by default to be included in the ePrivacy Regulation, which is still under discussion, and in the proposed Digital Services Act.

4.2 Put humans at the centre

Instead of plugging into the tech giants' ad networks, publishers would be able to sell their ad space directly to advertisers. Ads can be shown based on a website's context or, at most, targeted based on a small set of transparent criteria chosen by the user (opt-in). In the case of contextual ads, these would be broadcast according to the content of the website, the article being read, or the video being watched, regardless of the person doing the watching.

With only ad space to sell – and not personal data – the advertising industry would rely less on data intermediaries like Google and instead rebuild direct links between companies. This means more money for the publishers and online content providers.

Wherever users see ads or personalised content, they should be in charge of how the content and related ads are presented to them. It would be up to them to opt-in to the criteria according to which their content and ads are curated.

They should also be able to opt out of any choice they opted into at any time. Data used in recommender systems should be separated from data used in ad targeting. For each of these, people should be in charge of defining how they want content to be recommended and ads to be targeted.⁵¹

Limiting ad targeting alone does not solve all problems in the online advertising industry. Dominant players, for instance, would still

have a competitive advantage over companies that have less access to user data.

This is why such an in-depth reform of targeted advertising must go hand in hand with a strong enforcement of data protection, privacy legislation, and competition law.

This is the only way to challenge the unfair competitive advantage of the tech giants.

In particular, purpose limitation should be enforced so that when these platforms ask people for meaningful and informed consent, that consent cannot be recycled for other services or platforms that belong to the same company.⁵²

For example, users of Google Search must accept Google's privacy policy, which allows Google to collect and process data from their search history, but also from Android or Google Maps.

By agreeing to Facebook's terms and conditions, people also allow their data on WhatsApp and Instagram to be merged and connected to their Facebook account.⁵³

This is contrary to the purpose limitation principle of Article 5 GDPR and closer to the cinematic sentence "an offer you cannot refuse."

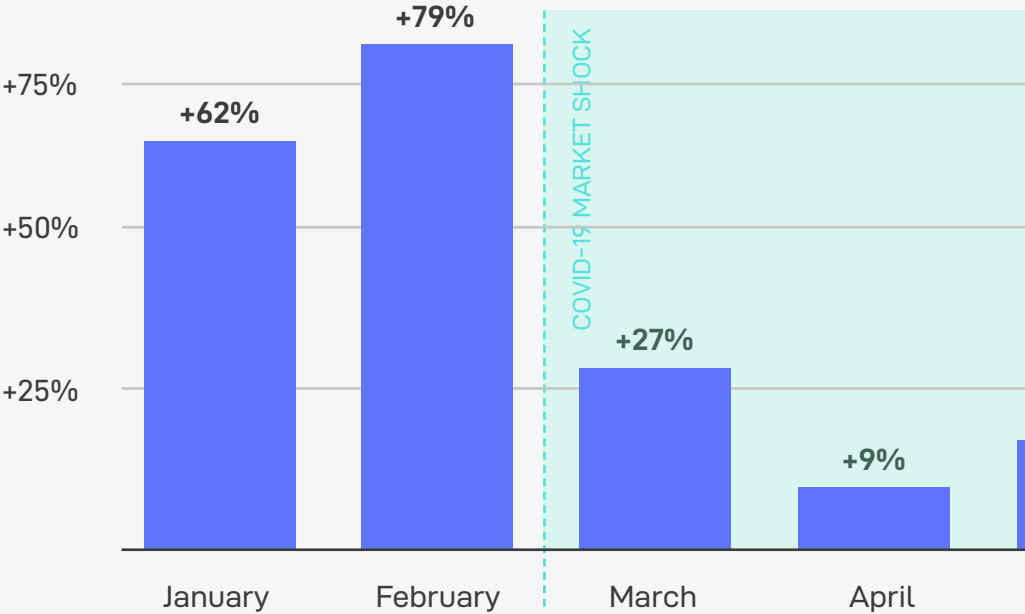
⁵¹ For more ideas on how to improve the situation see Birgit Stark and Daniel Stegmann, 'Are Algorithms a Threat to Democracy? The Rise of Intermediaries: A Challenge for Public Discourse' (Algorithm Watch, May 2020): <https://algorithmwatch.org/en/wp-content/uploads/2020/05/Governing-Platforms-communications-study-Stark-May-2020-AlgorithmWatch.pdf> p.48 and regarding YouTube specifically, Brandi Geurnik, 'Our Recommendation to YouTube', (Mozilla blog, 14 October 2020) <https://foundation.mozilla.org/en/blog/our-recommendation-youtube/>

