STUDY
Internet
Address: http://~www.a-study-about-surveillance-based~advertising.com
Internet

THE FUTURE OF ONLINE ADVERTISING

Exploring the impacts of surveillance-based advertising, current trends in adtech and the challenges and opportunities of a total ban on the use of personal data.

Duncan McCann, Will Stronge, Phil Jones

THE GREENS/EFA in the European Parliament
Autonomy

ACKNOWLEDGMENT

All errors are the sole responsibility of the authors and being interviewed should not be considered approval or endorsement of any of the arguments or conclusions in this report. We extend our thanks to all of those who offered guidance and took the time to be interviewed as part of this research:

Catherine Armitage, AWO; Robert Blank, Axel Springer; Robin Berjon, New York Times; Rueben Binns, Oxford Uni; Erik Brugge, Kobler; Christoph Fiedler, European Newspaper Publisher Association; Dr. Augustine Fou, ex CMO and adfraud expert; Bob Hoffman, Type A Group; Tim Hwang, Author; Karolina Iwańska, Panoptykon; Jason Kint, Digital Content Next; Ailo Krogh Ravn, Forbrukerradet; Don Marti, Café Media; Rasmus Nielsen, Oxford University; Tanya O'Carrol, campaigner; Matt Rogerson, The Guardian; Johnny Ryan, Irish Council of Civil Liberties; Tom van Bentheim, OptOutAdvertising; Pat Walshe, Privacy Matters; Linda Worp, OptOutAdvertising; Aram Zucker Scharf, Washington Post

Authors: Duncan McCann, Will Stronge, Phil Jones

This study has been commissioned by the **Greens/EFA.**

Published in October 2021.

THE AUTHORS

Duncan McCann is an Affiliate Researcher at Autonomy. Duncan is the main author and has worked for 10 years in the tech industry. He also now leads the Digital Economy Programme at the New Economics Foundation, where he is working to create a new regulatory and policy environment, as well as grassroots alternatives for the digital economy, as well as continuing to work freelance. Duncan's recent work has focused on the data collection practices of tech companies and problems with adtech, especially children.

Will Stronge is Autonomy's director of research and co-author. He has led on all major Autonomy projects to date, managing workflow, making analysis and writing proposal in a variety of policy areas including unemployment, working time, basic income and digital platform regulation. He holds a PhD in politics and philosophy from the University of Brighton and is Autonomy's lead industry consultant and with Helen Hester is currently writing Post-work (Bloomsbury 2022).

Phil Jones is co-author and one of the project's core researchers and member of the Autonomy Digital hub. His expertise lies in digital work, clickwork and surrounding policy. He is the author of *Work Without the Worker* (Verso, 2021).

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The rationale for collecting, selling, and sharing data is often based on the need to monetise our attention through the provision of personalised adverts. There is perhaps nothing that exemplifies the modern data economy more than the way that adverts are delivered online.

The form of advertising that dominates our online ecosystem, where the advert you see is based on the data, often personal, that the website publisher, and its adtech partners know about you, is very different from the forms we have seen over the last hundred years. During the twentieth century, advertising was all about companies and organisations securing the best space to show off their wares. Perhaps a strategically placed billboard, a particular magazine, or – more recently – a radio or television slot.

Today technology promises to ensure that we only see 'relevant' adverts that we actually want to see, thereby removing the annoyance of advertising and turning it into something useful. In reality, this new form of advertising has not won over a sceptical public, who when given a real choice – as they were recently on Apple iOS devices – reject this form of advertising en masse. In this report we explore some of the many inter-related reasons for this widespread rejection.

Given that it is a major funding source for some of the internet's core services, from search to maps to social media, there is a surprising lack of knowledge about how online personal data-based advertising works. In fact, when someone clicks a link to a webpage, between their clicking and the page loading, information about them is compiled and sent out in order for advertisers, or more usually adtech partners working on their behalf, to judge whether they want to show them an advert and at what price. These are called 'bid requests'. They can include hundreds of data points including very sensitive information, such as a whether a person suffers from depression, has children with special needs or is receiving support for incest or abuse. **We estimate that this is happening over 84bn times per day for EU internet users, representing 304 times per person per day. The frequency with which our sensitive personal data is broadcast across the auction network to thousands of adtech companies is why the system has been called the 'world's biggest data breach'.** [1]

But illegality isn't the only negative impact that this form of advertising inflicts on us as individuals, society and business. The online advertising industry, platforms, and tech giants claim that tracking-based advertising enables free internet browsing, while rewarding publishers for creating content, and enabling advertisers to promote their products or services. This sounds like a win-win situation for all involved. **But in truth, individuals, publishers, and even advertisers themselves are all – to a lesser or greater extent – losing out in terms of their privacy, revenue, or autonomy (or some combination thereof).**

Some actors within the online advertising world are horrified at the negative individual and social

[1] Irish Council for Civil Liberties. (2021). Landmark Litigation. Retrieved from https://www.iccl.ie/rtb-june-2021/

impacts of the sector that they work in and are actively engaged in creating alternative ways to show adverts and monetise content without breaching our rights or harming society. **They show us that there are viable alternatives that we can build the future of the digital economy around.**

Two of the most promising examples are contextual advertising and in-browser systems, where the data never leaves the device. **Contextual advertising, another form of online advertising that pre-dates tracking-based advertising, is enjoying a resurgence. Case studies have shown that it can be more valuable to publishers than tracking-based ads, with one contextual ad agency demonstrating that advertisers were willing to pay 3.4 times more for contextual.**[2] This is where adverts are tailored not to the user, but to the context and content of the article or website itself. This was the normal method of online advertising in the early days of the internet. Even today, contextual advertising is the foundation of Google Search where adverts are targeted to the keywords used in the search query as well as the characteristics of the user. Search ads continue to be among the most expensive adverts with some of the best click-through rates on the internet.

At the same time, certain companies at the heart of the adtech system are also trying to innovate to allow them to keep on targeting based on the personal data that the platforms have managed to collect on their users. **The adtech giants' preferred proposal are various forms of collective targeting. Their proposals continue to rely on massive data gathering and profiling, but no longer broadcasts individual and personal data to the wider adtech network. Under this proposal, adverts are targeted to cohorts or segments, groups of individuals, rather than to individual users with unique features.** An advertiser could, thus, target a group of people who like cars, without any personal data being broadcast. Such proposals address a very narrow conception of the problem, by only changing the type of information broadcast to the auction network, while continuing to use and collect personal data and enable social harms such as threatening national security, manipulating people and polarising society. For example, in a recent article, Johnny Ryan, of the Irish Council of Civil Liberties, notes that they have 'not yet provided sufficient information for one to judge whether its new advertising system will end the enormous data free-for-all among thousands of companies active [in the] online advertising industry'.[3]

For years, there has been a growing chorus of voices describing the dangerous consequences of tracking-based advertising. As advertising expert, Bob Hoffman, has noted:

> The leaders of our industry – the ANA, the 4As, IAB, and the chief marketing officers of our biggest advertisers – must face up to what adtech is doing to our society and act immediately and decisively to reform it.[4]

[2] Iwańska, K. (2020). Privacy friendly advertising. Panoptykon Foundation, p. 17. Retrieved from https://en.panoptykon.org/privacy-friendly-advertising

[3] Ryan, J. (2021). 4 big questions about Google's new privacy position. Irish Council for Civil Liberties. Retrieved from https://www.iccl.ie/digital-data/4-big-questions-about-googles-new-privacy-position/

[4] Hoffman, B. (2021). Ad Contrarian: How adtech helped radicalise the USA. Campaign Live. Retrieved from https://www.campaignlive.co.uk/article/ad-contrarian-adtech-helped-radicalise-us/1704228

On 3 March 2021, Google, a company at the heart of creating and promoting tracking-based advertising, published a blog confirming that it would change its online advertising system, and that it announced to move away from 'any technology used for tracking individual people as they browse the web.'[5] Although many who rely on advertising online see this as an attempt by Google to increase their market share by attracting even more advertising spending within their own walled gardens. **The change will require organisations to alter the way that they place adverts online, potentially impacting their revenue and impacting the economics of particular sectors.** Although, as with all transitions there will be those who are more affected by the changes, leaving big tech to decide on the future will be hugely problematic for publishers, as well as all those who currently rely of ad revenue for the sustainability of their business.

The present report contends that publishers, SMEs and the free online services, such as search and social media, can all continue to operate without the ability to target specific individuals, just as they survived before tracking-based advertising was invented.

Only by ending the tracking-based model can publishers, adtech companies and big tech begin to develop a relationship on more equitable and less extractive grounds. A ban would create certainty in the market, assuming the rules were enforced, and would require both publishers and advertisers to move to a new way of targeting their adverts. This would create a level playing field for publishers and allay their fears of moving unilaterally because advertisers would not be able to move the spend to publishers still using tracking-based advertising. In addition, publishers can also expect to capture more of each € spent on advertising because unlike tracking based advertising, where the publisher can expect to keep as little as 30%, contextual platforms offer publishers as much as 85%. This increase in the percentage gives some of the other variables in the system some slack to adjust over time. This means that even if there was a drop in advertising volume or price, the amount in publisher's pockets may remain static.

We conclude that a ban on the use of personal data to target adverts online has a positive impact on the many negative effects that widespread use of the system creates including individuals' data rights, the proliferation of disinformation and the decimation of fraud. This will have positive effects for individuals and society. Aside from the adtech industry itself, we see many opportunities for publishers and advertisers to survive, and even flourish, in a post personal data advertising world, despite having to navigate a complex transition.

[5] Temkin, D. (2021). Charting a course towards a more privacy first web. Retrieved from https://blog.google/products/ads-commerce/a-more-privacy-first-web

1

INTRODUCTION

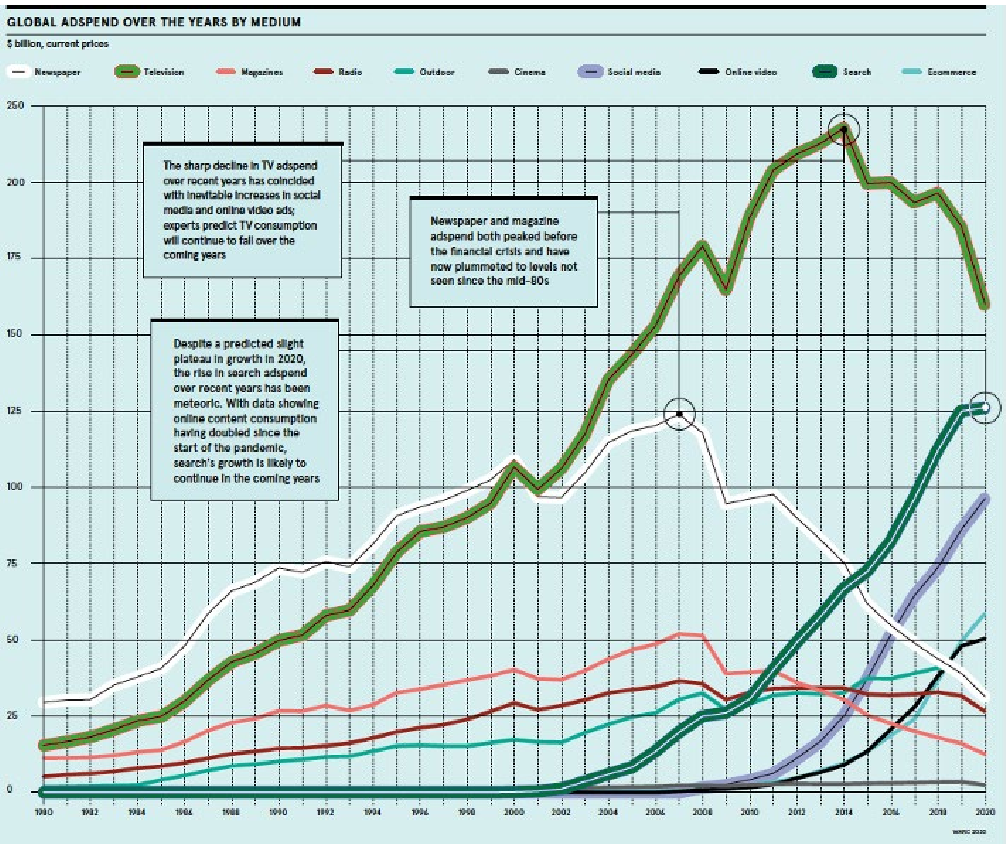
Our digital world today is recording and tracking user's every move, creating detailed profiles of users to show them relevant adverts targeted at their interests. The hunger for data has created a massive incentive for all digital companies, large and small, to collect as much information about individuals as possible – and create platforms that maximise time spent online, even when this might be harmful – all in order to show us as many adverts as possible. Unless we take active measures to limit the companies that engage in this surveillance, these invasive processes will only become more pervasive.

It has not always been this way in the online world. In fact, it's only in the last 25 years that online advertising has emerged from nothing into the pre-eminent business model of the digital economy. When online advertising first emerged in 1994, it followed many of the same rules and principles that offline advertising had. Advertisers had to locate the precise online spaces where an audience existed who would want to buy their products and services. Today, online advertising works in a radically different way, with advertisers able to track individuals as they move around the digital economy to target them wherever they are. What is also remarkable is that just two companies, Google and Facebook, have managed to capture the majority of this new market.

Alphabet, the parent company of Google and YouTube, generated $135bn, representing almost 84% of its revenue from online adverts. In the same period Facebook generated almost $70bn, representing over 98.5% of its revenue, in the same way, bringing in almost $70bn in 2020.[6] Figure 1 shows that revenue for all forms of traditional advertising such as television or newspapers have been in decline since at least 2013, with some starting a downward trend as early as 2007. On the other hand, Figure 1 demonstrates the rapid growth of all forms of online advertising from 2001 onwards, with social media and search advertising alone generating almost $225bn of revenue in 2020.

[6] Wallach, O. (2020). How big tech makes their billions. Visual Capitalist. Retrieved from https://www.visualcapitalist.com/how-big-tech-makes-their-billions-2020

Figure 1 – Global $bn spent on advertising per medium



The sharp decline in TV adspend over recent years has coincided with inevitable increases in social media and online video ads; experts predict TV consumption will continue to fall over the coming years

Newspaper and magazine adspend both peaked before the financial crisis and have now plummeted to levels not seen since the mid-80s

Despite a predicted slight plateau in growth in 2020, the rise in search adspend over recent years has been meteoric. With data showing online content consumption having doubled since the start of the pandemic, search's growth is likely to continue in the coming years

Source: https://www.raconteur.net/infographics/ad-evolution/

The model of online advertising that dominates the market today is tracking-based advertising, where adverts are placed in front of individuals based on personal data provided by the website and any adtech partners with whom they are working. This can be seen as troubling: from the way it invades personal privacy, to the way it might feed disinformation or damage national security.

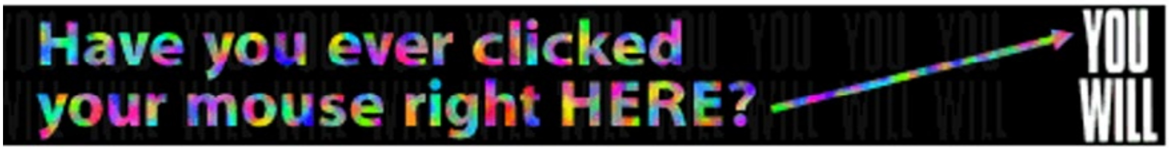
This report explores concerns surrounding the practice of tracking-based advertising today and examines in detail the most significant trends in the adtech market: from the rebirth of contextual advertising to new proposals by Google, Microsoft and others. The report concludes by looking into the potential impact of a ban on the use of personal data in online advertising, both on the issues that we raise in Section 3 as well as on some of the key entities that currently rely on the practice for the operations.

2

THE CURRENT ONLINE ADTECH ECOSYSTEM

The online ad world has evolved considerably since the first banner ad appeared in 1994 on the Wired website advertising AT&T (See Figure 2). Since that first advert, which relied on novelty and traditional ad placement techniques to induce people to click on the advert, the online advertising industry has changed beyond recognition. In those early days, internet users were still intrigued by new online ads, which led to an incredibly high click rate (the percentage of those who saw the ad and clicked on it) of 44%.[7]

Figure 2: First ever online banner ad



Since then, new forms of advertising have taken over the internet. There are currently three major categories of advertising online, all of which operate in very different ways: search advertising, classified adverts, and display advertising.

Search advertising

This is a marketing technique that places online ads in search engine results. Although paid results were originally hard to distinguish from organic results, in recent years most major search engines have taken steps to clarify where a result has been paid for. The businesses who use this system pay a small fee every time somebody clicks on one of their ads under a 'pay-per-click' model. The most obvious example is the 'sponsored results' that appear at the top of the page following a Google search. Currently, Google dominates the search market and generates the vast majority of all search advertising revenue.[8]

Classified adverts

Here, advertisers pay those managing paid listings to have their product or event included. Classified adverts are commonly used by those wishing to promote job offers, sell a car or property, or promote their services. Prominent examples are paid-for listings on sites such as Autotrader or yell.com.

Display advertising

The final category – which forms the main focus of this report – is display advertising. This involves static or video ads being displayed alongside the content a user is viewing. Facebook generates most of its ad revenue from this form of advertising. Alongside the 'walled gardens' operated by Facebook and others, there is an 'open display market' in which publishers, such as online newspapers, compete in real time to sell advertising inventory to advertisers.

[7] Lafrance, A. (2017). The first ever banner ad on the web. The Atlantic. Retrieved from https://www.theatlantic.com/technology/archive/2017/04/the-first-ever-banner-ad-on-the-web/523728/

[8] Competition and Markets Authority (2020). Online Platforms and Digital Advertising. Retrieved from https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study

> To ensure that adverts are placed in front of those with some interest in the product or service, an elaborate system has been built, involving massive data collection and the profiling of billions of internet users. This method of delivering online advertising is especially worrying in term of its impact on individuals, democracy, society and the publishers and advertisers themselves, as we explore further in section 3.

We now look in more detail at how tracking-based open display advertising works.

1 - How tracking-based open display advertising works

1. When you click on a webpage that has space for display adverts, the page does not come pre-loaded with adverts. As you click, the website you're visiting identifies the number of advertising slots for sale and starts to compile a 'bid request' to sell the ad spaces.

2. To compile this bid request, the website collates as much information about you as possible. This includes personal information from previous visits, as well as data collected from other

3. sources, such as cookies and other profile data bought from brokers, forming a detailed profile of the user.
    a. A standard bid request contains:
        i. a 'unique' user ID
        ii. the URL
        iii. year of birth
        iv. gender
        v. location
        vi. IP address
        vii. interests or segments derived from data already collected and analysed
        viii. Further inferred data based on your existing profile

4. The information contained in the bid request is then used by demand side platforms, working for advertisers, to decide whether, and how much, to bid in an auction for the right to show you a particular advert.

5. The winning bidder gets to place the ad on the page you're viewing and keep a copy of the data in the bid request.

This auction process happens repeatedly every time we surf the internet. Although the total number of bid requests being sent daily is not public, we do know that 'Google's Real Time Bidding (RTB) system now sends people's private data to more companies, and from more websites than two years ago',[9] and that a single ad exchange operated by Verizon using the Interactive Advertising Bureau

[9] Lomas, N. (2020). Ireland's data watchdog slammed for letting adtech carry on 'biggest breach of all time'. TechCrunch. Retrieved from https://techcrunch.com/2020/09/21/irelands-data-watchdog-slammed-for-letting-adtech-carry-on-biggest-breach-of-all-time

(IAB) RTB system now sends 600 billion RTB broadcasts in a day.[10]

For this report we have estimated that bid requests are being sent on EU internet users, containing their personal information, at the rate of at least 84 billion a day[11], or 304 per person per day, across all the ad-exchanges, and are seen by thousands of adtech companies, some of whom could be illegally collecting that data, without us being aware of it.

This whole process is automated from start to finish, with computers compiling the bid requests, AI systems analysing the value to advertisers of showing an advert to the person identified in the BID request and more systems managing the auction and placing the advert. All this usually takes just a tiny fraction of a second to complete.

Although there are many thousands of companies within the wider adtech ecosystem, this masks the fact that the real time bidding sector is dominated by just two organisations: Google and the Interactive Advertising Bureau (IAB), who are responsible for systems respectively known as Authorized Buyers and OpenRTB.

2 - Public attitudes to tracking-based advertising

Whereas in the past the online advertising industry could point to a range of surveys to show that users really wanted relevant adverts as they surfed the web and that they were willing to share data to get it, this illusion is increasingly hard to maintain. For instance, while an industry survey from 2016 proudly proclaimed that 'consumers crave a personalized advertising experience and that 71% of respondents prefer ads tailored to interests and shopping habits',[12] a more recent 2021 poll conducted by YouGov for the Norwegian Consumer Council yielded radically different results. They found that only 20% accepted that adverts should be based on personal information, with almost half thinking that adverts should never be based on personal data.[13]

71%

of respondents prefer ads tailored to interests and shopping habits'

20%

accepted that adverts should be based on personal information, with almost half thinking that adverts should never be based on personal data

Supplementing the important survey data is actual data about how people behave when confronted with tracking-based ads and given the ability to opt out. Firstly, we have seen the rise of ad-blockers, little bits of software that can be added to browsers that enables users to block online adverts, as well as extricate themselves from the tracking-based adverts auction system explained above. Figures for 2019 show that globally across all devices about 30% of users actively use an ad-blocker. Specifically in

[10] Yahoo! ad tech. (2020). Reach your ROAS goals with Verizon Media. Retrieved from https://www.verizonmedia.com/insights/reach-your-roas-goals-with-verizon-media

[11] This figure has been produced through our own calculations multiplying: (number of EU Internet users- prevalence of ad blocking in EU) X average number of page visits per day X avg number of ads per page X use of real time bidding system

[12] Adlucent. (2016). 71% of consumers prefer personalised ads. Retrieved from https://www.adlucent.com/resources/blog/71-of-consumers-prefer-personalized-ads/

[13] Forrukerrådet. (2021). Tracking-based advertising. Retrieved from https://fil.forbrukerradet.no/wp-content/uploads/2021/06/consumer-attitudes-to-tracking-based-advertising.pdf

the EU over 36% of computer users used an ad-blocker, dropping to 23% across mobile.[14] This number is likely to have increased.

