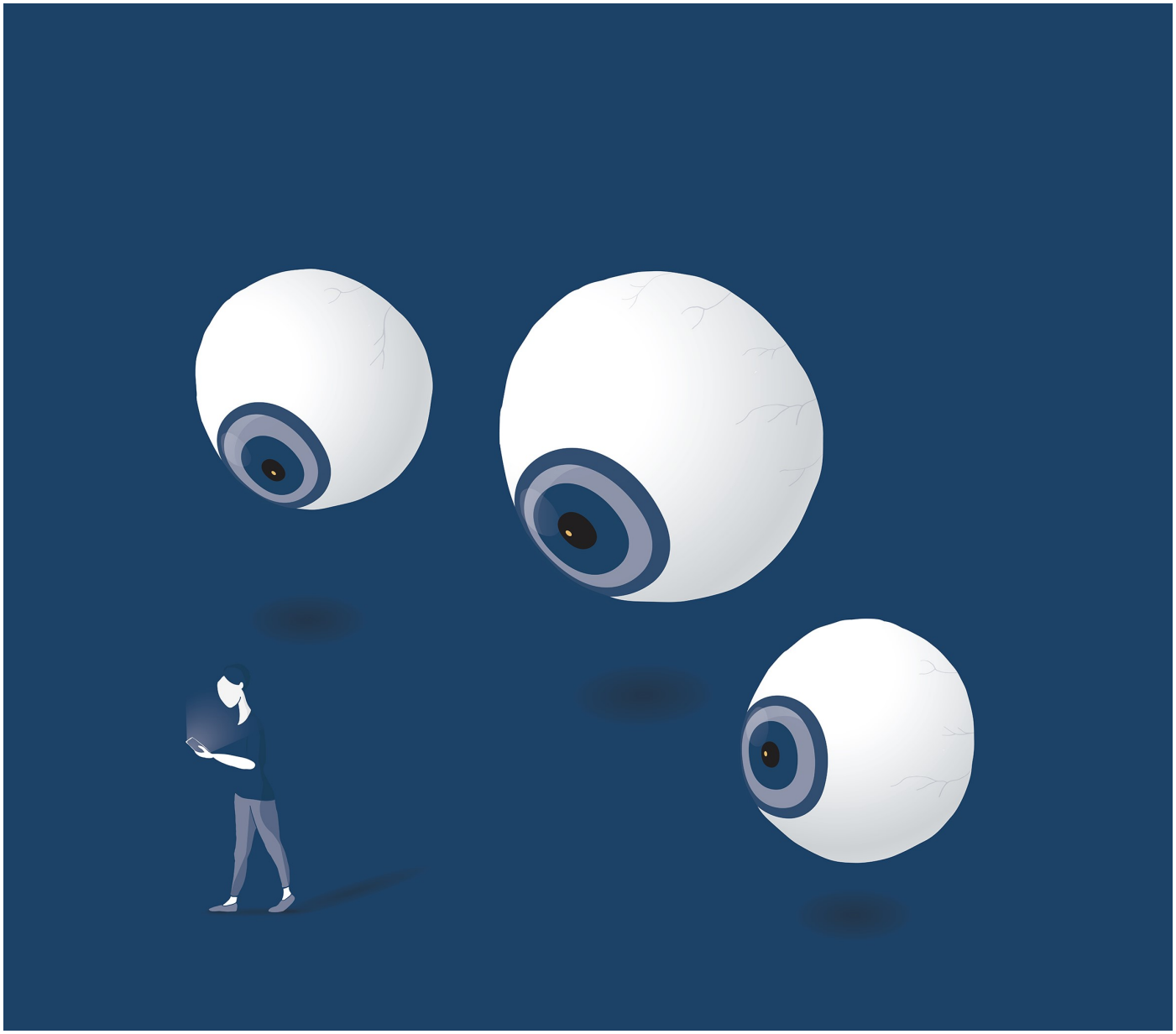

TIME TO BAN SURVEILLANCE-BASED ADVERTISING

The case against commercial surveillance online

June 2021

FORBRUKERRÅDET

Table of contents

1 Summary

Commercial surveillance and exploitation of consumers is now the norm across the internet. As we use various digital services, we are constantly monitored by a large number of commercial actors under the guise of showing us more relevant advertising. It is time to take a step back and consider the problems that this model has created and to imagine a new normal that empowers and protects consumers.

As pervasive commercial surveillance seeps into all aspects of our daily lives, it becomes clear that there is a need for a systemic reform of the online advertising industry. Discussions are currently under way in the European Union about how to handle surveillance-based advertising as a part of the Digital Services Act. At the same time, discussions are going on about enacting federal privacy legislation and legislative initiatives to curb surveillance-based advertising in the United States, where many of the companies engaged in surveillance-based advertising are headquartered. We therefore stand before a unique legislative opportunity to solve many pressing issues.

The result of these discussions could have significant consequences for the business model of the majority of online content, and consumers could stand to benefit from a new preventive approach. This document provides an overview of the challenges of surveillance-based advertising, and can thus be considered a part of these ongoing policy discussions.