⁵² Johnny Ryan, 'Failure to enforce the GDPR enables Google's monopoly' (Brave, 18 February 2020): <https://brave.com/competition-internal-external>

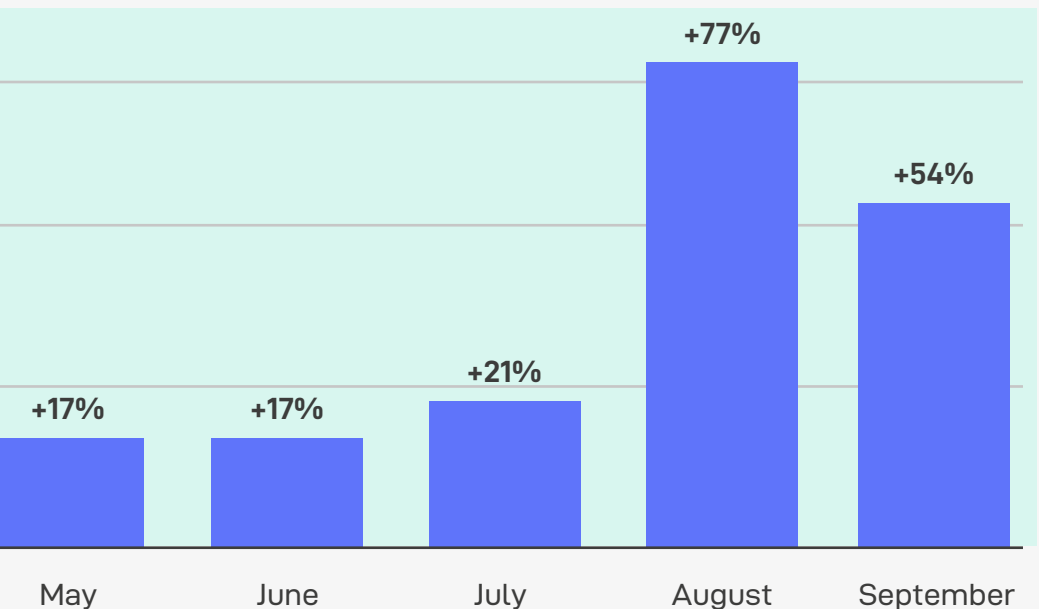
⁵³ Daniele Condorelli and Jorge Padilla, 'Harnessing Platform Envelopment through Privacy Policy Tying', (SSRN, 1 January 2020): <https://ssrn.com/abstract=3504025>

NPO (publisher) revenue increase, after removing all 3rd party ad tracking in 2020

Source: Irish Council for Civil Liberties



This is why such an in-depth reform of targeted advertising must go hand in hand with a strong enforcement of data protection, privacy legislation, and competition law.



“Making dominant
interoperable thro
secure mechanis
protocols) would
for example, to m
Facebook to an al
media service wit
their contacts.”

at online platforms
ough open and
ms (APIs or open
empower users,
ove from
ternative social
thout losing

4.3 Enable real alternatives

Any upcoming reform of the advertising industry needs to tackle existing power imbalances and lead to a new internet – an internet where alternative digital services can thrive, where monopolies are broken up and where interoperable services allow people to migrate from the *Ancien Digital Régime* to the new democratic digital era that will replace it. In order to make this change happen, we suggest the following urgent steps:

▸ Ensure data protection and privacy rights now

Data Protection Authorities (DPAs), and in case of inaction, the European Commission, must enforce the GDPR and ensure that the right to data protection is prioritised over manipulative business models.