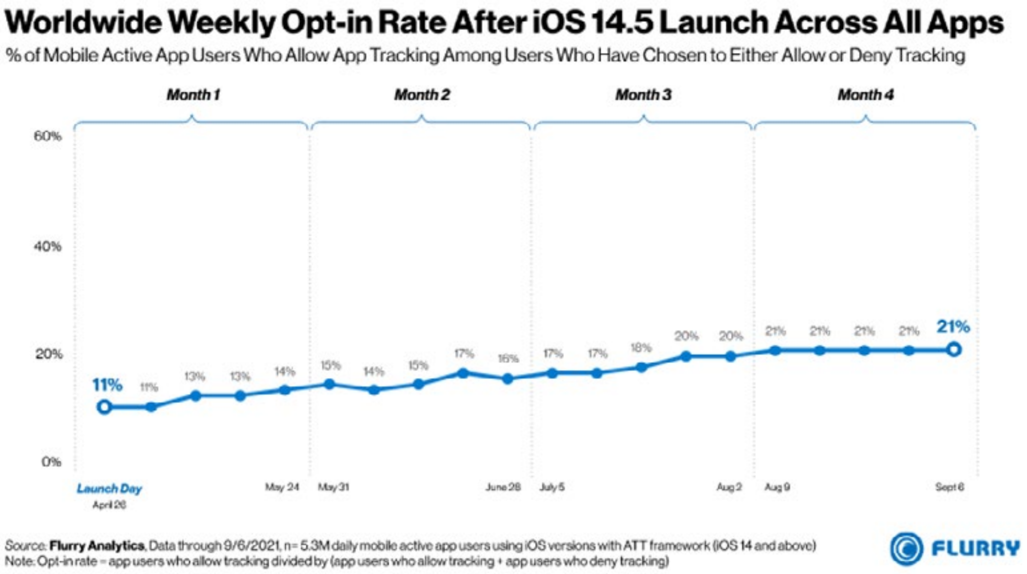
30%
of users actively use an ad-blocker

almost
1/3
of users said they had stopped visiting a website altogether (30%) to avoid being targeted

Beyond ad-blocking, recent work by the UK Information Commissioners Office found that many people are also using other techniques to avoid advertising online. The methods they revealed included practices such as actively deleting marketing cookies (36% of people) and changing browser settings (31%). Most interestingly, almost a third of users said they had stopped visiting a website altogether (30%) to avoid being targeted.[15]

We also now have real data about the number of people who want to opt-in to the tracking-based advertising model thanks to Apple's recent introduction in IOS 14 of the ability for users to easily reject the exchange of data for adverts in a clear and unambiguous fashion. Although opt-in rates have nearly doubled since the launch of the feature in April 2021 as of early September the rates were still at just 21%, as can be seen in the figure below.

Figure 3: Worldwide Weekly Opt-in Rates after iOS 14.5 launch across all Apps



Worldwide Weekly Opt-in Rate After iOS 14.5 Launch Across All Apps

% of Mobile Active App Users Who Allow App Tracking Among Users Who Have Chosen to Either Allow or Deny Tracking

Source: **Flurry Analytics**, Data through 9/6/2021, n= 5.3M daily mobile active app users using iOS versions with ATT framework (iOS 14 and above)
Note: Opt-in rate = app users who allow tracking divided by (app users who allow tracking + app users who deny tracking)

Source: https://www.flurry.com/blog/ios-14-5-opt-in-rate-idfa-app-tracking-transparency-weekly/

[14] SocialMediaToday. (2019). Global Ad Blocking Behavior 2019 [Infographic]. Retrieved from https://www.socialmediatoday.com/news/global-ad-blocking-behavior-2019-infographic/551716/

[15] UK Information Commissioner's Office. (2019). Adtech: Market Research Report. Retrieved from: https://www.ofcom.org.uk/__data/assets/pdf_file/0023/141683/ico-adtech-research.pdf

Why is YouTube Broadcasting Climate Misinformation to Millions?

3

THE IMPACT OF **SURVEILLANCE-BASED ADVERTISING**

A recent statement by Amnesty International neatly encompasses why we need to better understand the impact of tracking-based advertising:

> 'We have already seen that Google and Facebook's vast architecture for advertising is a potent weapon in the wrong hands. Not only can it be misused for political ends, with potentially disastrous consequences for society, but it allows all kinds of new exploitative advertising tactics such as preying on vulnerable people struggling with illness, mental health or addiction. Because these ads are tailored to us as individuals, they are hidden from public scrutiny.'[16]
>
> **Amnesty International**

We will examine the impacts both on the individual as well as wider society and democracy itself.

1 – Democracy & society

1.1 - COMPETITION ISSUES

The way that tracking-based advertising works means that the few companies who control the key infrastructure, such as Google, IAB or Facebook, or can collect the most detailed information about all of us, have a competitive advantage in the sector. The EU Commission has already fined Google €1.49bn for abusing its market dominance of display adverts.[17] In addition, other authorities from the UK[18] to the US[19] have already looked in detail at the area, trying to illuminate and quantify the issues while they assess what action to take.

A recent report by the UK's Competition and Market Authority (CMA) highlighted the dominant position that Google occupies across the whole adtech value chain, as can be seen in figure 4 below. The CMA noted that this kind of dominance raises 'clear conflicts of interest.'[20]

[16] Amnesty International UK (2019) Facebook and Google's pervasive surveillance poses unprecedented danger to human rights – new report. Retrieved from https://www.amnesty.org.uk/press-releases/facebook-and-googles-pervasive-surveillance-poses-unprecedented-danger-human-rights

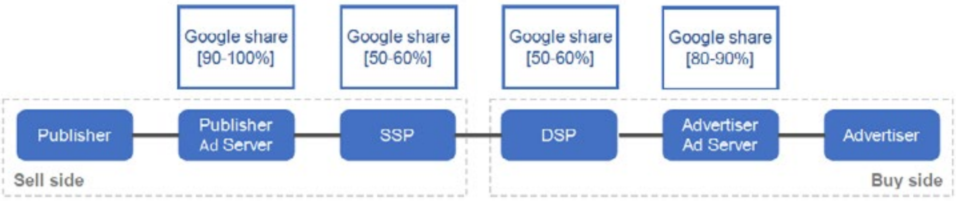
[17] EU Commission (2019) Antitrust: Commission fines Google €1.49bn for abusive practices in online advertising. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1770

[18] Competition and Markets Authority (2020). Online Platforms and Digital Advertising. Retrieved from https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study

[19] Stigler Committee on Digital Platforms. (2019). Final Report. Retrieved from https://www.chicagobooth.edu/research/stigler/news-and-media/committee-on-digital-platforms-final-report

[20] Competition and Markets Authority (2020). Online Platforms and Digital Advertising. Retrieved from https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study

Figure 4: Google's roles in advertising intermediation



Source: UK Competition and Market Authority report: Online platforms and digital advertising

Competition authorities looking into the online advertising sector have identified three issues that result from the lack of competition.

Firstly, the lack of competition may inhibit innovation and the development of new, valuable services for consumers.

Secondly, the lack of competition may lead to prices being higher than they would be in a more competitive market. These high prices manifest in two distinct ways. On the one hand the higher prices that advertisers have to pay may be 'felt in the prices that consumers pay for hotels, flights, consumer electronics, books, insurance and many other products that make heavy use of digital advertising.'[21] So although the services appear to be free, consumers may be paying through increased prices in other sectors driven by high advertising prices. On the other hand, these higher prices mean that as consumers we may not be getting a good deal, since the services are not really free, and that, in reality, we are all being undercompensated for our attention when we go online.

Thirdly, limited choice and competition also have the consequence that people are less able to control how their personal data is used. For many, this means that they have to provide more personal data to platforms than they would like.

1.2 - NATIONAL SECURITY ISSUES

The efficient targeting, even micro-targeting, of people and groups, enabled by tracking-based advertising, is increasingly being recognised as a potential national security issue. A recent article in Cyber Defence Review notes that 'fundamentally, domestic digital privacy is a national security issue,' and sees 'the current advertising economy is enabling and profiting from foreign and domestic information warfare being waged on its citizens.'[22] In September 2020, General Paul Nakasone, NSA Director and Commander of U.S. Cyber Command, called foreign influence operations 'the next great disruptor.'[23] Senator Ron Wyden stated that people 'must understand the serious national secu-

[21] Competition and Markets Authority (2020). Online Platforms and Digital Advertising. Retrieved from https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study

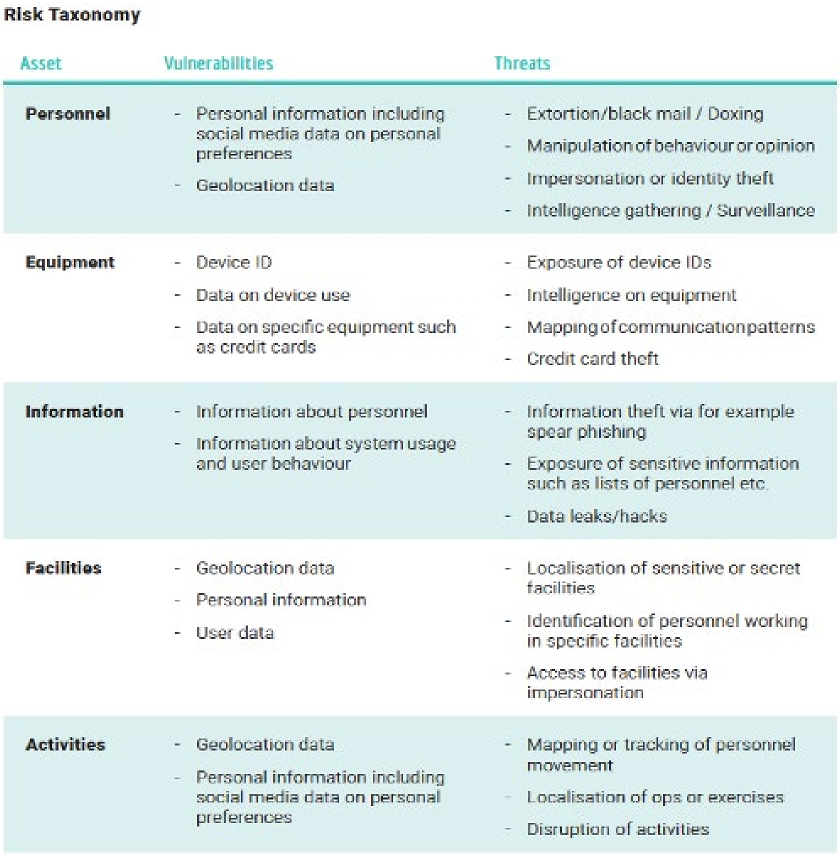
[22] Dawson, J. (2021) Micro-targeting as information warfare, The Cyber Defence Review 6(1): 63-80. Retrieved from https://www.jstor.org/stable/pdf/26994113.pdf

[23] Sparling, B. (2020) The Zhenhua Leak, IOS 14 and National Security. LinkedIn, Retrieved from https://www.linkedin.com/pulse/zhenhua-leak-ios-14-national-security-bryan-sparling.

rity risks posed by the unrestricted sale of Americans' data to foreign companies and governments.'[24]

Many in the west were first alerted to the danger of our tracking-based advertising system being exploited by other countries security services to influence behaviours and decisions in 2017. This was when it was revealed that the Russian government had been using Facebook to try and influence the 2016 US elections.[25] The Russian state continues to be interested in elections of other countries, with the latest evidence coming from Germany where in the run-up to the forthcoming general election RT Deutsch has become one of the biggest advertisers in the country.[26] The research shows that they have been promoting anti-vaccination fears as well as championing the far-right party, Alternative für Deutschland.

Table 1: Risk taxonomy from data leaks



Risk Taxonomy

Asset	Vulnerabilities	Threats
Personnel	- Personal information including social media data on personal preferences - Geolocation data	- Extortion/black mail / Doxing - Manipulation of behaviour or opinion - Impersonation or identity theft - Intelligence gathering / Surveillance
Equipment	- Device ID - Data on device use - Data on specific equipment such as credit cards	- Exposure of device IDs - Intelligence on equipment - Mapping of communication patterns - Credit card theft
Information	- Information about personnel - Information about system usage and user behaviour	- Information theft via for example spear phishing - Exposure of sensitive information such as lists of personnel etc. - Data leaks/hacks
Facilities	- Geolocation data - Personal information - User data	- Localisation of sensitive or secret facilities - Identification of personnel working in specific facilities - Access to facilities via impersonation
Activities	- Geolocation data - Personal information including social media data on personal preferences	- Mapping or tracking of personnel movement - Localisation of ops or exercises - Disruption of activities

Source: NATO Strategy Communications Report - Data Brokers and Security: risks and vulnerabilities related to commercially available data

[24] Davis, W. (2021) Bidstream Data Could Threaten National Security, Senators Warn. Media Post, Retrieved from https://www.mediapost.com/publications/article/362096/bidstream-data-could-threaten-national-security-s.html

[25] Hanlon, B. (2018). A Long Way To Go: Analyzing Facebook, Twitter, and Google's Efforts to Combat Foreign Interference. Alliance for Securing Democracy. Retrieved from https://securingdemocracy.gmfus.org/a-long-way-to-go-analyzing-facebook-twitter-and-googles-efforts-to-combat-foreign-interference/

[26] Scott, M. (2021) Russia sows distrust on social media ahead of German election, Politico. Retrieved from https://www.politico.eu/article/germany-russia-social-media-distrust-election-vladimir-putin/

A recent report by NATO outlined the national security risk from the data broker community and their business model of collecting as much information about all us in order to resell that information to interested third parties. One of the primary reasons for data brokers to exist is to supply the personal data and profiles necessary for a tracking-based advertising model to work. The risk taxonomy, shown in Table 1 below, shows how various types of data, easily obtainable from data brokers, as well as from other actors, can lead to real national security threats.

This issue has recently come to the fore in the US where some Senators raised the potential national security threat inherent in the mass sale of bidstream data[27] which is available to any interested third parties. In response to queries from Senator Ron Wyden, adtech and data brokers revealed that they had sold potentially sensitive bidstream data to companies based in Russia, China, and the United Arab Emirates. He concluded that 'this information would be a goldmine for foreign intelligence services that could exploit it to inform and supercharge hacking, blackmail, and influence campaigns.'[28]

The very same system developed for advertisers to target people with individual level messaging can also be leveraged by states to influence voting behaviour or exploit disinformation campaigns. The adtech sector has inadvertently created a tool that autocratic governments of the past could only dream of.

The Scottish Centre for Crime and Justice Research (SCCJR) recently conducted research which revealed that in the UK national and local government were also using online advertising to target individuals, often based on highly sensitive personal information, to try and 'nudge' people's behaviour. The research uncovered examples ranging from 'a Prevent-style scheme to deter young people from becoming online fraudsters to tips on how to light a candle properly.'[29] These domestic examples of governments actively trying to influence people further demonstrates the real personal and state level risks that tracking-based advertising delivers.

1.3 – THE THREATS OF MICRO-TARGETING

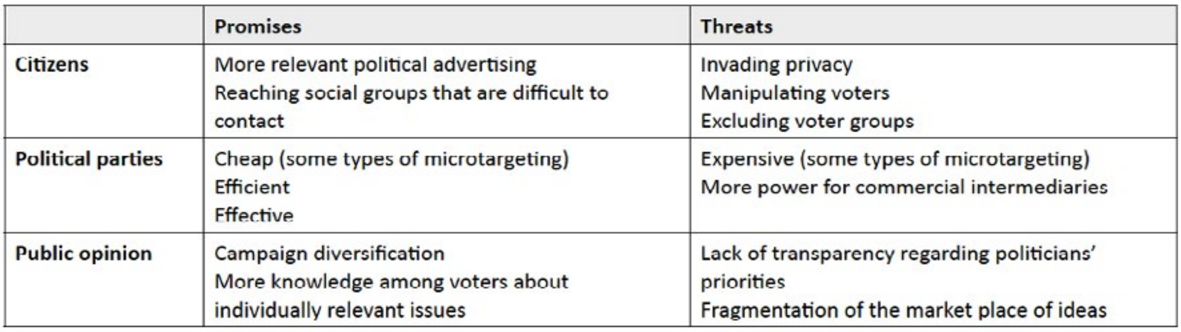
The main difference between military information operations, discussed in the previous section, and political or commercial microtargeting is *who does the targeting* and *who they target.* There is almost no difference in the data they require and the methods and tools they use to influence behaviour. And just as micro-targeting poses national security challenges, it also poses domestic challenges to our democracies and public sphere more generally. Table 2 below highlights the promises and threats of microtargeting. In this section we will focus in on political micro-targeting and its impact.

Table 2: Promises and threats of microtargeting for citizens, parties and public opinion

[27] Bidstream data comes from a publisher or app and includes basic facts about the ad unit, like publisher and URL, device type, IP address and ad format. It also might have other nuggets of info, like location or audience demographic data, that could entice buyers.

[28] Cox, J. (2021) The Hundreds of Little Known Firms Getting Data on Americans. Vice. Retrieved from https://www.vice.com/en/article/n7bdkq/hundreds-companies-bidstream-data-location-browsing

[29] Hern, A. (2021) Study finds growing government use of sensitive data to nudge behaviour. The Guardian. Retrieved from https://www.theguardian.com/technology/2021/sep/08/study-finds-growing-government-use-of-sensitive-data-to-nudge-behaviour



	Promises	Threats
Citizens	More relevant political advertising Reaching social groups that are difficult to contact	Invading privacy Manipulating voters Excluding voter groups
Political parties	Cheap (some types of microtargeting) Efficient Effective	Expensive (some types of microtargeting) More power for commercial intermediaries
Public opinion	Campaign diversification More knowledge among voters about individually relevant issues	Lack of transparency regarding politicians' priorities Fragmentation of the market place of ideas

Source: Zuiderveen Borgesius, F.J., Möller, J., Kruikemeier, S., Ó Fathaigh, R., Irion, K., Dobber, T., Bodo, B. and de Vreese, C., 2018. Online Political Microtargeting: Promises and Threats for Democracy. *Utrecht Law Review*, 14(1), pp.82–96

Political micro-targeting is the use of the tracking-based data driven advertising model to identify individuals or small groups to target them with specific tailored messages designed to appeal to them specifically.

As well as the issues we outline below, it is important to say that political micro-targeting also offers some exciting opportunities for democratic parties to re-engage with the electorate in a meaningful way. Done well it could increase participation in elections and wider public debates as well as lead to increased knowledge among voters about certain topics. The other factor causing many political parties to adopt a micro-targeting strategy is that it can be cheap, efficient, and effective. This potentially gives smaller parties the ability to get their message out effectively while using limited funds. However, smaller parties may rarely have the data or the internal expertise to manage a data-driven campaign. This means they might have to contract costly external expertise, buy access to personal data sets, and pay service providers, which all hand more power to intermediaries. As Bennett notes, in reality, microtargeting 'may very well consolidate power in the larger, and more well–financed, parties and make it more difficult for smaller parties to be nationally competitive.'[30]

On the other hand, however, microtargeting also threatens the public in three ways.

Firstly, it represents a further invasion of our privacy. For microtargeting to be effective, it requires large scale data gathering as well as combining with data collected and bought by others. This is then used to infer sensitive political preferences and interests. As well as the need for this data threatening our rights, it also creates databases containing our sensitive personal information that are valuable targets for hackers. These massive and detailed databases of personal data are, in turn, liable to be reused for other purposes, which could be harmful to particular individuals.

Secondly, people could be manipulated, although it may sometimes be hard to distinguish this from a normal political campaign which aims to influence people and change their mind. A pertinent ex-

[30] Bennett, C. (2013) The politics of privacy and the privacy of politics: Parties, elections and voter surveillance in Western democracies. Retrieved from http://firstmonday.org/ojs/index.php/fm/article/view/4789/3730#1

ample happened in 2016, when Donald Trump's campaign targeted African-American voters with messages designed to deter them for voting by circulating past remarks by Hilary Clinton calling African-American men 'super predators.'[31] The other aspect in which people could be manipulated is through parties presenting themselves as particularly interested or concerned in a particular issue. They could then cynically highlight a different issue for each voter, which could lead to a warped perception of the party's true priorities. This could even be hard to spot since there is no central database of political ads, although some websites do manage their own. If everyone were to receive customised and targeted political information, then this could threaten the public sphere through the fragmentation of the marketplace of ideas leading to a lack of common narrative.

Thirdly, people could be ignored or excluded. Just as we saw with the threat of discrimination, the same tools that allow people to be targeted can also be used to exclude people from messages that, in a democracy, they have a right to hear.

Although political microtargeting has been a feature of the last few US and UK elections it is less prevalent in the EU due to a variety of factors. The use of proportional representation system in the EU means the value of each vote is more evenly spread than in first past the post systems, as operate in UK and US. This means that EU elections are less likely to be decided by a small number of voters in some key districts, as is often the case in the US and UK. Another factor is the smaller budgets that EU parties have to fight elections. In comparison to the US, where the Democrats had a $1.4bn fund to fight the election, the largest party in Germany only have €47m, while the largest Dutch party spent just €4m.[32]

The damaging nature of political microtargeting has led to Twitter banning political adverts altogether, while in 2019 Google announced that political ads could not be targeted beyond age, gender and location.[33] Facebook however continues to allow all forms of microtargeting, despite some minor changes to their rules in 2019.[34]

1.4 - SPREAD OF DISINFORMATION

Although disinformation has been a feature of society since early history, and the internet since its inception, tracking-based advertising has enabled those publishing such information to monetise their content in an unprecedented way. This is because advertisers and their demand-side adtech partners are now able to follow individuals, or individuals with specific characteristics, as they surf the internet. Unsurprisingly, it is cheaper to advertise on disinformation or clickbait sites than on

[31] Green, J. & Issenberg, S. (2016) Inside the Trump Bunker, With Days to Go. Bloomberg. Retrieved from www.bloomberg.com/news/articles/2016-10-27/inside-the-trump-bunker-with-12-days-to-go

[32] Zuiderveen Borgesius, F.J., Möller, J., Kruikemeier, S., Ó Fathaigh, R., Irion, K., Dobber, T., Bodo, B. and de Vreese, C. (2018). Online Political Microtargeting: Promises and Threats for Democracy. Utrecht Law Review, 14(1), pp.82–96.