It is becoming clear that a majority of consumers do not want to be tracked and profiled for advertising purposes. In a population survey conducted by YouGov on behalf of the Norwegian Consumer Council, just one out of ten respondents were positive to commercial actors collecting personal information about them online, while only one out of five thought that serving ads based on personal information is acceptable. This resembles similar surveys from both sides of the Atlantic, and indicates that consumers do not regard commercial surveillance as an acceptable trade-off for the possibility of seeing tailored ads.

The challenges caused and entrenched by surveillance-based advertising include, but are not limited to:

- privacy and data protection infringements
- opaque business models
- manipulation and discrimination at scale

- fraud and other criminal activity
- serious security risks

In the following chapters, we describe various aspects of these challenges and point out how today's dominant model of online advertising is a threat to consumers, democratic societies, the media, and even to advertisers themselves. These issues are significant and serious enough that we believe that it is time to ban these detrimental practices.

A ban on surveillance-based practices should be complemented by stronger enforcement of existing legislation, including the General Data Protection Regulation, competition regulation, and the Unfair Commercial Practices Directive. However, enforcement currently consumes significant time and resources, and usually happens after the damage has already been done. Banning surveillance-based advertising in general will force structural changes to the advertising industry and alleviate a number of significant harms to consumers and to society at large.

A ban on surveillance-based advertising does not mean that one can no longer finance digital content using advertising. To illustrate this, we describe some possible ways forward for advertising-funded digital content, and point to alternative advertising technologies that may contribute to a safer and healthier digital economy for both consumers and businesses.

2 Introduction

'Surveillance-based advertising', or targeted advertising that is based on tracking and profiling consumers, is the dominant business model online today. This form of marketing uses information about each one of us in attempts to tailor the content of messaging, using factors such as our choice of channel and the point in time we are online to determine when we are most susceptible to behavioural influence.

Surveillance-based advertising has been a driving factor in the growth of the 'surveillance economy' online[1], where personal data is collected, aggregated and sold on through a large network of commercial actors.[2] This is at odds with the fundamental rights to privacy and protection of personal data, is detrimental to consumer protection, and may lead to manipulation and discrimination at scale. It also creates significant security issues due to the accumulation of personal data, and has given rise to a business model that drives a vast amount of disinformation, radicalized content, scams and fraud. The opaque individualization, personalization and microtargeting of advertising also make it difficult to uncover illegal activity and increase consumer vulnerability.

Taken as a whole, the potential boons of surveillance-based advertising seem insignificant compared to the major harms that the surveillance economy has brought. A comprehensive system that entails continuous monitoring of all consumers and that poses serious threats to a number of fundamental rights, with a promise to show potentially more relevant ads online, appears disproportionate. This would be the case even if the accuracy and added value of the surveillance were as high as advertised, which is not the case.

A number of different institutions and civil society organizations have pointed to the major challenges of surveillance-based advertising and to the surveillance economy that underpins the technology.[3] For example, both the European Parliament[4] and the European Data Protection Supervisor[5] have argued that

[1] The 'surveillance economy' is a blanket term for the digital economy based on the monitoring of consumers and commercialization of personal data, and covers processes such as collecting, processing, sharing, buying and selling personal data.
[2] 'Out of Control'. Forbrukerrådet. https://www.forbrukerradet.no/out-of-control/
[3] 'Targeted Online: How Big Tech's business model sells your deepest secrets for profit'. European Digital Rights. https://edri.org/our-work/targeted-online-big-tech-business-model-sells-your-deepest-secrets-for-profit/
[4] 'Digital Services Act: Improving the functioning of the Single Market'. European Parliament resolution. https://www.europarl.europa.eu/doceo/document/TA-9-2020-0272_EN.pdf

surveillance-based advertising should be phased out and, in time, banned. These discussions and challenges are not limited to a European context.

In the United States, for example, a broad coalition of NGOs involved in areas such as consumer rights, gun control, civil rights, child protection and free speech have recently called for a ban on surveillance-based advertising. The coalition cites concerns about issues such as spreading disinformation and extremism, facilitating discrimination, negative effects on public health, and gutting the journalism industry.[6]

As we will examine in depth in the following chapters, there are other forms of digital advertising that are not based on surveillance. This means that it is possible to finance digital content through advertising, even if the use of surveillance-based advertising were brought to a halt.

Every consumer is vulnerable when faced with systems that covertly collect information about us, exploit it, and target us in a way that makes us vulnerable by default[7] and commercializes all online activities. The massive scope of the technology means that consumers have little or no individual scope to protect themselves against massive data collection, profiling and pervasive targeting. The continuous development and proliferation of new technologies, including artificial intelligence and machine learning, means that these issues will only become more pressing as time goes on.

Surveillance-based advertising is harmful to economic sustainability, individuals and society at large. Parallels can be drawn to other areas where bans on certain practices have spurred positive change.