For this to happen, national data protection authorities must be given the political support and financial resources to investigate infringements of the ePrivacy Directive and the GDPR.⁵⁴

EU policy makers need to urgently adopt and implement a strong ePrivacy Regulation. All trackers, whether they are placed for the purpose of advertisement or not, would be deactivated by default, unless they are necessary for the site to function (language preferences, shopping cart, etc.).

If privacy by design and by default became the norm for all services and products available to the public,⁵⁵ the pervasive tracking practices of current advertising and platform industries,

and the useless cookie banners behind which they hide, would quickly end.

DPA's must take actions against the exploitative and intrusive use of personal data at the core of the ad tech business model. The European Data Protection Board (EDPB), the European Data Protection Supervisor (EDPS), and the EU Fundamental Rights Agency should provide guidance on how such a structural reform can be harmonised and implemented throughout the EU.

The EU needs to ensure that appropriate funding exists for the necessary research and support to explore alternative business models, notably for publishers and quality journalism.

▸ **Ensure meaningful interoperability and data portability**

A key condition to escape dominant online platforms is to ensure that people can move between similar services without being cornered in digital silos.

Making dominant online platforms interoperable through open and secure mechanisms (APIs or open

protocols) would empower users, for example, to move from Facebook to an alternative social media service without losing their contacts.

They would be free to choose the platform that respects their preferences, for instance in terms of content moderation practices or data protection, rather than being stuck with the incumbent platform merely because everybody else is stuck there as well.⁵⁶

▸ **Algorithmic transparency by default**

Data protection authorities must ensure that ad tech companies and online platforms uphold fundamental rights standards in the creation, development and use of automated decision-making systems, especially those that use 'Artificial Intelligence'.

All recommendations of the Council of Europe regarding the human rights impact of algorithmic systems must be ensured by Council of Europe member states.⁵⁷

Significant reform of how online advertising works combined with the implementation of strong privacy and data protection rules, enforceable transparency, and a legally-binding, human-rights based approach will ensure that the targeted-advertising industry can be held accountable for the way they shape our online environment.

The upcoming proposal for a Digital Services Act (DSA) and the ePrivacy Regulation are key instruments that will provide the opportunity for the European Union to decide how central aspects of the internet will look like in the coming years – probably not only for Europeans but for the rest of the world as well.

⁵⁴ In this regard, see the response of the Information Commissioner's Office which keeps failing to use its powers to investigate and put an end to the data breach affecting UK citizens: <https://twitter.com/johnnyryan/status/1258381720061124608>

⁵⁵ EDRI, 'Privacy by default and by design': https://edri.org/files/eprivacy/e-privacy-onepager_privacy-by-default.pdf

⁵⁶ See our position paper on the Digital Services Act, EDRI, 'Platform Regulation Done Right' (2020), https://edri.org/wp-content/uploads/2020/04/DSA_EDRiPositionPaper.pdf and Laureline Lemoine, 'The impact of competition law on your digital rights' (EDRI, 2020): <https://edri.org/the-impact-of-competition-law-on-your-digital-rights> and <https://www.eff.org/deeplinks/2019/10/adversarial-interoperability>

⁵⁷ Recommendation CM/Rec (2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems, https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154

“If privacy by design and by default became the norm for all services and products available to the public, the pervasive tracking practices of current advertising and platform industries, and the useless cookie banners behind which they hide, would quickly end.”