[33] Spencer, S. (2019) An update on our political ads policy. Google: The Keyword. Retrieved from https://blog.google/technology/ads/update-our-political-ads-policy/

[34] Scott, M. et. al. (2019) Facebook to cave to EU pressure after row over political ad rules. Retrieved from https://www.politico.eu/article/facebook-european-elections-advertising-political-social-media-europe/

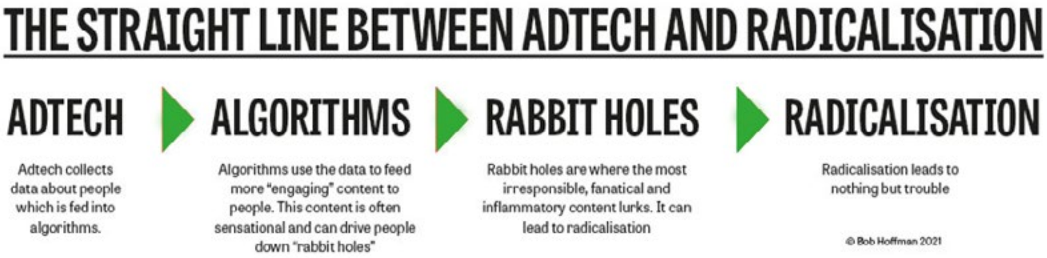
reputable sites. This can result in advertising money from some of the world's biggest brands supporting extremist and fake news content.[35] For instance, NewsGuard found that 'over 4,000 brands bought ads on misinformation websites publishing COVID-19 myths.'[36] Incredibly, this even included vaccine manufacturers like Pfizer.

According to a 2020 report from the Global Disinformation Index, nearly a quarter billion dollars' worth ($235 million) of advertising has been paid to sites spreading disinformation.[37] For the EU, they calculated that over $76m annually was being paid by advertisers to disinformation sites. While some may be running disinformation sites in order to promote specific narratives, others are doing so because of the significant money that can be earned, such as one owner of a network of fake news sites who claimed to be making up to $30k per month from tracking-based advertising.[38]

There is also evidence that adtech companies are buying a small number of adverts on premium publisher websites in order to collect enough information to be able to track those users across the web. The adtech company can then start to place adverts on less premium and disinformation sites since they offer a cheaper way to target the same audience. [39]

These practises do not just enrich purveyors of disinformation, they have serious political implications. Bob Hoffman, an advertising industry expert, has set out a plausible pathway that links the adtech industry and the wider radicalisation and polarisation of society, as can be seen in figure 5.

Figure 5: The Straight line between adtech and radicalisation



THE STRAIGHT LINE BETWEEN ADTECH AND RADICALISATION

ADTECH

Adtech collects data about people which is fed into algorithms.

ALGORITHMS

Algorithms use the data to feed more "engaging" content to people. This content is often sensational and can drive people down "rabbit holes"

RABBIT HOLES

Rabbit holes are where the most irresponsible, fanatical and inflammatory content lurks. It can lead to radicalisation

RADICALISATION

Radicalisation leads to nothing but trouble

© Bob Hoffman 2021

Source: https://www.campaignlive.co.uk/article/ad-contrarian-adtech-helped-radicalise-us/1704228

As the figure above illuminates, the large volumes of data collected by the adtech industry feed into

[35] Iwańska K,. (2020) To track or not to Track: towards privacy friendly and sustainable online advertising. Panoptykon Foundation, retrieved from https://en.panoptykon.org/privacy-friendly-advertising

[36] Skibinski, M. (2020) Thousands of world's most trusted brands funded COVID-10 misinformation, NewsGuard. Retrieved from: https://www.newsguardtech.com/special-report-advertising-on-covid-19-misinformation/

[37] Global Disinformation Index. (2019). The Quarter Billion Dollar Question: How is Disinformation Gaming Ad Tech?. Retrieved from https://disinformationindex.org/2019/09/the-quarter-billion-dollar-question-for-ad-tech/

[38] Sydell, L. (2016) We Tracked Down a Fake-News Creator In The Suburbs. Here's What We Learned. NPR. Retrieved from https://text.npr.org/503146770

[39] Silber, A. (2016) Clickbait and traffic laundering: how ad tech is destroying the web. Guerilla. Retrieved from https://theguerrilla.agency/clickbait-and-traffic-laundering-how-ad-tech-is-destroying-the-web

content recommendation algorithms, which ultimately lead to radicalisation. Indeed, an internal Facebook study, reported in the Wall Street Journal, found that '64% of all extremist group joins are due to our recommendation tools... Our recommendation systems grow the problem.'[40]

Tracking-based advertising's ability to fund disinformation and fuel radicalisation came together to help enable the violence that took place in the US Capitol on January 6th, 2021. As Jake Dubbins, co-chair of the Conscious Ad Network, has noted, 'advertisers have helped fund the misinformation that stoked fires in the US Capitol.'[41] The events of 6th January have done a lot to push to the fore the role of platforms and their algorithms in spreading disinformation. Without the lucrative revenue from tracking-based adverts, disinformation sites would be less prolific, and we would potentially have less radicalisation and polarisation in our society.

> '64% of all extremist group joins are due to our recommendation tools... Our recommendation systems grow the problem.'
>
> An internal Facebook study

1.5 - CARBON EMISSIONS

All online actions consume energy, not only because your laptop or phone needs to be charged, but also because online networks need energy to transfer data and power data centres. Google, for instance, has calculated that a user's average annual use of their search engine generates CO_2 emissions equivalent to one washing machine cycle.[42] Now this is not much when considered individually, but when multiplied by the billions that use Google, energy consumption becomes considerable.

This is also the case for the system that delivers tracking-based adverts. Although each one only takes a minute amount of energy, when multiplied out at an EU or global scale it becomes significant. The only study to have investigated this issue estimated that the global carbon footprint of online advertising was 60m metric tons in 2016.[43] Even though they only looked at the direct emissions from activity to actually serve the advert, it is still equivalent to the total annual greenhouse gas emissions of Ireland in 2019-20.[44]

[40] Horowitz, J. & Seetharaman, D. (2020) Facebook knows it encourages division. Top executives nixed solutions. Wall Street Journal. Retrieved from https://www.wsj.com/articles/facebook-knows-it-encourages-division-top-executives-nixed-solutions-11590507499

[41] Dubbins J., (2021) The Capitol coup shows online harms are now real-world harms – are your ads funding them?. The Drum, retrieved from https://www.thedrum.com/opinion/2021/01/07/the-capitol-coup-shows-online-harms-are-now-real-world-harms-are-your-ads-funding

[42] Google (2009) Powering a search. Retrieved from https://googleblog.blogspot.com/2009/01/powering-google-search.html

[43] Pärissen, M et. al. (2018) Environmental assessment impact of online advertising. Environmental Impact Assessment Review. Retrieved from: https://www.sciencedirect.com/science/article/pii/S0195925517303505

[44] European Parliament (2019) Greenhouse gas emissions by country and by sector. Retrieved from https://www.europarl.europa.eu/news/en/headlines/society/20180301STO98928/greenhouse-gas-emissions-by-country-and-sector-infographic

There are a number of reasons why this estimate is almost certainly an under-estimation, and potentially a significant one. Firstly, since 2016 the volume of tracking-based adverts has increased significantly. Secondly, because the study only looks at the direct emissions, it does not include many activities such as data collection, processing, analysis, the creation of detailed profiles based on that information, the additional data bought data from other companies who have collected and processed it, and the impact of the storage and management of all this information. All of these have a carbon cost, since they require data storage, transfer and analysis. Finally, there has been an increase in the use of, and reliance on, complex machine learning algorithms which can be very energy intensive, to process raw data into actionable and valuable insights for advertisers.

A recent report by the New Weather Institute found that there was 'sound empirical evidence' beyond the direct climate impacts raised above. The report concluded that advertising is indirectly responsible for 'climate and ecological degradation through its encouragement of materialistic values and goals, the consumption-driving work & spend cycle.'[45]

As countries around the world coalesce around the need for concerted action to mitigate the worst impacts of climate change, it will become hard to ignore the contribution of tracking-based advertising.

1.6 – THE RISE OF FRAUD[46]

Online ad fraud is a massive industry which is exploited not just by companies in the adtech ecosystem, but also organised crime. The World Federation of Advertisers predicts that by 2025 adfraud could be worth over $50bn a year to organised crime, representing their second highest source of income after the drug trade.[47] The attractiveness of adfraud is obvious given that the rewards can be significant while the risk of prison or even being caught is miniscule, especially when compared with their other major lines of work, drug trafficking, the arms trade or people smuggling.

By some estimates about twenty-five percent of ad spend is lost to fraud,[48] with experts labelling it 'one of the most profitable crimes with the least amount of risk'.[49] The US Association of National Advertisers, however, estimated that in 2017 it was 'only' $6.5bn, representing 3.6% of global online ad spend.[50] Ad expert Bob Hoffman has compiled startling figures based on numbers produced by

[45] Simms, A. (2020) Badvertising – stop adverts fuelling the climate emergency. New Weather Institute. Retrieved from https://www.newweather.org/2020/08/03/badvertising-stop-adverts-fuelling-the-climate-emergency/

[46] Fou, A. (2021) All Ad Fraud Looks The Same, If You Look. Forbes. Retrieved from:https://www.forbes.com/sites/augustinefou/2021/01/27/all-ad-fraud-looks-the-same-if-you-look/?sh=5e7814d02574

[47] Shields, R. (2016) Adfraud is 'second only to the drugs trade' as a source of income for organised crime. Business Insider. Retrieved from https://www.businessinsider.com/wfa-report-ad-fraud-will-cost-advertisers-50-billion-by-2025-2016-6?op=1&r=US&IR=T

[48] PPC Protect. (2018) The Ultimate list of click fraud and ad fraud statistics 2018. Retrieved from https://ppcprotect.com/ad-fraud-statistics/

[49] Silverman, C. (2018) 8 people are facing charges as a result of the FBI's biggest ever ad fraud investigation. Buzzfeed News. Retrieved from https://www.buzzfeednews.com/article/craigsilverman/3ve-botnet-ad-fraud-fbi-takedown

[50] Boudet, A. (2017) Publicité sur le web: 6,5 milliards de dollars détournés pa des sites frauduleux en 2017. Numerama. Retrieved from: https://www.numerama.com/tech/261182-publicite-sur-le-web-65-milliards-de-dollars-detournes-par-des-sites-frauduleux-en-2017.html

Adage and SpiderLabs which estimates the global loss to fraud at over $66bn, which is more than the total US adspend on radio, newspaper, magazine and outdoor advertising.[51]

The range of activity used to conduct adfraud is staggering, with bots[52] acting as a key to enable this activity at scale. Bots are used to generate false traffic, create fake audience segments, fake clicks and falsify purchases. They help create a virtuous cycle, whereby bots loading webpages creates traffic thereby generating more ads to sell. Bots can then click on the adverts to simulate engagement. Curated bots can target certain websites and pretend to be desirable audiences who advertisers are willing to pay extra to target.

We will examine very briefly four examples of fraudulent practices to expose the range and sophistication of the sector. Three are technical issues, such as click fraud, domain spoofing and unviewable ads, while the fourth is problematic business practice.

Remarketing fraud is where adtech companies make it appear that specific purchases were caused by remarketing programs, when no ads were even run, as experienced by Uber. In Uber's case, the adtech intermediaries that they were working with created false attribution records. This made it appear as if a significant number of the new installs of the Uber app were as a direct result of the marketing campaigns that the adtech companies were running. In reality, as Uber discovered when they reduced their spend by 90% from $150million to just $15million, almost all of these installs had happened naturally without any influence of an advert.[53]

Click fraud involves the widespread practice of using bots and automated scripts, as well as occasionally armies of paid humans, to click on adverts. This results in the advertising 'working' but capturing no attention. Although the exact scale is hard to quantify, one study estimated that in 2018 $51m was lost every day to click fraud, totalling $18bn.[54]

Domain spoofing uses unknown websites that are made to look like a high value website in order to get ads placed by legitimate advertisers. The website owners then use botnets[55] to drive traffic to the spoof site and other tricks to drive ad revenue to the site.

Another way in which the adtech ecosystem is accused of unfairly pocketing too much of the ad spend is through rebates being passed back through the system, with the Association of National

[51] Hoffman, B. (2020) The ad-contrarian newsletter. Retrieved from: https://typeagroup.cmail20.com/t/ViewEmail/d/0A90C2CFDBF6AA132540EF23F30FEDED/88D44131D52F0C550CC2E775D3CF5869

[52] Bots, or Internet robots, are software applications that are programmed to do certain tasks. Bots are automated, which means they run according to their instructions without a human user needing to manually start them up every time. They are also known as spiders, crawlers, and web bots. While they may be utilized to perform repetitive jobs, such as indexing a search engine, they often come in the form of malware. Malicious bots are usually used to infect large numbers of computers. These computers form a "botnet," or a bot network.

[53] Boutcher. S. (2021) How could Uber cut its ad spend by $100m and see no drop in conversion. Beacon. Retrieved from https://www.thisisbeacon.com/click-fraud/uber-ad-fraud/

[54] Juniper Research (2017) Ad fraud to cost advertisers $19bn in 2018, representing 9% of total digital advertising spend. Retrieved from https://www.juniperresearch.com/press/ad-fraud-to-cost-advertisers-19-billion-in-2018

[55] Botnets are collections of computers controlled by malicious code.

Advertisers making the shocking accusation that 'advertising agencies defrauded their own customers by failing to disclose rebates they received from vendors. They also routinely act as principals in buying ad impressions and then reselling them to clients at 30 –90% markups.'[56]

Even the major platforms have been caught providing misleading metrics to boost the perceived impact of the adverts placed. Facebook and Linkedin have both recently been found to have been overstating their metrics. Facebook are facing having to pay over $40 million back to advertisers, because for over 2 years they had been using metrics based on engagement with video on the platform that were vastly overestimated.[57] Linkedin also had an issue centred on video engagement metrics. They found that a bug, which allowed video ads to play while they were off-screen on Apple's iOS devices, affected more than 418,000 advertisers over the course of more than two years and had led to advertisers overpaying.[58]

2 - Users

2.1 - BREACH OF PRIVACY & DATA RIGHTS

One of the most serious issues with tracking-based advertising is that it requires data collection and processing practices that many consider to be illegal, in contravention of the GDPR. There is potential illegality not only through companies breaking the rules of how the online advertising system operates, such as recording the bidstream data, but also those following them. In 2020, the Belgian data protection authority (DPA) 'found serious GDPR infringements in the system Google and others use to legitimise online tracking.'[59] This clearly demonstrates that allegations of illegality at the heart of tracking-based advertising are well-grounded and provides a serious catalyst for wholesale change in the tracking-based advertising industry.

The Internet Advertising Bureau's (IAB) recent report on the potential of contextual advertising demonstrates how the industry fails to understand the nature of the laws and fundamental rights that they are breaking daily. In the report, the bureau talks of the need to 'enable a balance between consumers' privacy concerns and advertisers' need for relevance and precision.'[60] As the advertising

[56] Leathern, R. (2016) The Subprime Ad Crisis is Here. Retrieved from https://medium.com/@robleathern/the-subprime-ad-crisis-is-here-6ac028133c93

[57] Patel, S. (2019) Facebook reaches proposed settlement in video measurement lawsuit. Wall Street Journal. Retrieved from https://www.wsj.com/articles/facebook-reaches-proposed-settlement-in-video-measurement-lawsuit-11570482031

[58] Sloane, G. (2020) LinkedIn discloses inflated metrics glitch that led it to overcharge 418,000 advertisers. AdAge. Retrieved from https://adage.com/article/digital/linkedin-discloses-inflated-metrics-glitch-led-it-overcharge-418000-advertisers/2294276

[59] Irish Council for Civil Liberties. (2020). GDPR watchdog's investigation finds that tracking and consent pop-ups used by Google and other major websites and apps are unlawful. Retrieved from https://www.iccl.ie/news/gdpr-watchdogs-investigation-finds-that-tracking-and-consent-pop-ups-used-by-google-and-other-major-websites-and-apps-are-unlawful/

[60] IAB Europe (2021) The IAB Europe guide to contextual advertising. p.6. Retrieved from https://iabeurope.eu/knowledge-hub/iab-europes-guide-to-contextual-advertising/

executive Bob Hoffman remarked in an interview for this report, ‘since when did the needs of advertisers trump the rights of people?’ In reality, the industry should not be seeking the right balance but instead look for ways to operate, including the provision of adverts, that is fully compliant with our existing laws and that does not infringe our basic rights.

81%
of the websites had no ‘reject’ option on the first page, but rather had hidden it on another page

73%
of the websites used ‘deceptive colours and contrasts’ to lead users into clicking ‘accept

We claim that the adtech world is operating illegally or, at the very least, at the very edge of what is legal, in three ways:

1. Data is often collected without the necessary legal justification
2. Profiles of individuals are created using data that has been collected without the necessary legal justification and/or purchased from third parties who have collected that data without the required legal justification.
3. Personal data is broadcast[61] in bid requests over the online auction networks to thousands of adtech companies, without adequate legal justification or protection.

Personal data collection across the digital economy in the EU requires an approved legal basis. Although consent is often sought through lengthy terms & conditions that almost no one reads, in fact much more data collection and processing takes place under the ‘legitimate interest’ or ‘contractual necessity’ legal bases. Although these can act as legal justifications for some forms of data collection and processing there is a growing consensus that they are not appropriate for data collection intended to be used for targeting online advertising.[62]

The means by which consent is obtained is usually via a cookie banner asking us to accept the terms of the website and sometimes giving the user more granular control. The privacy rights organisation NoYB is currently taking action against many websites because ‘most [cookie] banners do not comply with the requirements of the GDPR.’[63] In their first batch of complaints they noted that:

- 81% of the websites had no ‘reject’ option on the first page, but rather had hidden it on another page
- 73% of the websites used ‘deceptive colours and contrasts’ to lead users into clicking ‘accept’, and
- 90% of the websites provided no easy way to withdraw consent.

There is growing agreement that consent is required for the processing of data for the purposes of providing adverts. It is therefore concerning that so many websites are still failing to meet the requirements of the GDPR to obtain consent. There is also a more general concern that the kind of consent that is given online when accepting terms and conditions does not meet the GDPR’s defini-

[61] Broadcasting data means the act of sending out the personal data in the bid request to the RTB network where there is no direct intention to share the data with the other parties and indeed, they are contractually bound to not take a copy of the broadcast data.

[62] UK Information Commissioner’s Office. (2019). Update report into adtech and real-time bidding. Retrieved from: https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf

[63] noyb (2021) noyb aims to end “cookie banner terror” and issues more than 500 GDPR complaints. Retrieved from: https://noyb.eu/en/noyb-aims-end-cookie-banner-terror-and-issues-more-500-gdpr-complaints

tion. Under the GDPR consent must be:

> 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.[64]

All this data processing is done, in part, with the intention of creating detailed profiles of people and their interests so advertisers can target them. This diffusion of our digital selves across thousands of organisations, from adtech intermediaries to specialist data brokers, most of whom mean nothing to us because we never directly interact with them, makes it impossible to keep track of them. And if we cannot keep track of all our profiles, it is hard to see how we are going to exercise our GDPR rights to effective control of our data, or the right to have data erased or amended. Just as there are serious legal questions to be asked of the industrial-scale data collection that is happening, the extensive trade in our personal data that fuels the data broker and profiling industry is also on a legally dubious footing, since a legal basis for the trade is alleged to be lacking in many cases.

Another significant problem with our digital profiles is that they are often built over time through third-party cookies, which may not be placed following freely given, specific, informed consent, and are often supplemented by buying data from brokers and others, where data collection practices can be legally contentious. In addition, the boundaries of any consent that we have in fact given may be broken if our personal data is sold not just by the company that we 'consented' with, but often also by companies that bought our data.

The adtech industry is potentially exposing every person who uses the internet to the non-consensual, and often unwitting, sharing of their data with thousands of companies who are all technically able to copy, share, and sell the data on again. Although the terms and conditions of major ad exchanges only legally allow the winner of the auction to keep a record of the data in the bid request, there are few technical impediments to copying the data. Although hard data is difficult to come by, there is good anecdotal evidence that some companies participate in the RTB process solely to get access to personal data.[65]

A recent case against tiny French data broker Vectaury found that it had illegally collected over 24.7 million records of people and their geolocation and almost 43 million other pieces of personal data through the RTB process.[66,67] Because of the obvious challenge of identifying whether adtech companies are actually recording the data they receive, we believe that the case against Vectaury represents only the tip of the iceberg.

[64] GDPR art 4(11).

[65] Iwańska, K. (2020) To track or not to track: Towards privacy friendly and sustainable online advertising. Panoptykon Foundation. Retrieved from https://en.panoptykon.org/privacy-friendly-advertising

[66] Kruzer, R. (2018). Why a French ruling against a small mobile ad firm has ad tech on the defensive. Marketing Land. Retrieved from https://marketingland.com/why-a-french-ruling-against-a-small-mobile-ad-firm-has-ad-tech-on-the-defensive-252090

[67] CNIL. (2018). Court Decision n°MED-2018 042. Retrieved from https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000037594451&fastReqId=974682228&fastPos=2

The bid request during the auction process totally fails to ensure the protection of personal data against unauthorised access. In fact, it is technically impossible to safeguard information shared via RTB. As already explained, when we click on a page link, between clicking and the page loading, information about us is compiled and sent out as a bid request for advertisers to assess the value of showing us an advert. However, these requests can broadcast significant information, often more than is strictly necessary for advertising purposes, and can include very sensitive information such as sexuality, ethnicity, or political opinions. This has been labelled the 'biggest data breach in history.'[68]

2.2 - BIAS & DISCRIMINATION

The targeting infrastructure that the adtech industry has developed can be repurposed into a powerful tool for discrimination and bias. For instance, when placing job adverts, adtech tools can be used to restrict them from being seen by certain groups, like women, migrants, or people of colour. The publication ProPublica set out to demonstrate how this could work by buying 'houses for rent' adverts on Facebook.[69] They then used Facebook's own tools to request that adverts not be shown to certain categories of users, such as African Americans, mothers of high school kids, people interested in wheelchair ramps, Jews, expats from Argentina and Spanish speakers. All of these exclusions are already illegal under a particular piece of US housing law which forbids discrimination. Despite their illegality, all such adverts were approved by Facebook within minutes, raising serious questions about Facebook and the wider adtech ecosystem's compliance with anti-discrimination and anti-bias legislation.

Even though the tools that ProPublica used have now been disabled in Facebook, researchers have found that Facebook's own ad delivery algorithm may be biased. A recent study by the University of Southern California found that 'Facebook's ad-delivery system shows different job ads to women and men even though the jobs require the same qualifications.'[70] In order to test for biases, the researchers posted jobs that required identical qualifications but where their real world demographics differed, while not specifying a desired audience for the adverts. This meant that the targeting was done based on Facebook's own algorithmic assessment of how to get the best results from the advert. They found that the jobs which were female dominated in the real world were shown to more women and vice versa. Another clear example of bias, which may also be illegal in many jurisdictions.