For example, bans and restrictions on advertising for alcohol and tobacco have resulted in positive outcomes in consumer health.[8] The ban on CFC gases in the 1980s had a positive effect on the phasing out of environmentally hazardous materials, and led to innovation in the production of environmentally friendly

---

[5] 'Opinion on the European Commission's proposal for a Digital Services Act'. European Data Protection Supervisor. https://edps.europa.eu/data-protection/our-work/publications/opinions/digital-services-act_en

[6] 'Ban Surveillance Advertising'. https://www.bansurveillanceadvertising.com/

[7] 'EU Consumer Protection 2.0: Structural asymmetries in digital consumer markets'. Natali Helberger, Orla Lynskey, Hans-W. Micklitz, Peter Rott, Marijn Sax, Joanna Strycharz. https://www.beuc.eu/publications/beuc-x-2021-018_eu_consumer_protection.0_0.pdf

[8] 'The effects of tobacco control policies on global smoking prevalence'. Luisa S. Flor, Marissa B. Reitsma, Vinay Gupta, Marie Ng, Emmanuela Gakidou. https://www.nature.com/articles/s41591-020-01210-8

alternative solutions. Similarly, the ban on asbestos in construction led to less hazardous materials being used in its place.

Some of the issues related to surveillance-based advertising are already regulated in the EU through the General Data Protection Regulation (GDPR) and the ePrivacy Directive. However, weak and lax enforcement has meant that the problems these laws sought to address still persist, and notably, the GDPR only addresses challenges that are related to data protection. It is clear that the challenges of surveillance-based advertising go well beyond the area of data protection and privacy.

With this in mind, it is now time to ban surveillance-based advertising. The proposed Digital Services Act, which is currently being discussed by EU legislators, provides an opportunity to do this. Additionally, some of these issues could and should also be addressed in other areas such as consumer law, ePrivacy rules, data protection law, and AI regulation.

3 What is 'surveillance-based advertising'?

All advertising is, to some degree, targeted. The context of an advertisement's placement and its design mean that any advertisement is tailored to, and seen more often by, some consumer groups than by others. This also applies to 'traditional' offline marketing, where advertisers purchase access to certain consumer groups' attention when they decide where they want to place their ads.

In this context, we use the term 'surveillance-based advertising' as a blanket term for digital advertising that is targeted at individuals or consumer segments, usually through tracking and profiling based on personal data. Surveillance-based advertising includes behavioural, personalized, and tailored marketing. In traditional offline marketing, adverts are placed in a pre-determined *context*, for example by purchasing ad space in a motor magazine in order to reach consumers interested in cars. Surveillance-based advertising is different because the advert is *targeted at an individual or group based on characteristics of the individual or group*. The context of *where* the ad is placed can be random because it is targeted *at the consumer* and because the ad can follow the consumer around in different contexts.

The technology promises that, through comprehensive data analysis, an ad may be shown to the 'right individual' at the 'right time', for example by showing an

ad for fast food when it has been calculated you might be feeling peckish, or for cosmetic surgery if you are feeling unattractive. Variations of this technology are also commonly referred to as 'behavioural advertising' 'microtargeting' or 'programmatic advertising'.

In most cases, surveillance-based advertising is shown as part of a fully-automated process, and each individual ad is chosen and placed in a matter of milliseconds. This means that neither the publisher (e.g. the owner of a website or app) nor the advertiser (e.g. the owner of the brand that is promoted) choose which ads to show and where to display them. This is automatically decided by technological systems that are often controlled by third-party middlemen (known as adtech companies).

A large number of these third-party companies are simultaneously collecting large amounts of personal data from consumers in order to create consumer profiles and segments that are used in attempts to target ads more efficiently. Automation of the process allows continuous monitoring and adaptation of the advertising, which also allows advertisers to measure and scale up targeted campaigns in different ways. However, as will be explained below, the use of surveillance-based advertising also poses significant challenges to publishers and advertisers regarding revenue, reputational damage, and opaque supply chains.

3.1 Alternative forms of digital advertising

A common argument in favour of surveillance-based advertising is that a ban will have negative consequences for service and content providers and lead to increased costs for consumers, since most 'free' services online are ad-funded.[9] As will be elaborated upon below, this argument is based on the fallacy that surveillance-based advertising is the only feasible way to fund digital content.

Another argument in favour of allowing surveillance-based advertising is that consumers find targeted ads to be useful and positive. This argument assumes that the only alternative to surveillance-based advertising is to show consumers completely random and irrelevant ads, which would be a nuisance and prevent consumers from receiving interesting offers. This is another flawed premise, as it is not a question of surveillance-based ads on the one hand and arbitrariness on the other.

[9] For an example of this industry argument, see 'What would an internet without targeted ads look like'. Interactive Advertising Bureau Europe. https://iabeurope.eu/knowledge-hub/iab-research-what-would-an-internet-without-targeted-ads-look-like/

Alternative forms of digital advertising already exist, and have proven to be effective sources of income for content providers. These alternative models are also based on targeting messages, but do not entail showing non-contextual ads that have no relevance for consumers.

For example, there are models where consumers who want interest-based advertising can self-report what type of ads they would like to see.[10] With such a model, a consumer could indicate her interest in sports, travel, music or more granular interests and receive ads that are relevant to these issues. This could be done at browser level, and could ensure that ads are relevant to consumer interests without relying on surveillance or tracking.

Another example of alternative forms of digital marketing is 'contextual advertising'. Contextual advertising works by allowing advertisers to purchase ad space on particular types of webpages or websites based on the content on the page.[11] This can be based on keywords so that, for example, ads for flights to England are placed next to articles about English football. In other words, contextual advertising allows advertisers to place ads for particular types of products and services in contexts where the ads will be displayed to consumers interested in particular types of content.