Sources

News Articles

Alex Barker, 'Half of online ad spending goes to industry middlemen' (The Financial Times, 6 May 2020), <https://www.ft.com/content/9ee0ebd3-346f-45b1-8b92-aa5c597d4389>

Caroline Cadwalladr, 'The great British Brexit robbery: how our democracy was hijacked' (The Guardian, 7 May 2017), <https://www.theguardian.com/technology/2017/may/07/the-great-british-brex-it-robbery-hijacked-democracy>

Jessica Davies, 'After GDPR, The New York Times cut off ad exchanges in Europe - and kept growing ad revenue' (Digiday, 16 January 2019), <https://digiday.com/media/gumgumtest-new-york-times-gdpr-cut-off-ad-exchanges-europe-ad-revenue>

David Dayen, 'Ban Targeted Advertising' (The New Republic, 10 April 2018), <https://newrepublic.com/article/147887/ban-targeted-advertising-facebook-google>

Gilad Edelman, 'Why Don't We Just Ban Targeted Advertising?' (Wired, 22 March 2020), <https://www.wired.com/story/why-dont-we-just-ban-targeted-advertising>

Glenn Greenwald, 'The CIA's Murderous Practices, Disinformation Campaigns, and Interference in Other Countries Still Shape the World Order and U.S. Politics' (The Intercept, 21 May 2020) <https://theintercept.com/2020/05/21/the-cias-murderous-practices-disinformation-campaigns-and-interference-in-other-countries-still-shapes-the-world-order-and-u-s-politics>

Alex Hern, 'Netflix's biggest competitor? Sleep' (The Guardian, 18 April 2017), <https://www.theguardian.com/technology/2017/apr/18/netflix-competitor-sleep-uber-facebook>

David Ingram, 'Google, Facebook show power of ad duopoly as rivals stumble' (Reuters, 28 July 2017), <https://uk.reuters.com/article/us-alphabet-facebook-analysis/google-facebook-show-power-of-ad-duopoly-as-rivals-stumble-idUKKBN1AD1ZY>

Paul Lewis, 'Fiction is outperforming reality: how YouTube's algorithm distorts truth' (The Guardian, 2 February 2018), <https://www.theguardian.com/technology/2018/feb/02/how-youtubes-algorithm-distorts-truth>

Arwa Mahdawi, 'Targeted ads are one of the world's most destructive trends. Here's why' (The Guardian, 5 November 2019), <https://www.theguardian.com/world/2019/nov/05/targeted-ads-fake-news-clickbait-surveillance-capitalism-data-mining-democracy>

Andrew Marantz, 'Big Swinging Brains and fashy trolls: how the world fell into a clickbait death spiral' (The Guardian, 7 February 2020) <https://www.theguardian.com/technology/2020/feb/07/big-swinging-brains-fashy-trolls-clickbait-death-spiral-internet-media>

Rani Molla, 'Law enforcement is now buying cellphone location data from marketers' (Vox, 7 February 2020) <https://www.vox.com/recode/2020/2/7/21127911/ice-border-cellphone-data-tracking-department-homeland-security-immigration>

David Pidgeon, 'Where did the money go? Guardian buys its own ad inventory' (Mediatel, 04 October 2016), <https://mediatel.co.uk/news/2016/10/04/where-did-the-money-go-guardian-buys-its-own-ad-inventory>

Byron Tau and Michelle Hackman, 'Federal Agencies Use Cellphone Location Data for Immigration Enforcement' (The Wall Street Journal, 7 February 2020) <https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-1158107860>

Charlie Warzel, 'The Loophole That Turns Your Apps Into Spies' (The New York Times, 24 September 2018), <https://www.nytimes.com/2019/09/24/opinion/facebook-google-apps-data.html>

Blog posts and websites

Andreea Belu, 'Real Time Bidding: The auction for your attention' (EDRI, 4 July 2019), <https://edri.org/real-time-bidding-the-auction-for-your-attention>

Bennett Cyphers, 'Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance' (2 December 2019) <https://www.eff.org/wp/behind-the-one-way-mirror>

Ronald Deibert, 'The Road to Digital Unfreedom: Three Painful Truths About social media' (Journal of Democracy, January 2019), <https://www.journalofdemocracy.org/articles/the-road-to-digital-unfreedom-three-painful-truths-about-social-media>