It becomes incredibly problematic when certain characteristics such as race or location (even if these criteria are not explicitly labelled as sensitive by targeting algorithms) are used to exclude people from certain services. This is confounded by the fact that people will generally not even know that they are being discriminated against, because they don't have access to ads that they haven't seen. This means that tracking-based advertising may be *actively obscuring* discriminatory behaviour, especially when this happens due to secret algorithms, potentially undermining our fundamental human rights.

[68] Irish Council of Civil Liberties. (2020). We are litigating to end the biggest data breach in history. Retrieved from https://www.iccl.ie/adtech/

[69] ProPublica. (2017). Facebook (Still) Letting Housing Advertisers Exclude Users by Race. Retrieved from https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin

[70] Hao, K. (2021) Facebook's ad algorithms are still excluding women from seeing jobs. MIT Technology Review. Retrieved from https://www.technologyreview.com/2021/04/09/1022217/facebook-ad-algorithm-sex-discrimination/

2.3 - ATTENTION ARMS RACE

People's antipathy towards advertising in general, but tracking-based advertising in particular, has led many to seek to actively extricate themselves from the system by denying consent, using privacy protecting browsers as well as ad-blockers. This trend, when taken together with our natural ability to become accustomed to marketing techniques, enabling us to (sub)consciously ignore them, renders advertising less effective over time. Companies therefore need to constantly develop new techniques to get our attention, since we, as users, develop resistance to certain types of advertising over time. For example, the first banner ad, placed by AT&T on HotWired.com in 1994, had a 44% click-through rate, while a similar ad today would get less than 0.06%.[71] Advertisers and their marketing consultants are, therefore, in an arms race for our attention.

This means that the adtech industry is constantly evolving. Whereas initially this involved adding some basic data, like previous shopping data, to personalise the advert, today most companies are combining data they, and their adtech partners, collect through cookies[72] and existing digital profile data available from data brokers. Some more sophisticated advertising operations try to combine rich personal data profiles with contextual, real-world data about weather, relevant events, and social media data to understand when we are most susceptible to an advert.

Some trace the start of this attention arms race to the early adtech 'innovation' of pop-up ads. These ads would, as the name suggests, 'pop-up' and pretty much force the user to engage. Although this made sense for an advertiser perspective who wanted to ensure that users paid attention to their adverts, many users considered that a line had been crossed and started to develop tools and techniques to block the pop-up. These tools first appeared as separate plug-ins for browsers but quickly became a standard feature in browsers. This 'forced' websites and advertisers to partner with 'innovative' ad tech companies to develop new techniques to bypass these protections. The next steps in the arms race were for the adtech industry to start to create deep and detailed profiles about users through extensive data collection as well as trying out new ways of getting users attention including placing ads in the middle of articles and autoplaying video ads.

One of the frontlines of today's arms race is digital fingerprinting. Digital fingerprinting is a development that allows companies to track us individually without requiring our permission. It is a dangerous development in the arms race because it 'allows companies to secretly track your private online activity across many websites, apps, and your internet connected devices.'[73] Fingerprinting involves collecting information about the specific setting on a user's device, such as the brand, the operating system it is using and even the number of pixels. This is done to create a unique combination of settings that apply only to that individual: a digital fingerprint. Adtech companies can then

[71] Greenfield, R. (2014). The trailblazing, candy coloured history of the online banner ad. Fast Company. Retrieved from https://www.fastcompany.com/3037484/the-trailblazing-candy-colored-history-of-the-online-banner-ad

[72] A small text file (up to 4KB) created by a website that is stored in the user's computer either temporarily for that session only or permanently on the hard disk (persistent cookie). Cookies provide a way for the website to recognize you and keep track of your preferences.

[73] Disconnect (2020) Our New Approach to Address the Rise of Fingerprinting. Retrieved from https://blog.disconnect.me/our-new-approach-to-address-the-rise-of-fingerprinting/

use this fingerprint to track the user as they move around the internet. Even though the technique is only used by a small minority today – just 3.5% of mobile apps in 2019 – this was already double the figure in 2016, and the end of 3rd party cookies is likely to lead to accelerated growth. Thankfully technologists have already developed techniques, plug-ins and solutions to help defend us against fingerprinting. Sadly, this does not mean the end of the war, but rather the start of the next battle in the ongoing arms race.

4

CURRENT TRENDS IN ADTECH

Mozilla has recently stated that they 'don't buy into the assumption that the industry needs billions of data points about people, that are collected and shared without their understanding, to serve relevant advertising.'[74] As more people and the industry come round to this position, we are seeing the proliferation of alternative models and systems for delivering online advertising. However not all the proposals seek to solve the same problem nor achieve the same solution.

Although there are encouraging signs that solutions exist that can work for advertisers without requiring any profiling or targeting of individual users with specific Ids, that is not the same thing as saying that audience targeting is going away or indeed, if the industry is left alone, individual targeting. Even in a world where the use of personal data was completely banned, advertising could still be targeted; it would just be targeted at context rather than the individual. At the same time as many are trying to develop new privacy preserving methods, such as contextual and group targeting, a section of the adtech world is moving towards more sophisticated and direct identification that further consolidates around the idea of profiling individuals, such Unified ID 2.0. We are at a crucially important crossroads and the stakes could not be higher. Online advertising is one of the major funding models for large parts of the internet that people have grown to rely on, and so it is vital that the new model both serves their needs but also minimises the impacts described in Section 3.

In this section, we will look at three alternative models for delivering adverts that are already in existence today. The three offer different solutions to delivering online advertising that respects our privacy and data rights. Firstly, we look at the rebirth of contextual marketing that does not rely on any personal information. Secondly, we examine a new wave of browsers with a specific privacy-protecting ad channel. Thirdly, we analyse new tools that ensure that websites have the actual consent of users and that enable consensual data sharing. We will also look at the initiatives of the big tech companies seeking to protect their valuable income streams by reforming the way online advertising is delivered. We look in detail at Google's FLoC, Microsoft's Parakeet and whether Apple may be entering the online advertising area in earnest.

One thing that is important to note is that most of these current trends address only some of the issues raised in the previous section Most seek to address the targeting mechanism by trying to de-individualise it, or by adding additional data noise into the bid request or undertaking all of the data collection and processing on the browser itself. Very few of them actually address the more fundamental issue of widespread user tracking online and the dangers of mass profiling.

1 - The rise of alternatives

The online advertising industry has not remained static but is in a state of constant evolution. Even the real time auction system based on massive amounts of personal data in use today is only just over a decade old. In this section we look at those within the online and technology sectors who are actively trying to build new privacy respecting systems that will enable online advertising in the future without infringing user's rights or causing social harms.

[74] Doffman, Z. (2021) Why You Should Avoid Google Chrome's New FLoC Tracking. Forbes. Retrieved from https://www.forbes.com/sites/zakdoffman/2021/05/01/stop-using-google-chrome-on-your-iphone-android-macbook-and-pc/

1.1 – THE REBIRTH OF CONTEXTUAL ADVERTISING

Contextual is one form of online advertising that can be highly privacy preserving and has been around longer than tracking-based advertising. The basic premise of contextual advertising is to target users based on the context of the content they are engaging with rather than personal data about them. Contextual targeting already drives one of the biggest online advertising markets: search advertising. Search advertising benefits from an incredibly strong signal about what the user is interested in, i.e. the searched-for term.

The global contextual advertising market is expected to grow quickly from $106bn in 2017 to an estimated $412bn by 2025.[75] Although contextual advertising has always been an important advertising channel, the move away from third party cookies and regulatory pressures means that contextual is proving increasingly interesting to marketeers. A recent poll commissioned by **IAB Europe found that 74% of respondents thought that contextual advertising was one of the most important strategies for dealing with the upcoming loss of 3rd party cookies, more than any other strategy.[76] The CDPI found that 65% of advertisers expect to increase their contextual ad spend.[77]**

As the director of marketing for ad agency Rakuten noted in an IAB report on contextual advertising:

> ‘As an industry, we should embrace contextual advertising for all of its obvious benefits and apply our learnings from the ‘old ways.’ When we truly start putting our customers first again and are mindful about privacy, brand suitability and our messaging, we might actually get consumers to start liking advertising again (beyond just being a necessary evil to access premium content for free). This does mean that the industry will need to make some drastic changes.’[78]

Director of marketing for ad agency Rakuten

These massive numbers however mask the fact that a segment of the contextual business is nevertheless reliant on vast data collection and profiling of people. What the recent CCPA termed ‘cross-context behavioural advertising’, which means the ‘targeting of advertising to a consumer based on a profile of the consumer, including predictions derived from the consumer’s personal information, where such profile is related to the consumer’s activity over time and across time and multiple busi-

[75] Big Market Research. (2018) Global Contextual Advertising Market. Retrieved from https://www.bigmarketresearch.com/global-contextual-advertising-market-size-study-by-approach-by-type-activity-based-advertising-location-based-advertising-by-deployment-mode-mobile-devices-desktops-digital-billboards-by-industry-and-by-regional-forecasts-2018-2025-market

[76] IAB Europe. (2021) The IAB Europe guide to contextual advertising, p.9, retrieved from https://iabeurope.eu/knowledge-hub/iab-europes-guide-to-contextual-advertising/

[77] Customer Data Platform Institute. (2021) Two-Thirds of Advertisers Plan Higher Contextual Ad Spend: Connatix Survey. Retrieved from https://www.cdpinstitute.org/news/two-thirds-of-advertisers-plan-higher-contextual-ad-spend-connatix-survey/

[78] IAB Europe (2021) The IAB Europe guide to contextual advertising. Retrieved from https://iabeurope.eu/knowledge-hub/iab-europes-guide-to-contextual-advertising/

nesses or across multiple, distinctively branded websites, applications, or services.’[79]

There are however some, like Kobler and Opt Out Advertising, who do offer truly privacy preserving contextual opportunities. This is because these platforms do not seek to identify individuals at all in the process of providing adverts online. A more realistic estimate of the size of the privacy respecting contextual market may be EUR 50bn, still a sizable and important segment.[80]

Contextual Advertising, not based on any personal data, has matured significantly beyond its ability to target based on content and keywords on a page. The more sophisticated contextual platforms can now target based on text, image, audio, location[81] and semantics of content on individual pages. Across the industry three broad kinds of contextual information are emerging:

- Categories - What are the topics on the page?
- Sentiment - Is the tone negative or positive?
- Emotions - What emotions are being conveyed?

Alongside these, in order to meet the needs of advertisers, analysis is done to analyse whether the content poses any potential brand safety risks. This gives advertisers assurance that their content will not appear next to inappropriate content. Multiple advertisers have already, for instance, shifted their marketing budget away from Youtube because their adverts appeared next to problematic content.[82]

When presented with a real-world example, **consumers demonstrated their preference for contextual relevance with 4 in 5 (81%)[83] of consumers preferring the advertisement that matched the displayed content, something which personal data-based advertising often does not do.**[84] Research conducted by STER also showed that ads related to the content were less annoying and had a better recall rate and increased buying intention.[85] Contextual relevance also tips the scale so that a majority of consumers actually likes the ad vs dislikes a non-contextually placed ad.[86]

[79] Friel, A. L. & Pepper, D. (2019) Just When You Thought It Was Safe to Go Back into the Water – CCPA 2, the Sequel. Data Counsel. Retrieved from https://www.bakerdatacounsel.com/ccpa/just-when-you-thought-it-was-safe-to-go-back-into-the-water-ccpa-2-the-sequel/

[80] Kobler company presentation shared with the author.

[81] Not the location of the individual based on IP or other personal data, but more about language of the article, location of the publisher itself or locations mentioned in an article or video

[82] Statt, N. (2017) YouTube is facing a full-scale advertising boycott over hate speech. The Verge. Retrieved from https://www.ft.com/content/5fbf4a36-0fc7-11e7-a88c-50ba212dce4d

[83] Integrated Ad Science (2020) Importance of Contextual. Retrieved from: https://integralads.com/uk/insider/power-of-contextual-ads/

[84] IAB Europe (2021) The IAB Europe guide to contextual advertising, retrieved from https://iabeurope.eu/knowledge-hub/iab-europes-guide-to-contextual-advertising/

[85] Ster (2019) Online Beleving. Retrieved from https://www.ster.nl/onderzoek/whitepaper-online-beleving/

[86] Study by Kobler and WFA Norway conducted by YouGov over the period 2019-2021

The successful move by NPO, the Dutch public broadcaster, away from using personal data to serve ads and towards contextual advertisement is often highlighted as proof that other publishers could migrate to 100% contextual and not take a hit to their revenue. Although each example does show that contextual can succeed, there are also specific factors that may account for their success that may not be replicated across all publishers. Indeed, for this project we interviewed a number of publishers who were sceptical that they could replicate what NPO have achieved. Another example that is often cited is the New York Times (NYT), who stopped using third party data altogether as well as programmatic channels for their EU users. Although they did build powerful contextual targeting tools, they continued to operate a first party targeting systems at the same time.

The facts around NPO are, briefly, that their legal teams interpreted the GDPR correctly to mean that only those who provided explicit consent could be targeted with adverts based on their personal data. When NPO implemented this policy they found that only 10% of users consented, leading initially to a massive drop in revenue, as they lost 90% of their addressable advertising market.[87] This caused Ster, NPO's own ad agency, to scramble to find a way to replace the missing revenue, which they succeeded in doing in a few quarters.

They ended up building a whole new automated platform for advertisers. Just as with the tracking-based adverts, when a user visits an NPO page, a signal automatically goes out to advertisers inviting them to bid to show that user their ad. The important difference in the systems is that with Ster's platform, advertisers get information about the content that the user is looking at rather than any information about the user.

Part of Ster's innovative approach was to leverage specific metadata from NPO's programme, which were already noted to develop a much deeper understanding of the context. They then used this information to sell their ad inventory with strong evidence to present to advertisers that they can still reach the most interested and relevant audience. The results they achieved are impressive, with a 27% growth from January – September 2020, vs. 2019 despite the pandemic hitting marketing revenues very hard.[88] This was partly due to NPO's special place within the Dutch market, where it is considered an almost essential platform for anyone wanting to conduct a major advertising campaign in the Netherlands. They also built a new contextual platform, which proved popular with advertisers. As well as performing well for NPO, they also noted benefits for advertisers and users.

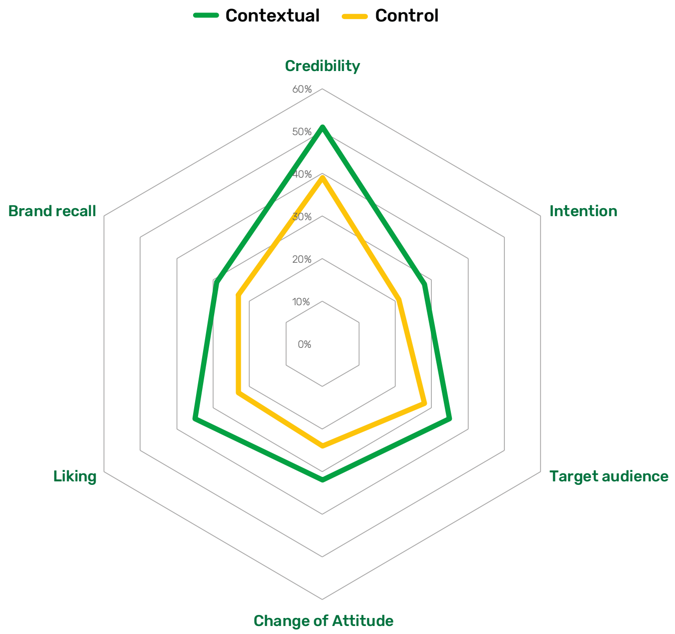
The contextual advertising platform Kobler has also noted the benefits for everyone participating in online advertising. For advertising they solve the opacity problem by providing 100% traceability with regard to revenue and placement. This transparency is essential to maximise the effect of contextual advertising by targeting the correct content. It also solves the inherently black-box nature of behavioural advertising that has led to advertisers financing ad fraud and misinformation on the internet today.

[87] AT Internet (2020) Ster – Boosting value with data-driven contextual advertising. Retrieved from https://blog.atinternet.com/en/ster-boosting-data-driven-advertising/

[88] Ibid.

In a study designed with World Federations of Advertisers in Norway, Kobler documents that ads placed contextually are up to 7.5 times more effective than tracking-based adverts due to the impact of the relevant context, as figure 6 below demonstrates.[89]

Figure 6 – Improved performance of contextual ads v tracking-based ads



Source: YouGov/Kobler company presentation shared with the author

68%
of the respondents liked the ad when it matched the displayed content, as opposed to only

47%
when it did not match the content

By simplifying the process and removing the need for personal data, you also remove the need for a data management platform, a demand-side platform, or a supply-side platform, resulting in more of the advertiser's budget reaches the publishers. Together with the full transparency of the contextual targeting, advertisers have consistently over a three-year period paid 3 times the average price for ad impressions through the Kobler platform across the +110 publisher sites in Norway and Sweden.[90] These sites include everything from the largest news sites to local and niche editorial sites.

For consumers the absence of personal data use when placing ads contextually means that data rights cannot be infringed. Contextual advertising also improves the experience for the user, as Kobler's study shows. 68% of the respondents liked the ad when it matched the displayed content, as opposed to only 47% when it did not match the content[91].

There are however some important considerations which could explain the success of NYT and NPO which means that we should be sceptical that their success can be copied by all publishers. The

[89] Kobler/WFA study where YouGov tested over 50 campaigns with over 7 000 respondents in Norway and Sweden

[90] Data provided to the author by Kobler

[91] Kobler/WFA study where YouGov tested over 50 campaigns with over 7 000 respondents in Norway and Sweden

NYT's success is at least partly due to the considerable amount of first party data they hold, since users are incentivised to login and those who do not can still be tracked, which has allowed it to continue to show adverts based on first party data. Both NYT and NPO have a very valuable brand and both would be considered an essential publisher for certain types of advertising campaigns. For NPO, given their dominant position in the Dutch online video market, they are similarly a key target of any large-scale national marketing campaign. As well as cementing their position, the switch to contextual also allowed them to grow other steams. For instance, in the open display segment, NPO was not an established publisher. Despite this, they still managed high revenue growth for display, because they were able to demonstrate the positive impact for the advertisers.

Despite these important points, the NPO case study still provides very good evidence that contextual marketing works for advertisers, since NPO found that advertisers converted more new customers using the contextual approach. They also prove that it can work for publishers themselves, because NPO has been making more ad revenue since they decided personal data should not be involved within the online advertising landscape, including contextual. NPO's model also works for users, 90% of which declined when offered the choice to trade surveillance for relevance.'[92]

Box 1 – Measuring Success in Contextual campaigns

One drawback of running ad campaigns without cookies is that it's more difficult to track users' behaviour after they've viewed content. It's therefore difficult to track the success of different campaigns. To find out more, Ster ran a 'major research project, a/b testing video and display campaigns to find out the relative success of personally targeted ads versus cookie-less ad campaigns.'[93]

The experience of NPO offers some interesting data on the potential of contextual campaigns. By asking visitors a brief question in the display slot about their relationship with the advertiser, Ster could gain information on the key brand KPIs such as familiarity, consideration, preference and behaviour. This measurement is carried out before and after campaigns and the difference between the brand KPIs after this interval indicates their effectiveness. Although this approach only works for display campaigns, they saw positive results for several advertising brands including Exterioo garden furniture, who saw an 8% increase in awareness, as well as larger brands such as DAS and Nationale Nederlanden.[94]

Ster also ran an experiment with 10 different advertisers, including American Express, to compare the performance of ads shown to users who opted in or out of being tracked. On the most important metric, conversions—the share of people who ended up taking the action the advertiser cared about, whether it was adding an item to their cart or signing up for a subscription or credit

[92] Edelman, G. (2020) Can Killing Cookies Save Journalism?. Wired. Retrieved from https://www.wired.com/story/can-killing-cookies-save-journalism/

[93] Brand Metrics (2021) How Ster used Brand Lift Measurement at Scale to Drive Revenue. Retrieved from https://www.brandmetrics.com/blog/post/bm-ster-interview

[94] AT Internet (2020) Ster – Boosting value with data-driven contextual advertising. Retrieved from https://blog.atinternet.com/en/ster-boosting-data-driven-advertising/

card—contextual ads did as well or better than microtargeted ones.[95]

When they looked at the click-through rate (the number of clicks on a banner versus the number of impressions) for these campaigns, they did not see any major differences between both routes: display campaigns which were served without cookies, generated the same volume of traffic to the website as campaigns that used cookie data. There was also no effect on the landing ratio - ratio between the number of clicks and the number of arrivals on the landing page. The bounce rate, session length & number of pages which helps advertisers understand the behaviour of users on your website after the consumer has clicked on the banner is mostly equal and, in some cases, even better without cookies. These results show that display campaigns without cookies can perform just as well in achieving the conversion objectives as those campaigns based on cookies.[96]

Johnny Ryan from the Irish Council of Civil Liberties has uncovered evidence that the NPO decision also benefited the smaller specialist publications within the group, such as Omroep MAX, an NPO publication targeted at people older than 50, growing their ad revenues by 92%.[97] This could mean that specialist publications as well as those producing quality content generating user loyalty could be the ones who find it easiest to flourish in the contextual advertising world.

As Aram Zucker-Scharff, the director of Ad engineering at the Washington Post, noted 'We're going to have a more private internet. It's either going to be through tech or regulation, or through users making choices with what they download or the extensions they use or how they interact with publishers through subscriptions or other mechanisms, I think that contextual is fundamentally the future of web advertising, and what they're doing at NPO is pretty much what every publisher's going to end up having to do.'[98]

1.2 - ON BROWSER ADVERTISING

One of the principal arenas where today's battle for our online privacy is being waged is the browser. A pivotal moment was when Apple decided to introduce Intelligent Tracking Prevention (ITP) into its Safari browser in 2017.[99] In 2019 Mozilla decided to go further and block third-party cookies by default in its Firefox browser in 2019. Apple introduced similar protections in Safari in 2020. Now most browsers have numerous features to help users take steps towards protecting their online privacy.