In a sense, contextual advertising may be compared to 'traditional' advertising. Similar to how the advertiser in an offline marketing situation purchases ad space in a magazine for motor enthusiasts to reach that consumer segment, contextual advertising lets the advertiser target ads based on the content of a website or service rather than target them based on characteristics of the consumer. Thus, advertisers can reach relevant audiences without collecting or aggregating personal data. This sidesteps some of the most pressing privacy issues of the marketing, since different actors in the supply chain only need to know where the ad is shown, not necessarily who is seeing it.[12]

This also increases the transparency and verifiability of the marketing, since the advertiser itself chooses what type of content or keywords trigger an ad being

[10] 'What is Vendor Relationship Management?'. Doc Searls. https://www.capgemini.com/2015/08/what-is-vendor-relationship-management/

[11] 'To track or not to track? Towards privacy-friendly and sustainable online advertising'. Karolina Iwanska. https://en.panoptykon.org/privacy-friendly-advertising

[12] There are different types of contextual advertising. Some of these can be partially based on processing personal data and creating user profiles, and may be used to circumvent perceived privacy protection. Throughout this report, we use the term 'contextual advertising' to refer to types of contextual ads that do not depend on tracking and profiling consumers.

shown. This means that many visitors to a particular website or app will see the same advert.

Experiences from certain publishers have shown that removing surveillance-based advertising in favour of contextual advertising has led to increased advertising revenue.[13] For example, the Dutch broadcaster NPO increased advertising revenue by up to 79% after moving to contextual advertising.[14] Furthermore, when The New York Times stopped serving surveillance-based advertising to European users, its advertising revenue kept growing as its advertising partners purchased ad space regardless of the targeting capabilities.[15] Although there is no definitive answer to whether these cases can be replicated by most publishers, it points toward the possibility of alternative revenue models that does not depend on surveillance.

A more transparent supply chain also reduces spending on third parties such as data brokers or verification tools, which means that advertisers and publishers will be left with a larger portion of the revenues. To illustrate this point, a 2020 industry study found that under the current digital advertising regime, only half of advertising spending actually reached publishers, while 15% of the money was unaccounted for.[16]

3.2 First-party and third-party data

There are various forms of surveillance-based advertising, and the potential risks and harms they cause may vary. Some forms of surveillance-based advertising involve transferring vast amounts of personal data to multiple third parties without the consumers' knowledge, creating serious privacy and security risks. This applies to what is typically called advertising based on third-party data.

[13] 'Can Killing Cookies Save Journalism?'. Gilad Edelman. https://www.wired.com/story/can-killing-cookies-save-journalism/
'After GDPR, The New York Times cut off ad exchanges in Europe — and kept growing ad revenue'. Jessica Davies. https://digiday.com/media/gumgumtest-new-york-times-gdpr-cut-off-ad-exchanges-europe-ad-revenue/
[14] 'Update (Six Months of Data): lessons for growing publisher revenue by removing 3rd party tracking'. Johnny Ryan. https://brave.com/publisher-3rd-party-tracking/
[15] 'After GDPR, The New York Times cut off ad exchanges in Europe — and kept growing ad revenue'. Jessica Davies. https://digiday.com/media/gumgumtest-new-york-times-gdpr-cut-off-ad-exchanges-europe-ad-revenue/
[16] ''A' is for ad money oddly gone missing: Probe finds middlemen siphon off half of online advertising spend'. Thomas Claburn. https://www.theregister.com/2020/05/07/ad_tech_fees_sucked/

The scale of data sharing and actors involved in serving surveillance-based advertising based on third-party data is enormous. For example, a single ad exchange may send hundreds of billions of 'bid requests' potentially containing significant amounts of personal data to thousands of companies on a daily basis. In practice, this means that hundreds of trillions of data points are shared with an unknown number of third-party companies every year in what has been described as 'the largest data breach ever recorded'.[17]

Other forms of surveillance-based advertising attempt to curb risks by limiting the sharing of data with third parties. Some actors, particularly the major digital platforms, use personal data they have collected from consumers through their own services.[18] This can be called advertising based on first-party data. The actor collecting the personal data will often have a direct relationship with the consumer, for example in the case where the operator of a social media platform or web browser collects information about its users. Although some could argue this may be less invasive from a privacy perspective since fewer companies can access the data, these types of surveillance-based advertising can entail serious risks related to, for example, manipulation and discrimination, in addition to raising antitrust issues.[19]

Although large companies such as Google and Facebook often rely on first-party data and share less data about consumers with third parties, this arrangement does not cure the problem for consumers. Intrusive profiling still raises issues of privacy, freedom of choice and incentives for manipulation. As 'digital gatekeepers', these companies collect data about consumers across a large number of services, both on their own platforms and across the web. For example, a consumer using an Android mobile device with a Chrome browser as well as Google Maps and Gmail is tracked by Google across these services. This provides opportunities to create highly detailed consumer profiles.[20] Furthermore, in some cases third parties masquerade as first parties in order to circumvent protective measures against third parties.[21] Efforts by some industry