Cory Doctorow, 'Adversarial Interoperability' (EFF, 2 October 2019) <https://www.eff.org/deeplinks/2019/10/adversarial-interoperability>

Epic.org, 'Online Tracking and Behavioral Profiling', <https://epic.org/privacy/consumer/online-tracking>

EDRI, 'Tear Down the Tracking Wall' (2017) <https://edri.org/tear-down-the-tracking-wall>

Augustine Fou, 'How brands are Solving Ad Fraud Themselves' (LinkedIn, 27 February 2019), <https://www.slideshare.net/augustinefou/how-brands-are-solving-ad-fraud-themselves>

EDRI, 'Your privacy, security and freedom online are in danger' (2016) <https://edri.org/our-work/privacy-security-freedom>

Brandi Geurnik, 'Our Recommendation to YouTube', (Mozilla Foundation, 14 October 2020) <https://foundation.mozilla.org/en/blog/our-recommendation-youtube>

Abi Gibbons, 'Time for change and transparency in programmatic advertising', (ISBA, 6 May 2020) <https://www.isba.org.uk/news/time-for-change-and-transparency-in-programmatic-advertising>

Karolina Iwańska, '10 Reasons Why Online Advertising is Broken' (Panoptikon Foundation, 9 January 2020), <https://en.panoptikon.org/online-advertising-is-broken>

Karolina Iwańska, 'Behavioural Advertising 101' (Panoptikon Foundation, 9 January 2020), <https://en.panoptikon.org/online-advertising-is-broken>

Andrew Laughlin, 'Fake ads; real problems: how easy is it to post scam adverts on Facebook and Google?' (Which? 6 July 2020) <https://www.which.co.uk/news/2020/07/fake-ads-real-problems-how-easy-is-it-to-post-scam-adverts-on-google-and-facebook>

Laureline Lemoine, 'The impact of competition law on your digital rights' (EDRi, 19 February 2020), <https://edri.org/the-impact-of-competition-law-on-your-digital-rights>

Diego Naranjo, 'Five things the online tracking industry gets wrong' (EDRi, 13 September 2017), <https://edri.org/five-things-the-online-tracking-industry-gets-wrong>

Mozilla Foundation, 'YouTube Regrets' <https://foundation.mozilla.org/en/campaigns/youtube-regrets>

Mozilla and independent researchers to Google and Facebook, 'Facebook and Google: This is What an Effective Ad Archive API Looks Like' (Mozilla, March, 2019), <https://blog.mozilla.org/blog/2019/03/27/facebook-and-google-this-is-what-an-effective-ad-archive-api-looks-like>

nyob, 'Say "NO" to cookies – yet see your privacy crumble?' (NOYB, 10 December 2019), <https://noyb.eu/en/say-no-cookies-yet-see-your-privacy-crumble>

Privacy International, 'Why am I really seeing that ad? The answer might be Real Time Bidding (RTB)' (21 May 2019), <https://privacyinternational.org/explainer/2974/why-am-i-really-seeing-ad-answer-might-be-real-time-bidding-rtb>

Privacy International, 'No Body's Business But Mine: How Menstruation Apps Are Sharing Your Data' (9 September 2019), <https://privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruations-apps-are-sharing-your-data>

Privacy International, 'I asked an online tracking company for all of my data and here's what I found' (7 November 2018) <https://privacyinternational.org/long-read/2433/i-asked-online-tracking-company-all-my-data-and-heres-what-i-found>

Johnny Ryan, 'Failure to enforce the GDPR enables Google's monopoly' (Brave, 18 February 2020), <https://brave.com/competition-internal-external>

Elizabeth Anne Watkins, 'Journalists are rightly suspicious of AdTech. They also depend on it' (Columbia Journalism Review, 4 December 2018), https://www.cjr.org/tow_center/journalists-are-rightly-suspicious-of-ad-tech-they-also-depend-on-it.php