[95] Edelman, G. (2020) Can Killing Cookies Save Journalism?. Wired. Retrieved from https://www.wired.com/story/can-killing-cookies-save-journalism/

[96] Ster (2020) A Future without advertising cookies. Retrieved from: https://www.ster.nl/media/h5ehvtx3/ster_a-future-without-advertising-cookies.pdf

[97] Edelman, G. (2020) Can Killing Cookies Save Journalism?. Wired. Retrieved from https://www.wired.com/story/can-killing-cookies-save-journalism/

[98] Ibid.

[99] CJ (2018) What You Need to Know about Apple Intelligent Tracking Prevention, CJ Junction. Retrieved from: https://junction.cj.com/article/what-you-need-know-about-apple-intelligent-tracking-prevention-itp

A few of these browsers are seeking to radically change the advertising model by putting the browser at the centre of delivering adverts in ways that protect our privacy and ensure our consent. We will examine only one model in detail, operated in the Brave browser, although there are many other options, such as Gener8 or Vivaldi.

The Brave browser ensures that no personal data ever leaves the device, with the basic profiling and ad selection done by the browser. Brave offers users the chance to earn part of the advertising revenue in a cryptocurrency token called the Basic Attention Token (BAT). We will first look at the ad delivery models in isolation before considering the wider issues with browsers getting into the ad delivery business.

Although the Brave browser was launched in 2016, Brave Ads - their new way of doing adverts online - only started in April 2019. Brave currently has over 34 million monthly active users[100], which is a lot of people but still only gets them a tiny market share.

Brave's model eliminates all ad trackers, something many browsers do today, and strips every site of every ad, something fewer do, but where Brave becomes unusual is that it also adds in its own adverts. Brave's adverts are not individually targeted but instead aimed at aggregate interest groups of the browser's user base, with the browser making the final choice of what advert to show the user. The revenue from advertisers is split between the user and Brave, taking 70% and 30% respectively. While users can convert their BAT into other cryptocurrencies Brave has 'not encouraged or facilitated this exchange trading in any way.'[101] Users are, in fact, encouraged to transfer their BAT to publishers. In February 2021, Brave claimed that 26m BAT, valued at $18.8m[102], had been transferred to their registered creator network, which now numbers over one million websites, social media influencers and other online creators.[103]

Brave still wants to show ads targeted at a specific user, but it lets the browser decide on the final targeting. It does this without ever transmitting your data over the network to publishers, advertisers or even Brave itself. The browser builds a limited profile of you based on the websites you visit and terms you search for.[104] At regular intervals the browser receives a number of adverts, which have all been labelled with target categories, and the browser decides which of them best matches your interests. Advertisers know only that their ads were seen, not who saw them.

Brave, and the others like Gener8, have taken on the serious challenge of creating new ways to make advertising privacy preserving and consensual. Together with sharing the advertising revenue, they hope to create an environment where people actually engage more. Brave, for instance, is programmed to show the adverts during moments where it thinks an interruption in attention will cause less annoyance.

[100] Brave (n.d.). Retrieved from: https://brave.com/transparency/

[101] Basic Attention Token (n.d.). Retrieved from: https://basicattentiontoken.org/faq/

[102] Based on BAT valuation of $0.7 correct as of Aug 10th, see: https://coinmarketcap.com/currencies/basic-attention-token/

[103] See: https://basicattentiontoken.org/

[104] Brave (2020) An Introduction to Brave's In-Browser Ads. Retrieved from: https://brave.com/intro-to-brave-ads/

Whereas they take a lot of care to ensure the consent of their users they do not accord publishers and website owners the same opportunity. All websites are automatically stripped of all their adverts irrespective of the wishes of the publishers. This prevents the website owner from monetising the content that they have produced. Gener8 places the adverts directly on the publisher webpages, whereas Brave displays them on a separate tab. This means they are stepping into the advertising money stream, while at the same time cutting out publishers.

The model has been challenged by some as free riding, because they use publisher content in order to show their adverts. Publishers only get a chance to be renumerated for their content if they are officially registered and users visit their sites or choose to donate their BAT to them. Gener8, on the other hand, only offer the user the opportunity to turn the ad blocking off for sites they want to actively support.

Brave is currently in Beta testing of a publisher ad service, where it would place ads directly on publisher websites. Under this arrangement publishers will keep 70%, while the user and Brave will evenly split the remaining 30%.[105] The 70% is significantly more than a publisher can expect to get using the RTB system. If Brave is able to build a good advertising platform for publishers and are able to significantly grow their user base then they could 'pose a credible disruption threat to the massive digital advertising industry.'[106]

1.3 - AUTOMATED PRIVACY SIGNALS

While some are working to completely end advertising based on personal data, others are trying to make it easier for those who want to opt out of the system whilst leaving alone those who want to be targeted by tracking-based adverts. The idea is that instead of having to choose your privacy settings every time you visit a new site or use a new app, you could set your preferences once, on your phone or in a browser extension, and be done with it.

Veterans of the privacy battle will remember the emergence of the 'do not track' (DNT) initiative in 2009, which emerged just as tracking-based adverts and real time bidding were being developed. DNT was a proposed HTTP header field, designed to allow internet users to opt-out of tracking by websites. The idea behind this particular 'failed experiment'[107] was that users should be able to set default privacy preferences which could be automatically communicated via browsers to website publishers, thereby removing the obligation to accept, decline or manage your settings for every page.

All browsers implemented the DNT signal in 2011-12 and it was widely adopted by users. A 2018 report by Forrester found that about 25% of US users still used the feature in an attempt to protect their privacy. However, the system failed to convince website owners and publishers to respect the

[105] Shankland, S. (2019) Brave's privacy-first browser ads arrive with promised payout for you. Cnet. Retrieved from https://www.cnet.com/tech/services-and-software/braves-privacy-first-browser-ads-arrive-with-promised-payout-for-you/

[106] Solarin-grasshopper (2021) Brave Browser: Disrupting Digital Advertising (An Investment Memo). Retrieved from https://solarian1.medium.com/basic-attention-token-investment-memo-43e86e20e7af

[107] Hill, K. (2018) 'Do Not Track,', the Privacy Tool Used by Millions of People, Doesn't Do Anything. Gizmodo. Retrieved from https://gizmodo.com/do-not-track-the-privacy-tool-used-by-millions-of-peop-1828868324

signal. The incoherent reaction to DNT can be seen in Google's integration of it into Chrome, while at the same time declining to honour the signal on its web pages. Ultimately the refusal of governments around the world to step in and give it any kind of legal authority meant this was always doomed to fail.

Just as DNT was being wound down, from its ashes have emerged a number of alternatives such as Global Privacy Control[108] (GPC) and Advanced Data Protection Control[109] (ADPC). These initiatives are seeking to learn from the failures of DNT to create viable solutions that will be respected by website owners and publishers as well as be enforceable by regulators.

The most advanced, in terms if implementation, of these new systems is GPC. They have already got backing from the likes of The New York Times; The Washington Post; Financial Times; WordPress-owner Automattic; dev community Glitch; privacy search engine DuckDuckGo; anti-tracking browser Brave; Firefox maker Mozilla; Digital Content Next; and digital rights group the Electronic Frontier Foundation. GPC was designed with the Californian Consumer Privacy Act (CCPA) in mind, which created the opportunity for Californians to opt out of having their data sold on. The idea was to create a tool that would qualify as a universal opt-out under the CCPA thereby ensuring that exercising your privacy right flipped 'from being hopelessly complex to extremely easy.'[110]

By getting major publishers on board GPC has in some ways already achieved more than DNT. The initiative received a massive boost when California's attorney general tweeted in support saying that 'This proposed standard is a first step towards a meaningful global privacy control that will make it simple and easy for consumers to exercise their privacy rights online.'[111]

Whereas the GPC is currently designed to send a single signal to websites to stop them from being able to sell the user's data the ADPC is seeking to provide users with more granular control on the data privacy, reflecting the more complex legislative framework we have in the EU. Although at an earlier stage than the GPC, the ADPC allows users to:

- Remember a variety of different settings to enable users to differentiate their privacy settings across different websites
- Send opt-in (consent) and opt-out (objection) signals
- Send general signals (like 'reject all') specific signals (like consent to a specific request) and a combination of general and specific signals (like "reject all, but consent to requests 'x' and 'y'")
- Predetermine settings and logic that will determine how requests are treated, such as white- and blacklisting.
- Protect against fingerprinting by not sending any signal if a domain does not support

[108] See: https://globalprivacycontrol.org/

[109] See: https://www.dataprotectioncontrol.org/

[110] Edelamn, G. (2020) 'Do Not Track' is back, and This Time It Might Work. Wired. Retrieved from https://www.wired.com/story/global-privacy-control-launches-do-not-track-is-back/

[111] See: https://twitter.com/AGBecerra/status/1313884769478828032?ref_src=twsrc%5Etfw

ADPC[112]

They have created a white-list functionality to enable users to treat websites they trust to manage their data carefully or that they want to explicitly support differently. The ADPC site specifically highlights that 'many users are probably willing to share more data with quality media, but don't want to give their data to hundreds of external tracking companies. With ADPC, for example, a newspaper association can advertise a whitelist with which certain data can be automatically processed by quality media. The user can thus support certain groups with one click.'[113] As privacy activist Max Shrems has noted, 'ADPC allows intelligent management of privacy requests. A user could say, for example, 'please ask me only after I've been to the site several times' or 'ask me again after 3 months.'[114]

What GPC and ADPC demonstrate is that there are technical solutions already developed that allows users to take effective control of their online data and communicate their preferences around data collection, sale and advertising easily. If implemented more widely, and if publishers and advertisers respected user-defined preferences, these tools would enable those who wanted to easily exclude themselves from tracking-based advertising. The massive potential impact of these tools is also why there has been so little voluntary adoption from publishers. For them to be transformative they will need legislative backing, the first signs of which we are starting to see in California.[115]

2 - Adtech's proposed futures

It is easy to get lost in all the proposals that companies involved in the online advertising sector are putting out. The various proposals, most of which have bird related names, such as Turtledove, Fledge, Unified ID 2.0, PIGIN, FLoC and Parakeet seek to reduce the personal data that is exposed through the provision of adverts online. None of the proposals seek to move away for massive data collection and profiling of individuals.

Many of the proposals are currently being proposed and debated publicly, with specifications published in Github. A multi-stakeholder working group is in the process of being set up in the W3C to discuss the various proposals so that they can be properly debated, and the proposals improved and optimised.

We do not have the space or capacity to review all of the proposals on the table at the moment. In this section, we explore Unified ID 2.0, FLoC and Parakeet in some detail. It is important to note that whereas Parakeet aims to be a comprehensive system, including vital features such as retargeting and

[112] See: https://www.dataprotectioncontrol.org/about/

[113] noyb (2021) New browser signal could make cookie banners obsolete. Retrieved from https://noyb.eu/en/new-browser-signal-could-make-cookie-banners-obsolete

[114] Ibid.

[115] Abernethy, S. & Ramos, G. A. (2021) Global Privacy Control Endoresed by California AG – Next Steps. GreenbergTraurig. Retrieved from https://www.gtlaw.com/en/insights/2021/2/global-privacy-control-endorsed-by-california-ag-next-steps

attribution, FLoC is deliberately only providing a solution for interest-based targeting. In addition, many of the elements of the various proposals are shared, however we will not assess each feature for each proposal. We will also outline why Apple may be an outsider to watch in this area.

2.1 - GOOGLE'S FLOC

The most talked about project in the adtech world in Google's Federated Learning of Cohorts, or FLoC as it is commonly known. [116] The stated purpose of developing FLoC is to give advertisers a way of targeting ads without exposing the personal details of individual users. It does this by grouping people with similar interests together in 'cohorts' which will be generated by an algorithm that Google has created. The algorithm then monitors and records all of the websites that you visit.

In version 89 of Chrome, released in early 2021 Google started to test the technology in the field. This involved millions of users being co-opted into the trial, without their opt-in consent. Given the way that they are testing the technology it is not surprising that they did not include any EU users in the trial. It is highly unlikely that such an opt-out consent system could comply with GDPR.

Although many agree that FLoC is probably more privacy preserving than third party cookies were, that is the wrong comparison, especially since many browsers, such as Safari, Brave or Firefox, have already eliminated third party cookies. Many acknowledge that FLoC is 'complicated and has some potential privacy implications of its own,' and that it 'does appear to keep you semi-anonymous, but there are enough details to hide dozens of devils.'[117] The biggest critics go further claiming that 'FLoC was dreamed up by math bros at Google who wanted to try and break consent on the internet just one more time' as Zach Edwards, co-founder of web analytics firm Victory Medium noted.[118]

Box 2: How FLoC works (as best we know)[119]

Don Marti from Café Media, which represents publishers selling their digital advertising, has used the FLoC to understand how the audiences of the 3000+ sites which Café Media represents are distributed into FLoCs. Below is an attempt to simplify the process as well as update with the latest understanding:[120]

1. If you browse the web with Chrome, it logs all the pages you visit.

2. The new FLoC Javascript code analyses the domain names (not individual pages) and turns that

[116] Slightly ironically Michael Kleber, the person from Google behind the proposal, regrets the name choice because as currently formulated the design includes neither federation nor learning

[117] Bohn, D. (2021) Nobody is flying to join Google's FLoC. The Verge. Retrieved from https://www.theverge.com/2021/4/16/22387492/google-floc-ad-tech-privacy-browsers-brave-vivaldi-edge-mozilla-chrome-safari

[118] Claburn, T. (2021) Google's FLoC flied into headwinds as internet ad industry braces for instability. The Register. Retrieved from https://www.theregister.com/2021/04/17/google_floc_adoption/

[119] More detailed version available from - https://cafemedia.com/early-status-of-the-floc-origin-trials/

[120] Marti, D. (2021) Early Status of FLoC origin trials. Retrieved from https://cafemedia.com/early-status-of-the-floc-origin-trials/

history into a super long number/symbol sequence called a “SimHash”

3. Once a week, the browser-based FLoC software contacts a Google server, sends it the unique SimHash and the Google server compares it to millions of other SimHashes it has received across the web.

4. Then the raw SimHash results will be counted. Then, the system learns which cohorts are large enough and therefore “safe” and publishes a map of the space that marks out safe and unsafe identifiers based on things like size and sensitivity. Then, browsers will get that map and generate identifiers from the ‘safe’ zones in that map

5. Now, when an advertising network seeks to place an ad in front of that browser’s user, it requests from the browser its latest cohort group ID, deciding if the user of the browser is an attractive-enough target to bid on the ad position.

At the same time as Google tries to claim that it is protecting users’ privacy it also has to convince advertisers that the system is as effective as the third-party cookies that preceded them. In this vein, they have found that the FLoC system is ‘still 95% as effective at getting users to click on ads’ as the previous model.[121] Some in the industry have welcomed Google’s intervention declaring that they are ‘not surprised in the least that cohorts can perform roughly as well as user-level or 1:1 cookie-based approaches. The idea that 1:1 was the holy grail of digital advertising was always a fallacy. It’s great to see Google blowing up that myth.’[122] Balancing the optimism of moving beyond 1:1 targeting, we find a lot of scepticism about FLoC’s effectiveness: ‘the industry needs a lot more research on the relative effectiveness of cohort-based versus user-level approaches to targeting.’[123] It is safe to say that the jury is still out on this point.

One thing we know about the design of the system is that FLoC cohorts will be re-calculated on a weekly basis, each time using data from the previous week’s browsing. This may ensure, if your browsing habits change over time, that your FLoC cohort is less useful as a long-term identifier, but it also makes them more potent measures of how users behave over time.

The description of the system by the EFF’s Bennet Cypher paints an illustrative and evocative picture of how FLoC will change our online interactions:

[121] The Economist (2021) Why is FLoC, Google’s new ad technology, taking flak?. Retrieved from https://www.economist.com/the-economist-explains/2021/05/17/why-is-floc-googles-new-ad-technology-taking-flak

[122] Schiff, A. (2021) The Industry Reacts to Google’s Bold Claim that FLoCs are 95% as Effective As Cookies. Ad Exchanger. Retrieved from: https://www.adexchanger.com/online-advertising/the-industry-reacts-to-googles-bold-claim-that-flocs-are-95-as-effective-as-cookies/

[123] Ibid.

> 'Each user's behaviour follows them from site to site as a label, inscrutable at a glance but rich with meaning to those in the know. Their recent history, distilled into a few bits, is "democratized" and shared with dozens of nameless actors that take part in the service of each web page. Users begin every interaction with a confession: here's what I've been up to this week, please treat me accordingly.'[124]
>
> **EFF's Bennet Cypher**

We will now explore the four most common issues that researchers have raised with the FLoC proposal:

- Helps with identification
- Creates additional data
- Could assign users to sensitive category assignment
- Worsen competition

The first issue is that it potentially allows for additional mechanisms to help identify individuals online. This is because it would provide an additional data point that could help those engaged in fingerprinting. Fingerprinting is the practice of gathering multiple pieces of information from a user's browser, such as version, screen size and language, to create a unique identifier for that browser. Google has already promised to ensure that the cohorts will be in the thousands, but this is already a massive help to fingerprinters who now only have to distinguish your browser from a few thousand others (rather than a many millions).

The adtech industry is already planning to integrate the new data into profiling, as a recent quote from the CEO of identity tech firm ID5 attests, 'The more signals we have, the more accurate we are, and FLoC IDs will be among signals we use.'[125]

There are others within the adtech industry who think that FLoC may be able to be used as a new persistent identifier, in the way that IP addresses do today. Like IP addresses, FLoC IDs will not be entirely static, but it is likely that for most users? A specific set of FLoCs will be associated with one person. It has also been noted by the adtech industry that 'If your behaviour doesn't change, the algorithm will keep assigning you in that same cohort, so some users will have a persistent FLoC ID associated with them — or could."[126]

The second problem is that the FLoC ids effectively act as additional data about individual users that can be added to profiles for those companies who already have an identifying piece of information about the user – for instance because the site requires a log in. The EFF has highlighted two different ways in which the FLoC ID could be problematic. Firstly, it does provide detailed information,

[124] Cyphers, B. (2021) Google's FLoC Is a Terrible Idea. Electronic Frontier Foundation. Retrieved from https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea

[125] Kaye, K. (2021) As ad tech firms test ways to connect Google's FLoC to other data, privacy watchers see fears coming true. Retrieved from https://digiday.com/marketing/as-ad-tech-firms-test-ways-to-connect-googles-floc-to-other-data-privacy-watchers-see-fears-coming-true/

[126] Ibid.

albeit in encoded form, about an individual's recent browsing history. People may be able to reverse engineer the cohort algorithm to identify with varying degrees of certainty the exact sites visited. Secondly, it may expose other information about an individual. Advertisers could learn over time that people in specific cohorts tend to have specific characteristics. 'For example, a particular cohort may over-represent users who are young, female, and Black; another cohort, middle-aged Republican voters; a third, LGBTQ+ youth.'[127]

A third identified issue is the problem of people being automatically assigned to sensitive or problematic categories, since, according to the specifications, this activity will be done purely algorithmically. This will mean that if Google is to follow through on its commitment to ensure that this does not happen, they will need to be constantly monitoring and analysing people's personal data and the cohorts they are put into.[128] Whenever their analysis reveals a cohort that falls into the sensitive or problematic category, they will need to adjust the algorithm and hope that the adjusted version does not do the same.

Finally, FLoC has also been accused of being anti-competitive. The European Commission[129] and the UK's Competition and Market Authority[130] are both conducting investigations in various aspects of Google's FLoC plans. The core of the issue is that Google is simultaneously removing third-party cookies, which prevents other companies collecting data from google sites, while at the same time collecting most Chrome users' data on everyone else's websites. FLoC then creates additional issues because it would make companies that use it reliant on semi-anonymised data to identify people, beyond the first party data they could collect.

Due to overwhelming pressure and criticism from so many corners, Google have at least decided to push back the timeline when they expect FLoC to be operational to Q3 2022.[131] We expect the company to release an updated technical proposal for FLoC v.2 in the coming months. This has also led Google to delay their phasing out of 3rd party cookies at the same time. This gives them the chance to process 'private and public feedback Google received from multiple sources.'[132]

The list of companies coming out to ban FLoC is considerable and range from major platforms like

[127] Cyphers, B. (2021) Google's FLoC Is a Terrible Idea. Electronic Frontier Foundation. Retrieved from https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea

[128] Munoz Medina, A., Kleber, M., Karlin, J. & Vale, M. (2021) Measuring Sensitivity of Cohorts-Generated by the FLoC API. Retrieved from https://docs.google.com/a/google.com/viewer?a=v&pid=sites&srcid=Y2hyb21pdW0ub3JnfGRldnxneDo1Mzg4MjYzOWI2MzU2NDgw

[129] EU Commission (2021) Answer given by Executive Vice-President Vestager on behalf of the European Commission. Retrieved from https://www.europarl.europa.eu/doceo/document/E-9-2021-000274-ASW_EN.pdf

[130] Competition and Market Authority (20201) Investigation into Google's 'Privacy Sandbox' browser changes. Retrieved from https://www.gov.uk/cma-cases/investigation-into-googles-privacy-sandbox-browser-changes

[131] Privacy Sandbox (2021) The Privacy Sandbox Timeline. Retrieved from https://privacysandbox.com/timeline

[132] Perrigo, M. (2021) Google is doing a double-take on its FLoC timeline and will split rollout into two phases. Retrieved from https://chromeunboxed.com/chrome-updated-floc-timeline

Amazon[133] or Microsoft[134], to browsers like Brave or Vivaldi, as have other privacy first companies like DuckDuckGo. Of all the moves against the technology, it is only Amazon's which will be of serious concern to Google, since it may cut them off from being able to access the valuable shopping data that Amazon provides. As well as being concerned about whether FLoC can deliver technically, many publishers are also afraid that it will disadvantage their market position because Google will still be able to see and have access to the personal data of the users, unlike the publishers who will only have the cohort data to work with.

2.2 - MICROSOFT'S PARAKEET

One other interesting proposal that was spoken about positively by a number of publishers interviewed for this report, is the Parakeet proposal from Microsoft. Parakeet stands for Private and Anonymized Requests for Ads that Keep Efficacy and Enhance Transparency. Its aim is to operationalise the concept of differentiated privacy, which has been an exciting area of research since first proposed in 2006,[135] and in this context can be thought of as a way of sharing data without revealing any personal identities.