[17] 'Two years on from complaint to the Irish Data Protection Commission, the RTB data breach is the largest ever recorded, and appears to have worsened.'. Johnny Ryan. https://www.iccl.ie/wp-content/uploads/2020/09/1.-Submission-to-Data-Protection-Commissioner.pdf

[18] However, this is often combined with third-party data or data collected through third party platforms, for example through tracking pixels. See for example 'Missed by Filter Lists: Detecting UnknownThird-Party Trackers with Invisible Pixels'. Imane fouad, Nataliia Bielova, Arnaud Legout, Natasa Sarafijanovic-Djukic. https://sciendo.com/article/10.2478/popets-2020-0038

[19] 'Google's FLoC Is a Terrible Idea'. Bennett Cyphers. https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea

[20] 'Online platforms and digital advertising market study'. Competition and Markets Authority. https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study

[21] 'Facebook to release first-party cookie option for ads, pull web analytics from Safari'. Ginny Marvin. https://marketingland.com/facebook-to-release-first-party-pixel-for-ads-web-analytics-from-browsers-like-safari-249478

actors to curb tracking of consumers has led to an arms race by adtech companies in order to avoid being blocked.[22]

Therefore, it is crucial to look at surveillance-based advertising from a holistic point of view – the risks and harmful effects of the technology are not limited to advertising based on third-party data. It is not as simple as third-party data being a problem and first-party data being good.

4 Harmful effects of surveillance-based advertising

Although surveillance-based advertising is sometimes presented as a trade-off, where consumers are happily exposed to targeted advertising in return for 'free' services, this is a shaky premise. While many online services are presented as 'free' to the consumer, revenue is driven by selling consumer attention, illustrated by Google generating USD 40 billion in advertising revenue in the first quarter of 2021.[23]

However, several studies indicate that the majority of consumers are uncomfortable with the collection of personal data.[24] A population survey conducted on behalf of the Norwegian Consumer Council showed that Norwegian consumers are particularly concerned about commercial surveillance.[25] Only one out of ten respondents were positive to commercial actors collecting personal information about them online, while only one out of five thought that serving ads based on personal information is acceptable.

Other research also indicates that consumers often do not want advertising based on personal data, and one study found that only 17% of respondents viewed online tracking for advertising purposes to be ethical.[26] Further supporting this point, a 2021 survey of consumers in Germany and France found that only 11% of respondents were 'fine with [their] personal data being

[22] 'The CNAME of the Game: Large-scale Analysis of DNS-based Tracking Evasion'. Yana Dimova, Gunes Acar, Lukasz Olejnik, Wouter Joosen, Tom Van Goethem. https://petsymposium.org/2021/files/papers/issue3/popets-2021-0053.pdf

[23] 'Alphabet reports big earnings beat as revenue grows 34%'. Jennifer Elias. https://www.cnbc.com/2021/04/27/alphabet-goog-earnings-q1-2021.html

[24] See, for example, 'Nordmenn og deling av persondata'. Norsk Regnesentral. https://www.nr.no/sites/default/files/files/NR-Rapport_Nordmenn-og-deling-av-persondata_ALerT2019.pdf

[25] 'Surveillance-based advertising: Consumer attitudes to surveillance-based advertising'. Norwegian Consumer Council. https://fil.forbrukerradet.no/wp-content/uploads/2021/06/surveilance-marketing-survey.pdf

[26] 'The Dark Side of Customer Data'. RSA. https://www.rsa.com/en-us/company/news/the-dark-side-of-customer-data

used to target [them] with ads'.[27] In the United States, a survey showed that four out of five consumers would support a ban on surveillance-based advertising.[28] In another indicator of consumer preferences, only between 4% and 6% of users chose to accept tracking after Apple introduced an opt-in system for ad tracking in apps.[29]

Although the prospect of ads that monitor your activities may have a significant 'creepy factor', many of the problematic issues related to surveillance-based advertising are 'invisible'. For example, it is impossible for consumers to know what personal data about them is held, how it is processed, transferred or exploited, and by whom. It is impossible for the individual to know why some consumers are excluded from seeing certain ads or messages. Manipulation is most effective when consumers do not know whether or how they are being manipulated, and are often unaware that they are in a vulnerable situation. In the digital environment, every consumer is potentially vulnerable. There are few measures consumers can take to limit these harmful effects, apart from giving up a large amount of useful and important digital services.

For the purpose of this paper, the Norwegian Consumer Council has looked at a number of harmful effects that are either created or exacerbated by surveillance-based advertising. The lack of transparency in the dominant system is an overarching problem and contributes to stronger harmful effects related to privacy breaches, manipulation, and discrimination. These are significant issues that cannot be solved by increased transparency or better information for consumers. Worse still, the lack of transparency and control for business actors in the system has contributed to creating financial incentives and business models for disinformation and fraud on a large scale.