Simona Levi, 'The fight against disinformation: a proposal for regulation'. (OpenDemocracy, 5 May 2020), <https://www.opendemocracy.net/en/democraciaabierta/fight-against-disinformation-proposal-regulation>

Reports

Amnesty International, 'Surveillance Giants; How the business model of Google and Facebook threatens human rights' (21 November 2019), <https://www.amnesty.org/en/documents/pol30/1404/2019/en>

Avaaz, 'Why is YouTube Broadcasting Climate Misinformation to Millions?' (6 January 2019) https://secure.avaaz.org/campaign/en/youtube_climate_misinformation

Avaaz, 'How Facebook Can Flatten the Curve of the Coronavirus Infodemic' (15 April 2020) https://avaazimages.avaaz.org/facebook_coronavirus_misinformation.pdf

CookieBot and EDRI, 'Ad Tech Surveillance on the Public Sector Web' (2019), <https://www.cookiebot.com/media/1136/cookiebot-report-2019-ad-tech-surveillance-2.pdf>

European Parliamentary Research Service, 'Polarisation and the use of technology in political campaigns and communication' (7 March 2019) [https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU\(2019\)634414](https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2019)634414)

EDRI, 'How the Internet works' (2012), https://edri.org/files/2012EDRIPapers/how_the_internet_works.pdf

Global Disinformation Index, 'Ad-Funded COVID 19 Disinformation: Money, Brands & Tech' (8 July 2020) https://disinformationindex.org/wp-content/uploads/2020/07/GDI_Ad-funded-COVID-19-Disinformation-1.pdf

Karolina Iwańska and Katarzyna Szymielewicz, 'Who (really) targets you? Facebook in Polish election campaigns' (Panoptikon Foundation, April 2020) <https://panoptikon.org/political-ads-report>

Nicolas Kayser-Bril, 'Left on Read: How Facebook and others keep researchers in the dark' (Algorithm Watch, 9 July 2020) <https://algorithmwatch.org/en/story/left-on-read-facebook-data-access>

Harriet Kingaby and Frederike Kaltheuner, 'Ad Break for Europe: The race to regulate digital advertising and fix online spaces', (September 2020) https://assets.mofoprod.net/network/documents/Ad_Break_for_Europe_FINAL_online.pdf

Floris Kreiken, 'Transparent consumers – a report by Bits of Freedom' (EDRI, 24 February 2016) <https://edri.org/transparent-consumers-a-report-by-bits-of-freedom>

Nathalie Maréchal, Ellery Roberts Biddle, 'It's Not Just the Content, It's the Business Model: Democracy's Online Speech Challenge' (Ranking Digital Rights and New America, 16 March 2020), <https://www.newamerica.org/oti/reports/its-not-just-content-its-business-model>

Norwegian Consumer Council – Forbrukerrådet, 'Out Of Control: How consumers are exploited by the online advertising industry' (14 January 2020), <https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf>

Norwegian Consumer Council – Forbrukerrådet, 'Deceived by design, How tech companies use dark patterns to discourage us from exercising our rights to privacy' (27 June 2018), <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf>

Johnny Ryan, 'Behavioural advertising and personal data' (September 2018), <https://brave.com/wp-content/uploads/2018/09/Behavioural-advertising-and-personal-data.pdf>

Birgit Stark and Daniel Stegmann, 'Are Algorithms a Threat to Democracy? The Rise of Intermediaries: A Challenge for Public Discourse' (Algorithm Watch, May 2020) <https://algorithmwatch.org/en/wp-content/uploads/2020/05/Governing-Platforms-communications-study-Stark-May-2020-AlgorithmWatch.pdf>

Xnet, '#FakeYou, Fake News and Disinformation – Governments, political parties, mass media, corporations, big fortunes: the monopoly of information manipulation and threats to freedom of expression' (Xnet, October 2019) <https://xnet-x.net/informe-fake-news-desinformacion>

Academic articles

Reuben Binns, Ulrik Lyngs, Max Van Kleek, Jun Zhao, Timothy Libert, Nigel Shadbolt, 'Third Party Tracking in the Mobile Ecosystem' (2018) <https://arxiv.org/pdf/1804.03603.pdf>