It uses a 'trusted server' that stands between the user and the advertising networks. Within this 'trusted server' every user would be individually identifiable with a unique ID, but this would never be transmitted. When a user clicks on a webpage with adverts the requests are routed through the server. Before the data is sent the server adds some 'noise' into the data, which can involve anonymising the IP address, or adding random data into different requests from the same user, or reducing the granularity or specificity of interest category. Rather than the noise being added to individual's data, which would be inefficient, the noise would be added once data had already been aggregated. This means that much less noise, than if done individually, needs to be added to retain individual anonymity. The data is then sent, with the noise, to the ad network which bids for the attention in the usual way.

Rather than the opaque FLoC IDs which we would be automatically assigned to and have little or no agency over, in Microsoft's proposal users will have access to view what cohorts they have been assigned to. Users will also be able to opt-out of being assigned to a particular cohort and control the ones they elect to participate in.[136]

[133] Kaye, K (2021) Amazon is blocking Google's FLoC — and that could seriously weaken the fledgling tracking system. Digiday. Retrieved from https://digiday.com/media/amazon-is-blocking-googles-floc-and-that-could-seriously-weaken-the-fledgling-tracking-system/

[134] The Economist (2021) Why is FLoC, Google's new ad technology, taking flak?. Retrieved from https://www.economist.com/the-economist-explains/2021/05/17/why-is-floc-googles-new-ad-technology-taking-flak

[135] Dwork, C., McSherry, F., Nissim, K. & Smith A. (2006) Calibrating Noise to Sensitivity in Private Data Analysis. In: Halevi S., Rabin T. (eds) Theory of Cryptography. TCC 2006. Lecture Notes in Computer Science, vol 3876. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11681878_14

[136] Sullivan, L. (2021) Microsoft Announces Parakeet For Privacy Controls, Bing API For Private Search. Retrieved from https://www.mediapost.com/publications/article/362530/microsoft-announces-parakeet-for-privacy-controls.html

Because we engage with the online world so much, even with the noise added, it is inevitable that over time individual users would start to be discernible in the data. Parakeet's proposal to fix this is to add a further module to the system that records privacy lost and ensures that no user exposes themselves beyond a defined level, to the extent of potentially no longer sending any accurate personal data with ad requests.

Where Parakeet again diverges from practice today is that they want to continue to mediate and protect the user after they interact with any of the adverts shown. They propose that if the user interacts with any of the adverts this connection is also routed through the 'privacy module', so that it can monitor and prevent data from being transferred from the user to the advertiser or publisher.

A further service that the 'trusted server' could provide, according to the proposal, is to report back to advertisers. At the most basic level, this would involve aggregate reporting on the activity, but if additional information was fed in from various parts of the advertising ecosystem, it could provide better attribution reporting, which allows advertisers to better understand the effectiveness of their campaign.

Microsoft expects that the trusted server operator, which according to the proposal would be Microsoft itself, would be paid for the functions that it carries out.

As with FLoC, Parakeet offers us a vision of how online advertising can work that is a great improvement on the model that currently dominates. However, as section 3 on the impacts of this business practice illustrated in detail, the current model is so problematic that the bar was already low when it came to privacy protection.

The technical specification so far highlights two specific areas of concern that will need to be addressed. Firstly, the inherent tension between maintaining anonymity for users, especially over the long term, and the needs of advertisers for accurate information with which to target individuals. Secondly, it gives a huge amount of power to the organisation that operates and owns the trusted server.

Getting the level of anonymisation and the level of the noise right demonstrate the challenges that remain for Parakeet to balance the competing interests of users, who want a system that obscures their identity and anonymises their data, while at the same time advertisers want to know as much relevant accurate information as possible in order to feel confident bidding. Although companies like Mozilla and others are working on mathematical ways of determining what an objective balance could be, an expert that we spoke to said that the 'evidence does not currently look good.'[137]

Microsoft's integration of differential privacy into Parakeet means that there is also a need to bound overall privacy loss over time. This leads to a requirement to set a limit or overall budget and ensure that it is not exceeded. The metric (often referred to as epsilon) that the budget uses is an estimate of the worst-case information leakage. If you measure the privacy loss on each query, you can add

[137] Interview with senior engineer actively working on these proposals.

up all the losses to ensure that you keep within your allocated budget. A well designed and operated differential private system can therefore provide strong guarantees of privacy.

The proposal in Parakeet is different to the privacy budget contained in the FLoC proposal, which uses a similar logic but it is not based on the firm mathematical grounding that differential privacy is. There is doubt that a system like FLoC could ensure that it never revealed enough data about to user to identify them. This had led the CTO of Mozilla recently noted that 'the privacy budget is more aspirational than a concrete proposal.'[138] Beyond this there is also concern from browser operators and website owners that the implementation of a privacy budget could disable important functionality. Finally, as Pete Snyder from Brave noted, implementing a privacy budget could reveal something unique about the particular user: 'the way you spend your budget is in itself a unique identifier, which is ironic three times over.'[139]

Trusting the 'trusted server' when it is owned and operated by one company is always going to be difficult for users, publishers and advertisers. For some a trusted server is always going to be a sub-optimal idea that will require many layers of safeguards, both technical and policy, to create the right environment. Some also worry that the hugely valuable data contained in the trusted server creates a huge incentive to attack it in order to access the stored data. This raises questions about whether the trusted server is the right way to proceed, with some in the community investigating whether multi-party computation, which allows multiple systems to work together to complete a function without needing to trust any of the parties, might be a better answer.

Others are working to make the trusted server model work by creating an 'overall vision and governance model able to support such trustworthy utility servers by having them owned and operated by an entity governed in common by different constituencies.'[140] This idea continues the thematic of bird names, being called 'Garuda' which means 'king of birds.' Were Garuda to create the positive ownership and governance structure that it lays out in its specifications then it would help to mitigate the problems raised here, since it would have a diverse range of stakeholders to manage the delicate balance between the anonymity of users and usable data for advertisers as well as helping to ensure that there was some transparency and control of the organisation that operates the 'trusted server.'

Although popular with certain sections of the online advertising community, Parakeet will still struggle to be adopted as the industry standard because Microsoft is not one of the major players in online advertising today (although their search engine Bing does generate some advertising revenue). They are therefore not in a powerful position to dictate technological adoption in an adjacent

[138] Kate, K (2021) Google's vague privacy cure-all is showing up in new proposals, but some say it could break the internet. Digiday. Retrieved from https://digiday.com/marketing/googles-vague-privacy-cure-all-is-showing-up-in-new-proposals-but-some-say-it-could-break-the-internet/

[139] Kate, K (2021) Google's vague privacy cure-all is showing up in new proposals, but some say it could break the internet. Digiday. Retrieved from https://digiday.com/marketing/googles-vague-privacy-cure-all-is-showing-up-in-new-proposals-but-some-say-it-could-break-the-internet/

[140] GARUDA (2021) Governance of Ad Requests by a Union of Diverse Actors (GARUDA). Retrieved from https://darobin.github.io/garuda/

segment of the online advertising sector, i.e. open display advertising. Microsoft will be relying on this proposal being adopted in forums like W3C which is in the process of creating the appropriate forum to try and build a consensus around the way forward.

2.3 - UNIFIED ID 2.0

Unified ID 2.0 is different from FLoC and Parakeet because it does not try to move beyond individual tracking but rather tries to improve online advertising by using pseudonymisation coupled with a reliance on industry self-regulation through a code of conduct to govern the system. This, they hope, creates a technology that can still track individuals around the internet which is not blocked by current anti-tracking mechanisms. Many of the biggest adtech companies have already signed up to be part of the network including Criteo, Index Exchange, Magnite, PubMatic, OpenX, SpotX, LiveRamp and Neustar, along with publishers like the Washington Post and Nielsen, the gold standard in media measurement.[141]

The proposal, which was first announced in summer 2020, has undergone significant change and is now being handled by the IAB Tech Lab and its Partnership for Responsible Addressable Media (PRAM) initiative. Unified IS 2.0 is currently in active use.

Unified ID 2.0 is still based on the requirement that companies receive the consent of the user to collect the data and be tracked individually. When a user first visits a site that is part of the Unified ID 2.0 network they will be asked to provide their consent. An additional step will see the sites request the user's email address which will be the basis of the identifier. To offer some privacy protection, the e-mail address is pseudonymised into a unique long-term identifier via cryptographic processes called 'salting' and 'hashing.' This pseudonymised alphanumeric string (UID2) then becomes the new identifier.

When a website wants to serve an advert to a user, it uses the same cryptographic tools to covert the e-mail to an encrypted token (also an alphanumeric string) which contains the UID2. The token is then broadcast over the auction networks to potential advertisers as part of the bid request. Advertisers who have signed up to the part of the Unified ID 2.0 system will be proactively sent decryption keys which will allow them to read the UID2. This decrypted UID2 can then be used to track the user and serve them an advert just as in the current system.

Proponents of the system view it as an 'upgrade and an alternative to third-party cookies'[142] because it offers:[143]

[141] The Trade Desk (2021) What the Tech is Unified ID 2.0?. Retrieved from https://www.thetradedesk.com/us/knowledge-center/what-the-tech-is-unified-id-2-0

[142] The Trade Desk (2021) The Trade Desk Adds Nielsen To Unified ID 2.0 Initiative as Advertisers Seek Upgrade to Cookies. Retrieved from https://www.thetradedesk.com/us/about-us/newsroom/the-trade-desk-adds-nielsen-to-unified-id-2-0-initiative-as-advertisers-seek-upgrade-to-cookies

[143] The Trade Desk (2021) The Trade Desk Adds Nielsen To Unified ID 2.0 Initiative as Advertisers Seek Upgrade to Cookies. Retrieved from https://www.thetradedesk.com/us/about-us/newsroom/the-trade-desk-adds-nielsen-to-unified-id-2-0-initiative-as-advertisers-seek-upgrade-to-cookies

- Encrypted identification
- Simple, transparent and effective user controls
- Single sign-on capabilities across the open internet
- A simplified consent mechanism

For advertisers it also offers the chance to track people rather than devices, as cookies used to do. The 'unified' element of the proposal signifies that advertisers will be able to link the user through the various devices and apps as well as connected TVs and connected vehicles.

One of the challenges for operating this system will be the consent management that will be required. Recent data from Apple's implementation of AppTrackingTransparency currently shows that only 21% of users are willing to consent to their data being collected for the purpose of advertising. Unified ID 2.0's reliance on this form of consent would seem to be severely limiting the number of users who can be served adverts by the system. Websites will need to regularly check that the users visiting their sites have not opted out centrally, even when they have already consented at the webpage, since consent may be removed at any time. The Unified ID 2.0 network has already developed a centralised tool for those who want to opt out of the system completely - https://transparentadvertising.org/. A process will have to be implemented to resolve conflicting consent signals for the same user from different webpages in the Unified ID 2.0.

In order to enhance the experience of the user and simplify the job of publishers in the network, Unified ID 2.0 proposes to allow for single sign on across the network. Although potentially a positive move because it streamlines the need to provide consent it is unclear whether this will be GDPR compliant.[144] If the single sign on cannot be implemented due to compliance concerns, especially if the provided e-mail address needs to be validated, this will lead to significant friction for someone visiting a new publisher site to read a quick article and could result in users leaving the page before completing the consent form.

only

21%

of users are willing to consent to their data being collected for the purpose of advertising.

There is an easily identifiable issue with the decryption methodology because the keys will need to be communicated to everyone in the network for it to work. This raises two issues. Firstly, that any organisation within the network may decide to break the code of conduct that they signed up to and share the decryption keys outside the network. As experts from Mozilla noted 'this presents a major privacy risk which seems hard to ameliorate, as there is no straightforward mechanism for tracking down the leaking consumer.'[145] Secondly, there is nothing technically 'preventing an attacker from minting their own tokens'[146] because the only validation for the validity of a token is the decryption key, which, as previously noted, are widely distributed and may be easily leaked.

[144] Adelphic (2021) What's Facing a Bigger Challenge Than iOS 14.5? Unified ID 2.0. Retrieved from https://www.adelphic.com/blog/whats-facing-a-bigger-challenge-than-ios-14-5-unified-id-2-0/

[145] Thomson, M. & Rescorla, E. (2021) Comments on SWAN and Unified ID 2.0. Retrieved from https://mozilla.github.io/ppa-docs/swan_uid2_report.pdf

[146] Thomson, M. & Rescorla, E. (2021) Comments on SWAN and Unified ID 2.0. Retrieved from https://mozilla.github.io/ppa-docs/swan_uid2_report.pdf

Unified ID 2.0 requires that users trust all of the organisations that are part of the wider Unified ID network. This is because there are very few technical limitations on using the data beyond the intentions of the system.

Although the whole proposal rests on the industry self-regulating itself, administer by a newly formed and independent organisation set up to enforce a code of conduct that has not been published yet. This is extremely disappointing and means that it is impossible to understand at present whether the system will be well governed. Without being able to analyse the content of the code it is impossible to understand how the behaviour of the large number of companies in the Unified ID 2.0 network will be constrained, how their performance and actions will be audited and what consequences will flow from breaking the code. It has also been noted that Unified ID 2.0 'depend so heavily on policy controls' while 'no technical controls ensure that they in fact conform to those policies.'[147] Since bad behaviour, like sharing the decryption key, would have very serious consequences for the network, it is disappointing that there no documented ways to automatically detect and deal with it.

Unified ID 2.0 also has an issue with measurement because for data to flow they need to get the consent of both publishers and advertisers. Although consent from the publisher would be a given, since otherwise it would not be requesting an advert to be placed through the Unified ID 2.0. However, advertisers may be harder to convince since 'The willingness – or lack thereof – of brands to share the emails and data points of users who have purchased a product or performed an action would be a significant blocker to measurement.'[148]

The analysis by Martin Thomson and Eric Rescola from Mozilla concludes with a worrying remark, that 'From a purely technical standpoint, these proposals are a regression in privacy in that they allow tracking of users who are presently protected against tracking.'[149] Due to the way that users fail to properly read consent notices online and the lack of detail about the policy controls imposed on companies in the network it is hard to justify the increased intrusion.

2.4 - APPLE

Apple has undoubtedly taken important steps to shape the rules of the online advertising game. Some will be surprised that the 'privacy-first' tech giant is already in the advertising game, with some forecasting that they may have big plans for the sector.[150] Apple though has a very interesting definition of private, similar in many ways to the Brave on browser model that we reviewed in Section 4.1.2. Apple considers that tracking is private if it all happens on your device. Anything that leaves the device or is processed in the cloud is therefore not private. This has allowed it to build a relatively

[147] Thomson, M. & Rescorla, E. (2021) Comments on SWAN and Unified ID 2.0. Retrieved from https://mozilla.github.io/ppa-docs/swan_uid2_report.pdf

[148] Adelphic (2021) What's Facing a Bigger Challenge Than iOS 14.5? Unified ID 2.0. Retrieved from https://www.adelphic.com/blog/whats-facing-a-bigger-challenge-than-ios-14-5-unified-id-2-0/

[149] Thomson, M. & Rescorla, E. (2021) Comments on SWAN and Unified ID 2.0. Retrieved from https://mozilla.github.io/ppa-docs/swan_uid2_report.pdf

[150] Benedict Evans (2021) Can Apple change ads?. Retrieved from https://www.ben-evans.com/benedictevans/2021/5/13/apples-ads-music

sophisticated tracking system on its devices, such as the iPhone, while at the same time claiming that they respect the privacy of their users.

Tim Cook noted on a recent earnings call that the $17.5bn they earned from various services meant that 'the company set records in music, video, cloud services, advertising and payments.'[151] Apple does not break down the services figure, so it is hard to ascertain exactly how much they earn specifically from advertising – but it is estimated at about $2bn.

This means that Apple currently has a market position more similar to the likes of Amazon, who earned £10bn from ads in 2018, or Microsoft, who earned £7bn in 2018, than the bigger players such as Google and Facebook, who earned $96bn and $50bn respectively.[152]

In the online advertising space, Apple is best known for disrupting the tracking operations of adtech companies, from being the first browser to switch off third party cookies to implementing the App Tracking Transparency feature in the recent iOS 14.5 update.

The reason that Apple may be looking for a new sector, is that at least a couple of significant revenue streams will be curtailed, probably severely, due to various court cases and regulator-led investigations around the world. The revenue streams of specific concern are App Store commissions, wherein Apple take 30% of all purchases on the platform – which is currently worth about $15bn per year - and the Safari default search engine fee, where Google currently pays Apple £10bn per year.[153]

Apple has already established a contained ad system that operates on its own apps and services on the iPhone. Despite their external reputation for privacy, iOS does actually track its users, but the data rarely leaves the device. In fact, Apple has developed a system relatively similar to FLoC, which places users into 'segments'. Apple uses a lot of data to do this, including[154]:

- Account Information: Your name, address, age, gender and devices registered to your Apple ID account.
- Downloads, Purchases & Subscriptions: The music, movies, books, TV shows and apps you download, as well as any in-app purchases and subscriptions.
- Apple News and Stocks: The topics and categories of the stories you read and the publications you follow, subscribe to, or enable notifications from.
- Advertising: Your interactions with ads delivered by Apple's advertising platform.

[151] Leswing, K. (2021) Apple demolishes earnings expectations, but stock falls after iPhone chip supply warning. CNBC. Retrieved from https://www.cnbc.com/2021/07/27/apple-aapl-earnings-q3-2021.html

[152] Wallach, O. (2020) How big tech makes their billions. Visual Capitalist. Retrieved from https://www.visualcapitalist.com/how-big-tech-makes-their-billions-2020

[153] Benedict Evans (2021) Can Apple change ads?. Retrieved from https://www.ben-evans.com/benedictevans/2021/5/13/apples-ads-music

[154] Apple (n.d.) Apple advertising and privacy. Retrieved from https://support.apple.com/en-gb/HT205223

Advertisers can only target segments that have over 5000 individuals in them.[155] Although the system has a lot of resemblance to FLoC, one important difference is that it does not broadcast the segment data, like Google does with the cohort ids. In Apple's system, only Apple can find out in which segment the user seeing that advert has been placed. This removes some of the most important objections to the FLoC system with regards to enabling identification and broadcasting additional data related to a user.

Apple only addresses the sensitive category issue by stating in the policy document that 'Apple does not know or make available to advertisers information about your sexual orientation, religious beliefs or political affiliations.'[156] Apple also makes clear that financial and health data are not used to put people into segments.[157] Although this is welcome, as with Google, it requires us to accept that a technology company will be in charge of deciding which categories are deemed sensitive, as well as resolving cases when they appear.

Some commentators noticed with interest that just as Apple changed its setting on iOS to make tracking opt-in, it started selling targeted adverts in the App store.[158] Together with the projected revenue hole from ongoing legal and regulatory challenges, it is tempting to join the dots and see Apple entering the ad market. While Apple focuses exclusively on advertising on their own apps and services it will remain a relatively small revenue stream for the company. However, if it decided to open up its segment-based ad delivery system beyond its own apps and services, so that others could allow advertisers to target people without exposing any data about the user, this line of business could grow dramatically.

At the moment, the online advertising market is in flux and all of the momentum leads towards models of advertising that respect privacy far better than those in use today. This means that Apple is in a good place, as the privacy-first big tech company, to make privacy preserving advertising work. As Benedict Evans noted, 'Apple has both the market power and the brand to launch a new privacy-based tracking and targeting ad model, and offer it on hundreds of millions of high-spending users' devices.'[159] However, with great opportunity comes great risk and should Apple get the offer wrong they could undo years of careful positioning in the market.

[155] Apple (n.d.) Apple advertising and privacy. Retrieved from https://support.apple.com/en-gb/HT205223

[156] Apple (n.d.) Apple advertising and privacy. Retrieved from https://support.apple.com/en-gb/HT205223

[157] Apple (n.d.) Apple advertising and privacy. Retrieved from https://support.apple.com/en-gb/HT205223

[158] Benedict Evans (2021) Can Apple change ads?. Retrieved from https://www.ben-evans.com/benedictevans/2021/5/13/apples-ads-music

[159] Benedict Evans (2021) Can Apple change ads?. Retrieved from https://www.ben-evans.com/benedictevans/2021/5/13/apples-ads-music

5

BANNING **THE USE OF PERSONAL DATA** TO SERVE ONLINE ADVERTS

As we have seen from the previous section, we are entering a new world of online advertising, whether tech companies, adtech intermediaries, advertisers and publishers like it or not. What is much less certain is the model that will replace the existing tracking-based online advertising, not just in terms of targeting individuals but also measuring the impact. The demise of the 3rd party cookies and easy unique mobile identifiers is taking us away not just 'from third party audience targeting but from cookie-based measurement solutions in general.'[160]

There are many within the industry who view this time as a unique opportunity to move forward and avoid repeating the mistakes of the past. As the EFF noted 'instead of re-inventing the tracking wheel, we should imagine a better world without the myriad problems of targeted ads.'[161] Even the IAB has publicly stated that 'it is important to leverage privacy centric approaches.'[162]

However, trying to understand the impact of a particular legislative prohibition is challenging because the range of interventions are so wide. For instance, there is a massive difference between a future where real informed consent is required to serve tracking-based adverts, and a world where the need for consent is coupled with a total prohibition on the use of third-party data, and finally where the use of personal data is completely prohibited.

For the purposes of this section, we will proceed on the basis that a total ban on the use of personal data has been achieved through legislation, and that this restriction applies to all forms of online advertising, including both that done over the real time bidding systems, as well as the model where deep profiles are built up and the platforms allow advertisers to target specific categories or collections of categories. It would also mean an end to the use of first party data for the purpose of advertising. This ban would also include any collection and analysis that happened on the device or browser of the user, even when not shared with the parent company.

> "instead of re-inventing the tracking wheel, we should imagine a better world without the myriad problems of targeted ads."
>
> The EFF

1 – The impact on issues raised in Section 3

Given the major impact this would have on a core funding model for the internet, we need to ensure that any alternative that we propose will not fall fowl of the same issues. In this section. we will very briefly re-examine each of the issues that we raised in Section 3 to understand how a complete ban on the use of personal data would impact the issue.

Firstly, let us look at the three issues that arise for individuals: the breach of privacy and data rights, bias and discrimination, and the attention arms race that tracking-based advertising turbo charges.