Surveillance-based marketing also has significant harmful effects on business actors. Anti-competitive behaviour and effects serve to entrench dominant actors' positions while complex supply chains and ineffective technologies lead to lost revenues for advertisers and publishers. All of these factors have created a situation where consumers generally have little trust in digital services. A lack of trust means that consumer uptake of new technologies slows down. It is also difficult for consumers to distinguish between 'good' and 'bad' actors in the digital sphere, which means that legitimate actors, amongst them many small and medium sized enterprises, are directly affected by the actions of

[27] 'Do people really want personalised ads online?'. Global Witness. https://www.globalwitness.org/en/blog/do-people-really-want-personalised-ads-online/
[28] 'Accountable Tech Frequency Questionnaire'. Accountable Tech. https://accountabletech.org/wp-content/uploads/Accountable-Tech-Frequency-Questionnaire.pdf
[29] 'iOS 14.5 Opt-in Rate - Daily Updates Since Launch'. Estelle Laziuk. https://www.flurry.com/blog/ios-14-5-opt-in-rate-att-restricted-app-tracking-transparency-worldwide-us-daily-latest-update/

unscrupulous companies. This, in turn, harms both consumers and businesses. All of these issues are explained further in the following sections.

4.1 Lack of transparency

The individualization and personalization of surveillance-based advertising means that different individuals will see different ads based on a number of factors such as time, context, demographics, personal characteristics, etc.[30] A new ad is served for each page visit, and often only to a few individuals at certain points in time. The ads become 'fleeting', with a short and limited lifespan.

The fleeting nature of these ads mean that it is very difficult to verify or control them, in contrast to marketing that is not based on surveillance. In other forms of advertising, for example when an advertiser purchases ad space directly from a publisher such as a newspaper or TV broadcaster, it is simple to return to the medium to control what ad was printed or shown on a TV channel at a particular time.

Advanced algorithmic systems can become so-called 'black boxes', where data is fed into the box and results are extracted, while the reasoning behind the results is opaque. This can obscure the basis of certain decisions, decisive factors and other potentially problematic aspects of the technology. As will be detailed below, this has led to hidden discriminatory practices. Opacity also makes it difficult for supervisory authorities to survey and sanction infringements of the law, which may have downstream consequences for various rights violations that become difficult or impossible to uncover.

The dominant form of surveillance-based advertising makes it practically impossible for consumers to understand why they were shown a particular ad, which segment they have been placed in, and how personal data is shared and used. Even if this information were accessible in any meaningful form, it would be difficult or even impossible for consumers to make use of it due to the technical complexity and the scope of the practice, and because they rarely have a real choice.[31]

[30] The nuances and distinction between individualization and personalization is explored in 'EU Consumer Protection 2.0: Structural asymmetries in digital consumer markets'. Natali Helberger, Orla Lynskey, Hans-W. Micklitz, Peter Rott, Marijn Sax, Joanna Strycharz, p. 94. https://www.beuc.eu/publications/beuc-x-2021-018_eu_consumer_protection.0_0.pdf

[31] '10 Reasons Why Online Advertising is Broken'. Karolina Iwańska. https://medium.com/@ka.iwanska/10-reasons-why-online-advertising-is-broken-d152308f50ec

How will the lack of transparency be solved by a ban?

A ban against surveillance-based advertising would get rid of adverts that are targeted and placed on the basis of data on individual consumers. If this happened, it would be easier to survey and control the ads, as they would no longer be individualized and fleeting. Ad platforms or social media platforms could, for example, more easily establish registries of all the ads they display, making it easier to control content and ensure that contextual targeting is not used improperly to exploit consumer vulnerabilities.[32] This would contribute to more effective enforcement against unfair commercial practices, privacy violations, and more.

4.2 Violations of privacy and data protection

In order to tailor marketing to individuals or groups, and to display 'the right ad to the right person', a large number of companies collect and process vast amounts of information about individual consumers. Data about us is processed every time we use an app, visit a website, shop in a store, or move around in public spaces (e.g. through WiFi tracking).

At the beginning of 2020, the Norwegian Consumer Council published the report *Out of Control* in which we revealed how a large number of companies collect, use, and share personal data about consumers every time they visit apps and websites.[33] This information is aggregated, often by both the owner of the website/app and various third parties. The data is used for purposes related to marketing and personalized services, but can also be used (inadvertently or not) for purposes of discrimination, exclusion and manipulation.

Consumers are constantly manipulated into accepting comprehensive tracking through behavioural techniques or obfuscating design features ('dark patterns'),[34] forced into commercial surveillance systems in order to access necessary services[35], and are generally exposed to data collection without their knowledge and (valid) consent. The enormous amount of data also means that

[32] Such ad registries would have to avoid a number of pitfalls in order to be useful. See for example 'Platform ad archives: promises and pitfalls'. Paddy Leerssen, Jef Ausloos, Brahim Zarouali, Natali Helberger, Claes H. de Vreese. https://policyreview.info/articles/analysis/platform-ad-archives-promises-and-pitfalls

[33] 'Out of Control'. Forbrukerrådet. https://www.forbrukerradet.no/out-of-control/

[34] 'Dark Patterns'. Forbrukerrådet. https://www.forbrukerradet.no/dark-patterns/

[35] 'Offentlige nettsteder sporer oss'. Teknologirådet. https://teknologiradet.no/offentlige-nettsteder-sporer-oss/

attempts to pseudonymize or anonymize the information have proven ineffective.[36]

The scope of data collection and sharing is so vast that it becomes practically impossible to know how personal data may be used. As a consequence, in the context of surveillance-based advertising, it becomes difficult to exercise fundamental rights provided under the Charter of Fundamental Rights of the EU (Charter) and further elaborated in the General Data Protection Regulation (GDPR), including the rights to be informed, have access to, rectify, and delete data or to contest decisions that affect our lives.