Daniele Condorelli and Jorge Padilla, 'Harnessing Platform Envelopment through Privacy Policy Tying' (16 December 2019), <https://ssrn.com/abstract=3504025>

Rob van Eijk, [diss. Leiden], 'Web Privacy Measurement in Real-Time Bidding Systems. A Graph-Based Approach to RTB System Classification' (January 29, 2019). SSRN: <https://ssrn.com/abstract=3319284>

Jeff Gary & Ashkan Soltani, 'First Things First: Online Advertising Practices and Their Effects on Platform Speech' (The Knight Institute, 21 August 2019), <https://knightcolumbia.org/content/first-things-first-online-advertising-practices-and-their-effects-on-platform-speech>

Veronica Marotta, Vibhanshu Abhishek & Alessandro Acquisti, 'Online Tracking and Publishers' Revenues: An Empirical Analysis' (May 2019), https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf

Justin McCarthy, In U.S., most oppose micro-targeting in online political ads (Knight Foundation, 2 March 2020) <https://knightfoundation.org/articles/in-us-most-oppose-micro-targeting-in-online-political-ads>

Lisa Maria Neudert and Nahema Marchal, 'Polarisation and the use of technology in political campaigns and communication' (Panel for the Future of Science and Technology, European Parliamentary Research Service, March 2019)

Urbano Reviglio and Claudio Agosti, 'Thinking Outside the Black-Box: The Case for "Algorithmic Sovereignty" in Social Media' (Sage Journals, 28 April 2020) <https://doi.org/10.1177/2056305120915613>

Márcio Silva, Lucas Santos de Oliveira. et al., 'Facebook Ads Monitor: An Independent Auditing System for Political Ads on Facebook' (31 January 2020) <https://arxiv.org/pdf/2001.10581.pdf>

Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz, '(Un)informed Consent: Studying GDPR Consent Notices in the Field' (ACM SIGSAC Conference on Computer and Communications Security, 2019), <https://arxiv.org/pdf/1909.02638.pdf>

Others

Article 29 Data Protection Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (wp251rev.01), adopted on 6 February 2018, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

Committee of Ministers to member States on the human rights impacts of algorithmic systems, available at https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154

European Commission, 'European Commission survey shows citizens worry about interference ahead of the European elections' (Press Release, 26 November 2018) https://ec.europa.eu/commission/presscorner/detail/en/IP_18_6522

European Data Protection Board

(EDPB), Guidelines 05/2020 on consent under regulation 2016/679 (2020) https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

EDRi, 'Privacy by default and by design', https://edri.org/files/eprivacy/e-privacy-onepager_privacy-by-default.pdf

EDRi, 'Platform Regulation Done Right' (2020) https://edri.org/wp-content/uploads/2020/04/DSA_EDRiPositionPaper.pdf

Information Commissioner's Office,

'Update report into AdTech and real time bidding' (20 June 2019) <https://ico.org.uk/media/about-the-ico/documents/2615156/AdTech-real-time-bidding-report-201906.pdf>

Complaint filed with the UK Information Commissioner's office by **Mr James Killock and Mr Michael Veale**, <https://brave.com/wp-content/uploads/2018/09/ICO-Complaint-.pdf>

This publication was made possible thanks
to contributions by:



▾ **Press enquiries**

press@edri.org

▾ **Brussels office**

brussels@edri.org

▾ **Phone number**

+32 2 274 25 70

▾ **Visit us**

Rue Belliard 12

1040 Brussels

Belgium

▾ **Follow us**

Twitter

Facebook

LinkedIn

Youtube



EUROPEAN DIGITAL RIGHTS

European Digital Rights (EDRi) is the biggest European network defending rights and freedoms online.

We promote, protect and uphold human rights and the rule of law in the digital environment, including the right to privacy, data protection, freedom of expression and information.

www.edri.org