[160] IAB Europe (2021) The IAB Europe guide to contextual advertising. p.21. Retrieved from https://iabeurope.eu/knowledge-hub/iab-europes-guide-to-contextual-advertising/

[161] Cyphers, B. (2021) Google's FLoC Is a Terrible Idea. Electronic Frontier Foundation. Retrieved from https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea

[162] IAB Europe (2021) The IAB Europe guide to contextual advertising. p.6. Retrieved from https://iabeurope.eu/knowledge-hub/iab-europes-guide-to-contextual-advertising/

An online advertising system that does not rely in any way on personal data would no longer infringe on our data and privacy rights. The major challenge in this area will be to ensure that there is proper enforcement of the legislation. As we noted earlier, much of what happens in the tracking-based advertising sector is already illegal under current legislation, the problem is that it is not being enforced. Enhancing our data rights and protections with a clear ban on the use of personal data for advertising in either the upcoming e-Privacy Regulation or the Digital Services Act, would be hugely welcome and 'a general ban may force overarching structural transformation of surveillance business models.'[163]

A post-personal data driven advertising world would also make it harder to discriminate against people in the same way as today. No longer would there be lists of personal characteristics that can be used to filter messages. Instead, advertisers would mainly be able to choose from a wide variety of interest segments that are contextually relevant to the content. It is possible that some contextual data could be used as proxies for characteristics such as race, religion or sexuality, but much less so than today.

Regarding 'the arms race', this is something that would still take place in the post personal data world because we would still train ourselves to ignore adverts and marketeers would do their best to capture our full attention. One aspect of the attention arms race that would disappear with making the use of personal data illegal is the huge effort to continue to track people, even those who have taken steps to protect themselves.

Secondly, we shall explore the issues that affect our wider society and democracy. To name some of the key problems, the sector is anti-competitive, a threat to national security, allows for micro-targeting, produces lots of carbon emissions and enables large scale adfraud.

A general ban on the use of personal data is likely to have both positive and negative impacts on the level of competition in market. On the one hand, the elimination of the use of personal data removes one of the major competitive advantages that the biggest players, such as Google and Facebook, have over the rest of the industry. This change would therefore seem to create much more of a level playing field for all publishers to compete on. However, this is not the whole picture, and some publishers that we spoke to were worried that the biggest players would further cement their dominance in the post personal data world. This is because, they note, in a world where advertisers are looking for the right context to target ads, it is those with the largest and most varied web presence that will have the biggest range of context for advertisers to target. To tackle the power of the largest tech companies there must be robust enforcement of existing antitrust regulations in the EU as well further measures, especially in the DSA, to curtail their anti-competitive dominance.

From a national security perspective anything that reduces the incentive to gather huge troves of personal data, create detailed profiles and most importantly allow entities to track and target them with specific, often highly tailored, messages will reduce the associated risk. It is important to note

[163] Forbrukerradet (2021) Time to ban surveillance based advertising. p.16. Retrieved from https://www.forbrukerradet.no/wp-content/uploads/2021/06/20210622-final-report-time-to-ban-tracking-based-advertising.pdf

that a ban on the use of personal data for advertising does not mean that it will cease to be collected. Personal data has many uses beyond advertising, such as in generating recommendation algorithms to keep users on this site and training artificial intelligence systems that are used for a wide variety of purposes.

It will be much harder to design an effective micro-targeting campaign following the reforms. The reason for this is that the individual user targeting engine has been dismantled. This will however not be the end of the targeting of political messages, only a shift away from them being used to target small groups, and individuals, with specific messages, to a system where they are able to target all the users engaging with a particular context.

Just as the dissemination of disinformation did not start with tracking-based advertising, banning the practice will not end it altogether. However, a general ban would have a massive effect on the ability of these sites to easily monetise their activity by showing adverts. They can, of course, continue to provide adverts, but advertisers will now be targeting based on the content, which as 'disinformation' is highly unlikely to be attractive to advertisers or brands. In addition, the increased transparency in the system would make it much easier for advertisers to know exactly where their adverts have been placed. Since few advertisers will want to be on such sites, this should lead to a significant reduction in the quantity and profitability of disinformation.

Although preventing personal data collection would have the positive effect of lowering the carbon footprint of online advertising it would not eliminate it completely. Indeed, the report that we cited, which only calculated the direct emission from the actual provision of the ad over the auction network, may in fact reflect the reality of emission much more closely. This is because we would no longer have to take into account the associated carbon emission related to the collection of personal data and its analysis by all publishers and advertisers as well as adtech intermediaries and data brokers. Just as we cautioned against the increased use of artificial Intelligence (AI) to better analyse personal data, a mandated move away from personal data would also lead to a lot of AI systems trying to improve the contextual data.

The reform will also affect adfraud. This has flourished due to the complexity and opacity of the current market. Many people that we spoke to for this report highlighted that a post-personal data marketing world would not require as many intermediaries, thereby making it much less complex, creating a more transparent environment, which would provide much less opportunity for adfraud operators to flourish. The hope is that the overall reduction in adfraud would then also reduce publisher's and advertiser's investments in fraud detection and reduction methods, thereby leading to less revenue wastage, which could result in lower prices for advertisers or more revenue for publishers.

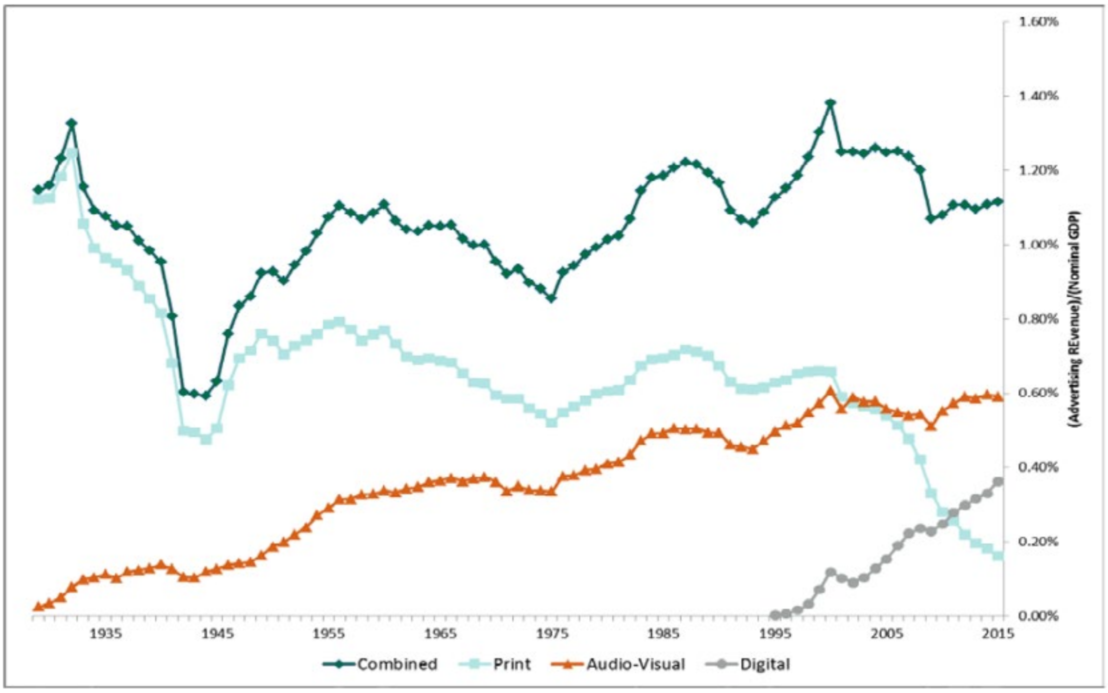
2 - The impact on online advertising spending

The previous section demonstrated that a general ban would have a positive impact on the issues that tracking-based advertising raises for individuals and society. It is also important to consider how those who rely most on *actually using the system* would fare after a ban. In this section we will explore the evolution of spending on advertising and how it may shift after a ban is imposed, look at the potential of contextual advertising and whether it can scale. The section will conclude by examining some of the challenges and opportunities for publishers, SMEs, big tech companies and advertisers.

2.1 - TOTAL AD SPEND: IT'S ALL ABOUT REDISTRIBUTION

As figure 7 demonstrates below, **the % of GDP that is spent on advertising has remained remarkably stable since the 1930s, between 1 and 1.4% of GDP, except for a significant dip during the First World War.** In the chart, it is possible to see the spending on advertising dip after periods of crisis. For instance, there is a noticeable drop after the dotcom crash around 2000 and the financial crisis of 2008, but always within the long-term bounds. Indeed, the advent of tracking-based targeting of online adverts in 2009-10 does not show the growth in ad spend increase dramatically but really only start to regain recent losses.

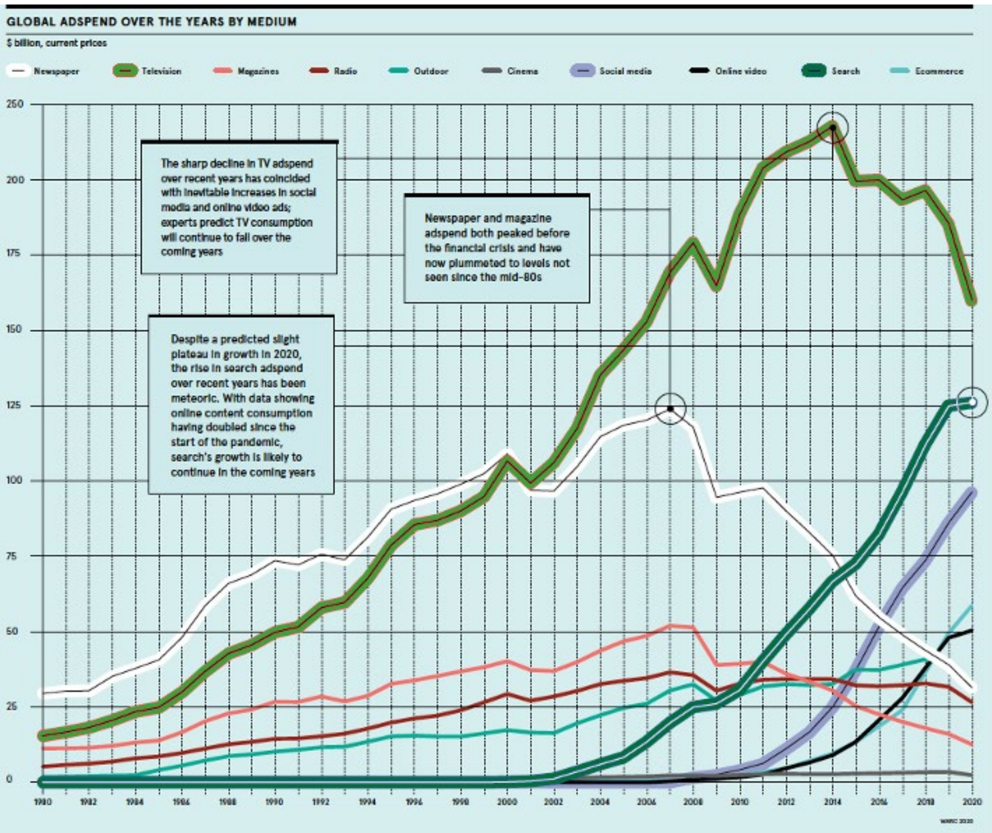
Figure 7: Advertising Revenue as a % of GDP



Source: Measuring the "Free" Digital Economy Within the GDP and Productivity Accounts (2017)

The more granular detail that Figure 8 below gives us into the distribution of adspend globally by medium really shows the winners and losers from the last 10 years. The figure shows that newspaper adspend has been in decline since 2005 from $125bn to just over $30bn in 2020, while television advertising peaked in 2014 at $240bn declining to $160bn by 2020. At the same time spending on search, social media and online video all rose dramatically going from nothing at the turn of the century to $125bn, $95bn and $50bn respectively.

Figure 8: Global $bn spent on advertising per medium



Source: https://www.raconteur.net/infographics/ad-evolution/

Therefore, despite all the massive societal changes we have seen in the last 100 years and the radical transformation in how most advertising is delivered, nothing short of a world war has actually managed to alter the level of global advertising expenditure, as we noted in figure 7. If, as has been shown, the development of tracking-based advertising did not lead to a correlative growth in advertising spend, then we can expect a reduction in tracking-based methods will equally not lead to a decrease in overall spend. Put more intuitively: there will always be demand for advertising on the part of business, irrespective of the techniques used to deliver it. Indeed, the broader trends that we outline above would allow you to believe that total ad spend would remain relatively steady even after a ban was implemented.

As a marketing executive recently remarked, 'While the rates might go down (read premium for advanced targeting) and some things will break (or not work as well) in the end, the shift of spend to other mediums won't happen. Eyeballs are still online and buyers will find them. The tactics and strategies will change, which is not a bad thing.'[164]

So, what we really need to be interested in is how the advertising spend may re-distribute itself once

[164] Claburn, T. (2021) Google's FLoC flies into headwinds as internet ad industry braces for instability. The Register. Retrieved from https://www.theregister.com/2021/04/17/google_floc_adoption/

tracking-based advertising has been outlawed. Some publishers I spoke to were positive about the redistribution citing the fact that if advertisers have to start paying to appear based on the context of the content that it will advantage those publishers who produce quality content. At the same time, they hoped that it would also 'put out of business the long tail of low-quality or outright fraudulent sites that currently soak up much of the money spent on automated programmatic advertising.'[165]

However other publishers and experts with whom I spoke were less positive. One industry expert was very dismissive of the possibility that adspend would flow back in any significant quantity to news outlets. Other publishers worried a lot about whether the spend would flow instead into the walled gardens of the likes of Google and Facebook, as well as to other mediums like Connected TVs. There is good evidence that the worry is well-founded. Since 2016, Google and Facebook have increased their share of global ad revenue from 19% to 34% in 2020.[166] Therefore, without rigorous enforcement of EU competition rules to ensure a well-functioning market, together with further regulation in upcoming legislation such as the DSA, there is a risk that enforcing rules primarily designed to protect the rights of individuals could lead to further consolidation of power within the tech giants.

2.2 - CONTEXTUAL ADVERTISING WORKS AND IT CAN SCALE

Another clear point is that there exists a technical solution that can deliver the volume of online advertising needed, using the existing (or slightly repurposed) auction infrastructure – contextual advertising 'works.'[167] This type of advertising can be done programmatically, meaning that it can be automated. This is the only way to ensure that the massive volume of ad inventory can be sold. Although we do envisage some publishers re-investing in the creation of a direct sales model for some of their inventory, almost all those interviewed for this report were clear that the future had to involve programmatic ad delivery.

A recent report by the IAB supports this when it concludes that 'contextual solutions provide the scale advertisers need without the use of hashed emails, user opt in or any cookie like mechanism, making it even more valuable in the current landscape.'[168]

We noted in Section 4.1.1 a **74% of marketing executive consider contextual one of the most important strategies**[169] **and that 65% of advertisers expect to increase their contextual ad spend.**

[165] Edelman, G. (2020) Can killing cookies save journalism. Wired. Retrieved from https://www.wired.com/story/can-killing-cookies-save-journalism/

[166] Turvill, W. (2021) Quintopoly? Five tech companies now earn 46% of global ad revenues as news media left behind. Press Gazette. Retrieved from https://www.pressgazette.co.uk/global-advertising-spend-2020-quintopoly/

[167] IAB Europe (2021) The IAB Europe guide to contextual advertising. Retrieved from https://iabeurope.eu/knowledge-hub/iab-europes-guide-to-contextual-advertising/

[168] IAB Europe (2021) The IAB Europe guide to contextual advertising. Retrieved from https://iabeurope.eu/knowledge-hub/iab-europes-guide-to-contextual-advertising/

[169] IAB Europe (2021) The IAB Europe guide to contextual advertising. p.9. Retrieved from https://iabeurope.eu/knowledge-hub/iab-europes-guide-to-contextual-advertising/

[170] Major publishers are coming out in favour of the move to contextual. For instance, the head of ad operations and monetization of major publisher Conde Nast noted ‘a lot of publishers are thinking about how do we get back to context, and it’s almost like everything old is new again.’[171] Similarly, Aram Zucker-Scharff from the Washington Post has publicly stated that he thinks that ‘contextual is fundamentally the future of web advertising, and … what every publisher’s going to end up having to do.’[172] Other publishers that I spoke to noted that contextual could work very well for specialised publications that have built a dedicated following.

Other publishers I spoke to were much more sceptical. As well as highlighting the issue mentioned in the previous section that the move away from personal data may in fact benefit big tech the most, they raised additional concerns, especially for news publishers. They pointed out that not all context is equal and that in fact news and sports coverage does not perform well for context driven marketing. For some of the best-known publishers this sort of content represents the bulk of the advertising inventory. They highlighted that there is currently very little demand for context-based advertising and that therefore they may struggle to fill their inventory. They also expressed concern about the increased use of contextual resulting in blacklisting many of their pages due to brand safety reasons. The recent COVID outbreak is a good example. Many companies decided to block their adverts from being placed next to articles about COVID, leading to many pages on which publishers struggled to sell ad inventory.

These concerns may be true today, where personal data-based advertising is still permitted. However, when advertisers no longer have this option, they will need to find other ways to connect with their audience. It makes intuitive sense that respected news outlets publishing quality content with great contextual interest fields and the latest sentiment analysis should be able to provide advertisers with ad inventory they want to secure. For instance, the COVID article might actually be about the pandemic ushering a new world of remote working. Understanding the article in this depth would actually lead to good advertising opportunities. We therefore believe that the imperative to no longer use personal data, coupled with well implemented contextual targeting systems can allow publishers to continue to monetise their content. It will also be important to influence the actions of advertisers and their sometimes over-zealous marketing partners or legal teams to ensure that in the pursuit of brand safety they do not ignore good opportunities.

> **‘contextual is fundamentally the future of web advertising, and … what every publisher’s going to end up having to do.’**
>
> **The EFF**

[170] Customer Data Platform Institute (2021) Two-Thirds of Advertisers Plan Higher Contextual Ad Spend: Connatix Survey. Retrieved from https://www.cdpinstitute.org/news/two-thirds-of-advertisers-plan-higher-contextual-ad-spend-connatix-survey/

[171] Peterson, T. (2020) ‘A system that is out of alignment’: Online ad industry faces its identity crisis at IAB’s annual meeting. Digiday. Retrieved from https://digiday.com/marketing/system-alignment-online-ad-industry-faces-identity-crisis-iabs-annual-meeting/

[172] Edelman, G. (2020) Can killing cookies save journalism. Wired. Retrieved from https://www.wired.com/story/can-killing-cookies-save-journalism/

2.3 - SMES

The reliance of SMEs on tracking-based advertising is regularly used by the adtech industry, especially Facebook, as a justification for blocking major reform in this area. Facebook currently has around 2 billion monthly active users all categorised into hundreds if not thousands of interests and segments. For many SMEs, this offers them a marketing channel where they can effectively target prospective customers.

For a bricks and mortar SME, this may mean targeting based on the location, supplemented by an interest in the service, product or something related. An online SME can simply target disparate people all over the world who might be interested in their product or service. The tracking-based advertising ecosystem also offer a service that can accommodate any budget. Facebook, and others in the adtech world, claim that without them offering their personal data based targeting that SMEs would be considerably disadvantaged since they do not have the money for relatively expensive print or TV adverts. However, we believe these claims to be overblown. Just taking Facebook, where a lot of SME marketing spend happens, it seems obvious that the company would be able to build an excellent contextual targeting system that would allow SMEs with physical locations seeking local people to target by focusing on when users view or interact with businesses and/or events that are registered in that particular area. At the same time, an online SME with no physical location should still find enough people to target based on contextual interest information of people engaging with content.

We noted in Section 3.2.6 the huge prevalence of adfraud. The businesses most at risk of adfraud are the SME community who want to use the opaque tracking-based advert targeting system but do not have in-house marketing expertise, nor large budgets, to prevent fraud and abuse. This is because many big players spend significant sums on vendors and software to try and detect adfraud to reduce and hopefully eliminate it. Dr Augustine Fou, an expert on adfraud, notes that 'virtually all marketers spending money in programmatic know how crappy it is, and have therefore spent extra money buying fraud verification, hoping to detect [their] way out of trouble.'[173]

Some even question the efficacy of some of the more sophisticated adfraud detection tools and consider that 'current fraud detection can't catch anything,[174] is prone to error,[175] and still doesn't help you[176].'[177] If the professional and expensive software does not solve the problem of adfraud, as its wider prevalence suggests, then the SMEs who have little marketing expertise and no revenue to

[173] Dr Fou, Augustine. (2021) Three Step Plan To Kick The Digital Marketing Habit. Forbes. Retrieved from https://www.forbes.com/sites/augustinefou/2021/05/18/three-step-plan-to-kick-the-digital-marketing-habit/?sh=574f0a0a15c1

[174] Dr Fou, Augustine. (2020) What Your Fraud Detection Vendor Misses. Forbes. Retrieved from https://www.forbes.com/sites/augustinefou/2020/11/23/what-your-fraud-detection-vendor-misses/

[175] Dr Fou, Augustine. (2020) Examples Of Incorrect Measurements By "Black Box" Fraud Detection. Forbes. Retrieved from https://www.forbes.com/sites/augustinefou/2020/07/24/how-to-select-a-fraud-verification-vendor/

[176] Dr Fou, Augustine. (2019) Even if Bot Detection Tech Works, It's Still Useless - Here's Why. Retrieved from https://www.linkedin.com/pulse/assuming-fraud-detection-works-its-still-useless-/

[177] Dr Fou, Augustine. (2021) Three Step Plan To Kick The Digital Marketing Habit. Forbes. Retrieved from https://www.forbes.com/sites/augustinefou/2021/05/18/three-step-plan-to-kick-the-digital-marketing-habit/?sh=574f0a0a15c1

protect against adfraud are likely to be hit the hardest. Many in the industry warn that 'If you're spending advertising dollars and using the free version of Google Analytics to track results, you're long overdue for a reality check.'[178]

This means that moving away from tracking-based adverts will not necessarily be a massive issue for the SME community since both place-based and online businesses should be able to continue to access their desired customer bases while at the same time the increased simplicity and transparency of the post personal data advertising sector means that less of their spend should be wasted due to fraud.

2.4 - PUBLISHERS

Anyone who creates content to put online is an online publisher. The expansion of online advertising to all publishers has enabled some to make a living who would not have survived in the old analogue world. Equally other publishers, who had been able to rely on advertising revenue, are now struggling in the online world.

An important subset of publishers is represented by news organisations, some with a foot firmly in print still, while others are purely digital. A vibrant news sector is a critical element of a well-functioning democracy. This means that the financial viability of the sector is also something that everyone should be concerned with. Over the course of the last century many publications developed a financial model that meant they were dependent, to varying degrees, on advertising. Since the development of the internet and tracking-based advertising in particular the sector has been struggling to maintain its advertising revenue.