How will the risk of violations for privacy and data protection be solved by a ban?

The risks of surveillance-based advertising for privacy and data protection are already largely regulated in Europe through the ePrivacy Directive and the GDPR. After the entry into application of the GDPR in 2018, enforcement of the law has unfortunately been slow and in some cases non-existent, with significant bottlenecks in cross-border enforcement. Simultaneously, there is little indication that the proliferation of the surveillance economy has slowed down despite stronger regulation. This has resulted in a cross-border enforcement gap that needs to be urgently addressed.[37]

A general ban on surveillance-based advertising would be positive for and complement the fundamental rights to privacy and personal data protection that are protected under the Charter, the GDPR and the ePrivacy Directive. Despite the introduction of the GDPR, many actors in the surveillance economy have largely operated under the guise of business as usual, although we have observed that some actors have introduced relatively minor changes in how they ask for consent to process personal data. Others have simply attempted to move to a different legal basis for processing data.[38]

The GDPR cross-border enforcement gap and the emergence of new challenges that go beyond the protection of personal data have shown that there is a need for a more systemic and preventive approach, and a general ban may force overarching structural transformation of surveillance business models.

---

[36] 'Oracle's BlueKai tracks you across the web. That data spilled online'. Zack Whittaker. https://techcrunch.com/2020/06/19/oracle-bluekai-web-tracking/

[37] The GDPR enforcement gap is described in detail in 'The Long and Winding Road: Two years of the GDPR: A cross-border data protection enforcement case from a consumer perspective'. BEUC. https://www.beuc.eu/publications/beuc-x-2020-074_two_years_of_the_gdpr_a_cross-border_data_protection_enforcement_case_from_a_consumer_perspective.pdf

[38] 'Facebook's GDPR bypass reaches Austrian Supreme Court'. Noyb. https://noyb.eu/en/facebooks-gdpr-bypass-reaches-austrian-supreme-court

As a complement to a ban, it is necessary to strengthen relevant enforcement authorities and procedures, both in the GDPR and ePrivacy Directive (or a new ePrivacy Regulation that will replace the Directive[39]) and in the upcoming Digital Services Act.

4.3 Manipulation

The rise of surveillance-based marketing has contributed to the attempted manipulation of individuals and groups on an unprecedented scale. Companies in possession of large amounts of data can use algorithmic systems in attempts to decide when individuals are most susceptible to behave in certain ways or to react to particular images, sounds or messaging.

This may entail, for example, that consumers are exposed to ads for beauty or diet products when their self-confidence is low[40] or that gambling ads are targeted at consumers struggling with addictions.[41] These issues are exacerbated by the proliferation of marketing of harmful products and services to children.[42] Automation makes the process even more opaque, and the optimization of messaging may have negative effects if unethical and harmful yet effective methods are automated.

Advertising can exploit consumer vulnerabilities even without directly observing the said vulnerabilities. For example, through the use of so-called 'lookalike audiences', advertisers can duplicate consumer groups with certain characteristics in order to reach new consumers who share the same characteristics.[43] In this way, advertising for pharmaceuticals may, for example, be shown to groups of consumers that have characteristics in common with other consumers with similar ailments, even though the advertiser has no

[39] 'Shaping Europe's Digital Future. Proposal for ePrivacy Regulation'. European Commission. https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation
[40] 'Facebook told advertisers it can identify teens feeling "insecure" and "worthless"'. Sam Levin. https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens
[41] 'What a Gambling App Knows About You'. Adam Satariano. https://www.nytimes.com/2021/03/24/technology/gambling-apps-tracking.html
[42] 'Facebook allows advertisers to target children interested in smoking, alcohol and weight loss'. Josh Taylor. https://www.theguardian.com/technology/2021/apr/28/facebook-allows-advertisers-to-target-children-interested-in-smoking-alcohol-and-weight-loss
[43] 'About Lookalike Audiences'. Facebook. https://www.facebook.com/business/help/164749007013531?id=401668390442328

information that directly indicates the health status of these consumers.[44] Similarly, this form of targeting has been linked to radicalization.[45]

Through surveillance-based advertising, all consumers are rendered vulnerable by default; in theory we can be targeted in our most vulnerable moments in order to optimize the effects of the marketing.[46] The constant bombardment of advertising across digital spaces also serves to break down ingrained defences against persuasion and manipulation.[47] This becomes particularly harmful when children and other especially susceptible groups are subjected to manipulation and extreme commercialization.[48]

How will the risk of manipulation be solved by a ban?

A general ban on surveillance-based advertising will not solve all issues related to manipulative marketing, as all marketing can potentially be used to manipulate consumers. Despite this, a ban on surveillance-based advertising will contribute to putting an end to individualized ads that are optimized to reach consumers in vulnerable situations, as well as mitigate the effects of ongoing 'vulnerability by default' created through application of constantly improved persuasion profiles.