Although partly a story of inevitable technological change a number of decisions taken by these publishers, sometimes for good reasons, have ultimately led to the grave situation they find themselves in today. There were two critical decisions that primarily shaped this future. Firstly, most publishers decided to publish all their material online for free, which has led to the situation where many people do not think that they need to pay for their news. Many may have underestimated the challenge of getting people to pay for something that they have come to think of as free. Secondly, as they embraced the tracking-based advertising model most acquiesced to having the adtech industry and big tech companies place trackers on their website. This meant that news publishers were essentially allow many other companies to track and collect data about their users. This ultimately led to the situation today where most news publishers really struggle to get people to pay for content, while they are losing their key unique asset, their readers' data.

Eliminating the ability of publishers to use any personal data will create an additional challenge for the publishing industry. This is especially the case if the prohibition of personal data use extends to first-party data they may continue to collect from their users for purposes other than targeting advertising. A recent report my McKinsey estimated that the publishing industry will need to replace

[178] Hopf, P. (2016) What Marketers Can Learn From The Cautionary Tale Of Criteo Vs. SteelHouse. Retrieved from https://www.mediapost.com/publications/article/284237/what-marketers-can-learn-from-the-cautionary-tale.html

about $10bn of ad revenue that are currently based on tracking-based advertising.[179] Two of the recommendations that McKinsey suggest to rectify the shortfall do not require collecting and analysing personal data. They recommend that as well as relying on paywalls 'updated contextual targeting' should also be part of the mix.

A report recently published by PriceWaterhouseCooper, commissioned by the Incorporated Society of British Advertisers, concluded that, when considering the complexity of the adtech ecosystem and the amount of money it pocketed, that 'these challenges and complexities do not serve the principal interests of advertisers or publishers.'[180]

2.4.1 - Moving unilaterally via legislation

The challenge of how to fund publishers, especially news outlets, is one of the major challenges that the switch to online has helped accelerate. Many of the publishers that I spoke to for this report were fearful for their future without the ability to use personal data to provide the kind of targeting that, they claim, advertising want. This leads to a challenge for publishers that they do not feel that they can move away from the use of personal data unilaterally, because many of the advertisers would shift their adspend to a platform still targeting individuals.

This could be overcome by legislating an end to the use of personal data. This would create certainty in the market, assuming the rules were enforced, and would require both publishers and advertisers to move to a new way of targeting their adverts. This would create a level playing field for publishers and allay their fears because advertisers would not be able to move the spend to publishers still using tracking-based advertising.

The way that EU law is implemented also helps ensure that there is an orderly transition. It is normal for most EU laws to come into force in Member States two years from their adoption by the EU. This will put the sector on notice, while giving everyone time to adapt their operations to the new reality. According to Ster 'part of NPO's rapid success came from the fact that advertisers saw the privacy writing on the wall and were eager to find out if a nontargeting ad platform could deliver results.'[181]

2.4.2 - Publishers can get more of ad $

In recent years, there has been work to try and understand the flow of money from advertiser to

[179] Brodhersen, M. et al (2021) The demise of third-party cookies and identifiers. McKinsey & Co. Retrieved from https://www.mckinsey.com/business-functions/marketing-and-sales/our-insights/the-demise-of-third-party-cookies-and-identifiers

[180] Incorporated Society of British Advertisers (2020) Time for change and transparency in programmatic advertising. Retrieved from https://www.isba.org.uk/article/time-change-and-transparency-programmatic-advertising

[181] Edelman, G. (2020) Can killing cookies save journalism. Wired. Retrieved from https://www.wired.com/story/can-killing-cookies-save-journalism/

publisher. This has shown that publishers forgo between 35%[182] and 70%[183] of every € spent on online adverts on their websites to a number of adtech intermediaries who each take a thin slice of pie. Even the conservative estimate from the UK's CMA of 35% still caused them to note that, 'although intermediaries are undoubtedly performing valuable functions, including targeting advertising and evaluating bids from multiple demand sources in real time, it is striking that collectively they are able to take more than a third of the total amount paid by advertisers.'[184] Very worryingly the calculation from the Incorporated Society of British Advertisers (Isba) found that one third of the adtech ecosystem supply chain costs were unattributed.[185] This means that money spent on showing adverts could not be traced back to any publisher or adtech middleman, which at best is illustrative of the opacity at the heart of the tracking-based advertising system and at worst implies large scale fraud worth billions of pounds annually.

One of the mains reasons that such a significant percentage of each ad euro goes to adtech intermediaries is that the system is so complex and opaque. This requires that publishers spend money to help build the right audience for the campaign, find the right channels to advertise on and monitor for adfraud.

By contrast publishers using Kobler's contextual targeting platform can get 85% of each ad euro spent thanks to a hugely simplified system, which does not rely on rich personal data sourced from a multitude of adtech companies and offers full transparency. Imposing a general ban on the use of personal data therefore offers up the prospect of publishers being able to capture a much greater percentage of the total adspend. This increase in the percentage gives some of the other variables in the system some slack to adjust over time. This means that even if there was a drop in advertising volume or price, the amount in publisher's pockets may remain static. It also holds out the prospect that if there is no or little drop in volume or price, that publishers could actually start to make more revenue from advertising, as the example of NPO in Section 4.1.1 demonstrated.

2.4.3 - Reset the asymmetrical relationship with big tech and adtech

An analogy of a bookshop can be useful in understanding the relationship between publishers and big tech, because it intuitively shows that certain practices that have been normalised in the online world are totally inappropriate. The publisher, who uses tracking-based advertising to monetise their customers, takes the role of the bookshop. For this bookshop business to operate they must allow tracking-based advertising. This requires them to create space for advertising, which in turn means installing trackers that allow the bookshop as well as 3rd parties to track their customers.

[182] Competition and Markets Authority (2020). Online Platforms and Digital Advertising. p.65. Retrieved from https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study

[183] Ice, B. (2016) Guardian buys own ad inventory, only gets 30p to the pound. Retrieved from https://www.marketingmag.com.au/news-c/guardian-programmatic-advertising/

[184] Competition and Markets Authority (2020). Online Platforms and Digital Advertising. p.65. Retrieved from https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study

[185] McCarthy, J. (2020) 'Big hole in the value chain': one third of adtech costs unattributable finds Isba. The Drum. Retrieved from https://www.thedrum.com/news/2020/05/06/big-hole-the-value-chain-one-third-adtech-costs-unattributable-finds-isba

However, their big tech & adtech partner in fact uses the data that they collect not only to compete directly with the bookshop by selling books, but also to recommend other bookshops. As if this was not enough, their big tech & adtech partners also use the insight provided by the data to encourage the bookshop to outsource their infrastructure to the big tech/adtech companies. More and more bookshops, and other businesses, make the jump because 'when you don't comply they drop you off the map and send people to your competitors.'[186] This analogy demonstrates the self-destructive nature of the current system for publishers.

Only by ending the tracking-based model, which would fundamentally change the nature of the game, can publishers, adtech companies and big tech begin to develop a relationship on more equitable and less extractive grounds. The general ban will remove one of the major incentives to track users around the internet and mean that publishers will no longer feel obligated to enable this huge industry. In addition, adverts no longer based on personal data would reduce the dependence of publishers on adtech intermediaries. The general ban on personal data would, in itself, be insufficient to reset the relationship, especially with big tech, but without the ban it would be very hard.

2.5 - BIG TECH

There is a worry that moving away for tracking-based advertising could also spell the end of all the many 'free' services, from maps to search to e-mail, that we have all come to rely on – and want to remain 'free'. In reality, of course, we do pay for these services, with our attention.

The end of tracking-based advertising should not damage the revenues of the tech giants since Google, Facebook and the other major tech platforms will still be the platforms where internet users spend significant amounts of time. The giants will still be able to monetise the attention of these users. They will just have to do so using alternative methods to deliver adverts, such as contextual. Therefore, their direct advertising business should not be hit by the general ban. Some are even predicting that, at least initially, many advertisers may move their spending on advertising to the tech giants, meaning that in the short term they may even see revenues rise.

Where there may be an impact will be in two areas: the fees they collect for owning so much of the adtech infrastructure, and their overall balance sheet.

Google is a significant player at every stage of the adtech ecosystem, with many other companies competing to get a foothold in various parts of the market. This is because a lucrative model has emerged with intermediaries able to capture between 35-70% of each € spent on online advertising. In a post tracking-based advertising world, there will be less demand for many of the adtech services currently available, since it will no longer be necessary to combine the data the various companies hold on users. This means that they will not be able to collect commission for the various intermediary roles that they play in the current adtech system. In fact, if there is a massive move to contextual this will decimate the adtech intermediary since this form of marketing just does not require the same kind of intermediation.

[186] Berjon, R. (2021) Pushing back against privacy infringement on the web. Smashing Magazine. Retrieved from https://www.smashingmagazine.com/2021/08/against-privacy-infringement-web/

The tech giants will also take a hit on their balance sheets. If personal data was no longer able to be used for the provision on adverts online, then this would dramatically reduce the value of the personal data troves that they have built up over the years. A ban on the use for advertising will not reduce its value to zero, however, since, bar additional regulatory restrictions, they will still be able to use it to refine and improve various algorithms to increase engagement and keep users on the platforms for as long as possible, such as their recommendation algorithms.

5.2.6 - Advertisers

Advertisers are often blamed for the growth of tracking-based advertising. Many publishers, even those who understand the negative impact of the practice, feel bound to maintain the model due to fears of losing revenue. As we explored in the section on publishers, there remains a huge fear around moving unilaterally away from the model because the received wisdom is that advertisers will just go to other publishers that still allow them to target specific individuals based on their personal data.

Part of the reason that tracking-based advertising is so popular with advertisers is that it quantifies their activity. The famous marketing saying that 'half the money I spend on advertising is wasted; the trouble is I don't know which half,'[187] neatly illustrates the limited understanding of the impact associated with different advertising methods and messages. Surveillance based advertising changed all of that and now 'gives marketers the high they've been seeking — enormous reach, low prices, and high engagement.'[188]

As we have noted in previous sections, there remains a serious debate to be had about whether the metrics really tell the marketeers what they think they do, and also whether, thanks to the prevalence of adfraud, they can be trusted. There are three core metrics that many online advertisers use: impressions, clicks and conversion. In theory this tells advertisers how many people saw their ad, how many engaged with it and that engagement led to actual purchases. However, when you look at the detail of what is has been promised and what is actually delivered, at least some of the shine of tracking-based advertising wears off. For instance, one of the ways that advertisers can pay is per 'impression' (or more often per thousand or million impressions). An impression is supposed to tally with the advert actually being seen. But, in reality, the definition of the metric falls far short of this. Apple, for instance, defines an impression as 'each time at least 50 per cent of your ad is visible for one second.'[189] what they are really selling is a sort of Schrodinger's cat of impressions. While the definition allows for the possibility that the advert was seen, it cannot confirm it for certain.

The click metric is not subject to the same uncertainty because it is actually measuring a well-defined action: a click. The challenge with this metric is to understand whether the person ever intended to

[187] Chait, G. (2015) "Half the money I spend on advertising is wasted; the trouble is I don't know which half". Retrieved from https://www.b2bmarketing.net/en-gb/resources/blog/half-money-i-spend-advertising-wasted-trouble-i-dont-know-which-half

[188] Dr Fou, Augustine. (2021) Three Step Plan To Kick The Digital Marketing Habit. Forbes. Retrieved from https://www.forbes.com/sites/augustinefou/2021/05/18/three-step-plan-to-kick-the-digital-marketing-habit/?sh=574f0a0a15c1

[189] Apple (n.d.) Understand Search tab campaigns. Retrieved from https://searchads.apple.com/uk/help/advanced/0071-book-search-tab-campaigns/

click. Someone who never meant to click on an ad and closes the tab or window immediately should not be counted in the same category as someone who saw the ad and wanted to engage with it. However, research shows that up to 60% of banner ad clicks on mobiles are accidental, mainly due to the small screen.[190] While rates are much lower in adverts placed on laptops and desktops the issue remains a problem. Some companies, such as Facebook, have changed the way they count clicks for advertisers, so that they are not charged if the ad webpage is closed within 2 seconds.[191]

60%

of banner ad clicks on mobiles are accidental, mainly due to the small screen.

The third major metric that advertisers have become dependent on is conversion. This attempts to measure whether a particular advert has led to an actual sale, or any other activity that the advertiser is seeking. Because conversion is the most desirable outcome, a lot of effort goes into proving that a particular vendor's ad placement was responsible rather than another, since many large advertisers will use multiple adtech companies for their campaign. Some of the biggest adtech companies, such as Steelhouse, have been accused of tricking advertisers into thinking they were responsible for the conversion.[192] Problematic conversion metrics have also been highlighted by Uber who, following an experiment to find out which of their adtech vendors was placing their adverts on Breitbart website, stopped 80% of their online marketing without altering their customer retention and acquisition. Uber's legal documents note that 'the number of installations supposedly attributable to mobile advertising (i.e., "paid signups") decreased significantly, while the number of organic installations rose by a nearly equal amount. This indicated that a significant percentage of the installations believed to be attributable to advertising were in fact stolen organic installations. In other words, these installations would have occurred regardless of advertising.'[193] Many other major companies have also conducted 'turn off experiments' with shocking results. Proctor and Gamble cut $200m with no effect[194], Chase reduced its reach[195] by 99% with no effect[196] and AirBnB cut over $800m with no effect.[197]

[190] Digital Content Next (2016) Sixty percent of mobile banner clicks are accidental. Retrieved from https://digitalcontentnext.org/blog/2016/02/10/sixty-percent-of-mobile-banner-clicks-are-accidental/

[191] Loechner, T. (2017) Up to 13% of mobile video ad clicks are accidental. Retrieved from https://www.pixalate.com/blog/accidental-clicks-mobile-ads-data

[192] Hopf, P. (2016) What Marketers Can Learn From The Cautionary Tale Of Criteo Vs. SteelHouse. Retrieved from https://www.mediapost.com/publications/article/284237/what-marketers-can-learn-from-the-cautionary-tale.html

[193] Dr Fou, Augustine. (2019) Stone, Meet Glass House - The Significance of Uber's Second Ad Fraud Lawsuit. Retrieved from https://www.linkedin.com/pulse/stone-meet-glass-house-significance-ubers-second-ad/

[194] Vranica, S. (2018) P&G Contends Too Much Digital Ad Spending Is a Waste. Wall Street Journal. Retrieved from https://www.wsj.com/articles/p-g-slashed-digital-ad-spending-by-another-100-million-1519915621

[195] Reach is the range of sites that the advert appears on. They had previous been on 400,000 different webpages but they decided to go with just 5000.

[196] Maheshwari, S. (2017) Chase Had Ads on 400,000 Sites. Then on Just 5,000. Same Results. New York Times. Retrieved from https://www.nytimes.com/2017/03/29/business/chase-ads-youtube-fake-news-offensive-videos.html

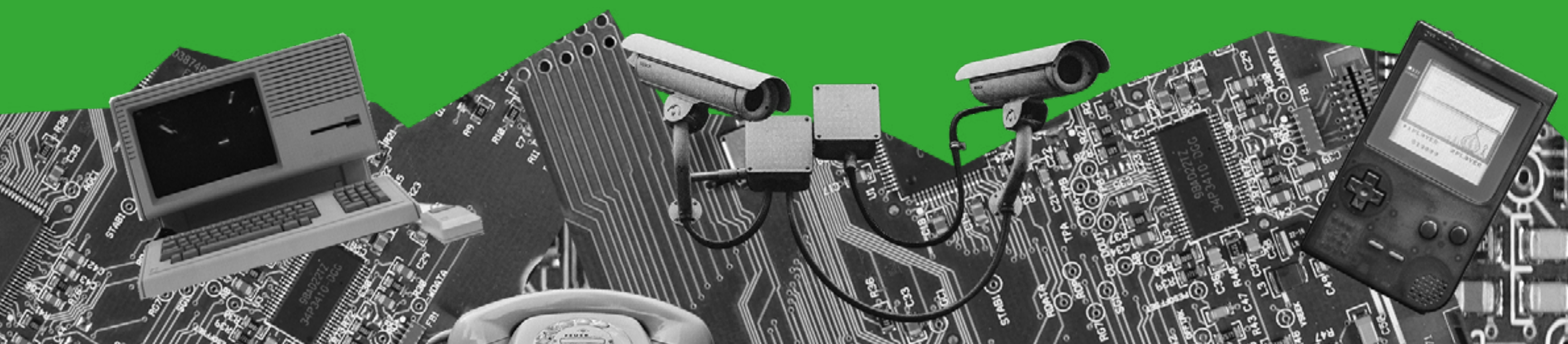
[197] Glenday, J. (2020) Airbnb halts marketing spend in $800m savings plan. The Drum. Retrieved from https://www.thedrum.com/news/2020/03/30/airbnb-halts-marketing-spend-800m-savings-plan

Taken with the huge issues raised by adfraud affecting both reputable platforms, like the examples of Facebook and LinkedIn that we mention in Section 3.2.6, but also criminal actors seeking their piece of the advertising pie, the whole tracking-based ad ecosystem does not look like the optimise engine for advertisers that many claim it to be

This means that although it will require a massive change for advertisers it will not necessarily harm their businesses. Brands will still need to connect with their audience and marketeers will still find ways of doing so. They will almost certainly be more effective than the marketing programmes that the likes of Uber, Airbnb and Ebay were running.

6

CONCLUSION



Trying to predict how online advertising will be able to target an audience is wrought with uncertainty. The only certainty is that we will move away from the current form of tracking-based advertising that we describe in Section 2. We know that this is going to happen for two reasons. Firstly, as a society, we are starting to appreciate the myriad of issues that tracking-based advertising causes. The massive infringement of our hard-won privacy rights is causing civil society groups, such as Amnesty and EDRI, to start-up campaigns to outlaw the practice, while a range of other organisations have also come out in favour of a ban. Regulators are also starting to take action, either voluntarily, as in the case of Belgian Data Protection agency[198], or by being compelled to do so, as in the case of Johnny Ryan in Germany.[199]

Secondly there are a whole host of alternative systems, all of which are improvements on the current one, to varying degrees. Of all of the alternatives that we explored, only contextual advertising would be permissible if there was a total ban on the use of personal data to target a user with adverts. Even ignoring all of the issues that the report raises with the other proposals, and assuming they worked perfectly, meaning that they protected our personal data, none of these alternatives would be permitted under a strict and complete ban. Despite the stated intentions by the likes of FLoC, Parakeet and other systems, there is good reason to believe that these alternatives would not provide the privacy and security that an outright ban could. The various other proposals that we explore aim to keep user's data safer in a variety of ways, while still relying on it. From Brave, which ensures that users' data never leaves your device, to FLoC, which creates groups of users with similar interests, to Parakeet, which seeks to utilise differential privacy, they all try and give users the privacy that is abundantly clear they want while at the same time providing advertisers the ability to target.

Without new legislation it is almost impossible to predict whether many of these proposals will co-exist or whether one will emerge to become the dominant replacement for the current system. It is important to recognise the powerful position that some of the players, like Google and Facebook, have in shaping the future. Changes to the online advertising system will require that businesses who rely on it, both to advertise and for revenue, must seriously adapt their advertising strategies. Many of the people that I interviewed spoke of the benefit of certainty and the challenges associated with current uncertainty. And this may in fact be one of the reasons to be in favour of a ban, although this was not the sentiment of all those we spoke to. If a total prohibition could be passed in legislation – although it would require significant adaption for many advertisers and publishers the prohibition would produce a new system that could garner strong public support and be subject to less change.

Given the importance of online advertising, being a key source of revenue for many publishers and technology companies, it is vital to consider the implications of any potential ban. A complete ban would do a lot to counter many of the issues raised in Section 3. From stopping the massive breach of our privacy rights, to making it harder to fund disinformation sites, to reducing the national se-

[198] Delli Santo, M. (2020) Belgian DPA fires a warning shot at adtech, what's next?. Open Rights Group. Retrieved from https://www.openrightsgroup.org/blog/belgian-dpa-fires-a-warning-shot-at-adtech-whats-next/

[199] Irish Council for Civil Liberties. (2021). Landmark Litigation. Retrieved from https://www.iccl.ie/rtb-june-2021/

curity risk, the benefits of a ban are considerable when measured against the problems that today's tracking-based advertising causes. It is also important to think about the impact to those involved in buying and selling tracking-based advertising today. It is undeniable that a complete ban would be resisted by many businesses in the sector, although it is also true that we spoke to many people from advertisers, publishers, and adtech companies who would welcome it. Many businesses who have relied on advertising for their revenues are facing challenging times and are fearful that a total ban would prevent them from selling their ad inventory. At the same time, we spoke to businesses who had already moved away from tracking-based advertising and were not just surviving but flourishing.

By looking at the long-term historical data it seems unlikely that a shift away from tracking-based advertising will do much to reduce the overall level of spending on advertising in the economy. This means the key question is how will the adspend be re-distributed. It is very hard to predict how it will be redeployed, as it would depend not only on the legislative environment but also the way that the policy is implemented technically. A poorly implemented contextual platform will never take off. However well-run contextual platforms are flourishing, contextual really does 'work', as IAB put it, and the system can scale. This means there is a system that could, if properly developed, take the load. For many publishers this would be a worrying transition but there are three reasons to think that it need not be so. It offers them a chance to reset their relationship with big tech and adtech companies, to stop giving them access to their users' data, and to start to keep a significantly larger share of each dollar. It also resolves the issue that some publishers had who about the fear of moving away from tracking-based advertising on a unilateral basis.

Just as there are potential positives for publishers the report also finds that advertisers may also find that a total ban is not a problem for their businesses who rely on its effectiveness. We showed that not only are major companies realising that a lot of their spend is actually wasted, as the examples of Uber and eBay show, the prevalence of fraud is so great that for many without sophisticated anti-fraud detection capabilities it is actually very difficult to know what you are getting from the current system. The increased transparency that a contextually driven ad market creates will surely be a welcome change. SMEs will also still be able to access audiences, just as they did 10 years ago prior to tracking-based advertising. Finally, we also find that there is very little systemic risk to big tech and the 'free' services that many rely on every day.

A total ban on the use of personal data in online advertising would bring benefits to individuals and society, would usher in a new world of online advertising with plenty of opportunity for innovation and starting new companies and, most crucially, is technically possible. Only with legislation, though, is that future possible.

© Credits:
Design and development of this campain by
Liesbeth Smit https://www.liesbethsmit.com/

THE GREENS/EFA
in the European Parliament

60 rue Wiertz/Wiertzstraat 60
1047 Brussels, Belgium
www.greens-efa.eu
contactgreens@ep.europa.eu