Manipulation that happens through other forms of advertising, such as content marketing[49], must be solved through means other than a ban on surveillance-based advertising, such as through provisions in the Digital Services Act[50] and a revised Unfair Commercial Practices Directive.

---

[44] 'How Big Pharma Finds Sick Users on Facebook'. Colin Lecher. https://themarkup.org/citizen-browser/2021/05/06/how-big-pharma-finds-sick-users-on-facebook

[45] 'Despite A Ban, Facebook Continued To Label People As Interested In Militias For Advertisers'. Ryan Mac. https://www.buzzfeednews.com/article/ryanmac/facebook-militia-interest-category-advertisers-ban

[46] For more on the need for new and updated conceptions of consumer vulnerability, see 'EU Consumer Protection 2.0: Structural asymmetries in digital consumer markets'. Natali Helberger, Orla Lynskey, Hans-W. Micklitz, Peter Rott, Marijn Sax, Joanna Strycharz. https://www.beuc.eu/publications/beuc-x-2021-018_eu_consumer_protection.0_0.pdf

[47] 'WTF is dark pattern design?'. Natasha Lomas. https://techcrunch.com/2018/07/01/wtf-is-dark-pattern-design/

[48] For more on the adverse effects of digital marketing on children, see 'Big Food, Big Tech, and the Global Childhood Obesity Pandemic'. Jeff Chester, Kathryn C. Montgomery, Katharina Kopp. https://www.democraticmedia.org/article/big-food-big-tech-and-global-childhood-obesity-pandemic

[49] Content marketing includes sponsored content in online newspapers, influence marketing, and other paid promotional content.

[50] 'The Digital Services Act Proposal – BEUC Position Paper'. BEUC. https://www.beuc.eu/publications/beuc-x-2021-032_the_digital_services_act_proposal.pdf

4.4 Discrimination

In addition to creating new opportunities to reach 'the right person', surveillance-based advertising creates new opportunities to exclude and discriminate against individuals and groups.[51] The automation of advertising enables this on an increasing scale. For example, Amnesty International has described the surveillance-based business model of companies such as Google and Facebook as a threat to a number of fundamental human rights, including freedom of speech and the right to non-discrimination, due to how the surveillance business model creates chilling effects and sorts individuals into groups for targeting purposes.[52]

Segmentation and targeting can be used to *not display* certain ads to particular people or consumer groups. For example, advertisers can choose to show housing ads only to people who fit their ideal profile for individuals they want to have living in a certain neighbourhood and exclude 'undesirable' individuals who may nonetheless be able to afford living there. Similarly, potential employers can choose what kinds of people are shown certain job listings, which may for example exclude potential female candidates, either deliberately or through algorithmic discrimination.[53] In fact, any such choices will necessarily exclude some individuals or groups.[54] This is exacerbated by the level of opacity and the impossibility of knowing who is seeing what ad.

It is impossible for consumers to know what job listing or housing ad they are *not seeing*. While traditional marketing can be observed by looking up the content and analysing it in retrospect, this is often unfeasible if the ad was only shown to one particular consumer or group at a certain point in time. If discrimination is happening as part of automated algorithmic processes, it becomes very difficult to uncover and remedy the issue. Thus surveillance-based advertising may contribute to obscure discriminatory or exclusionary practices because the problematic issues happen inside the 'black box'. This undermines the right to non-discrimination, which is a fundamental human right.

---

[51] For a detailed analysis of discrimination in surveillance-based advertising, see 'How online ads discriminate'. Frederike Kaltheuner. https://edri.org/our-work/how-online-ads-discriminate/

[52] 'Facebook and Google's pervasive surveillance poses an unprecedented danger to human rights'. Amnesty International. https://www.amnesty.org/en/latest/news/2019/11/google-facebook-surveillance-privacy/

[53] 'Facebook's ad algorithms are still excluding women from seeing jobs'. Karen Hao. https://www.technologyreview.com/2021/04/09/1022217/facebook-ad-algorithm-sex-discrimination/

[54] 'Credit Card Ads Were Targeted by Age, Violating Facebook's Anti-Discrimination Policy'. Corin Faife and Alfred Ng. https://themarkup.org/citizen-browser/2021/04/29/credit-card-ads-were-targeted-by-age-violating-facebooks-anti-discrimination-policy

These forms of discrimination and exclusion are not necessarily due to a deliberate act of malice on the part of the advertiser; algorithms optimizing the ads may be automatically facilitating problematic practices.[55] This may lead to automated discrimination, for example by making geolocation a proxy for protected attributes such as ethnicity, sexual orientation or religious beliefs, because statistic models show that some groups of people have overlapping attributes.[56]

In other words, even if a system explicitly disallows targeting consumers based on religious beliefs, the fact that an individual regularly visits the geolocation of a mosque or uses a certain prayer app may be used as a proxy for the attribute 'Muslim'.[57] This type of automation continuously risks creating new proxy attributes as the system evolves and decides which individuals should see what adverts.

The segmentation of consumer groups may also lead to individualized pricing of goods and services. This form of price discrimination may lead to unfair differentiation between consumers, make it difficult to compare prices, and make consumers reluctant to compare prices because it may affect the final price of the product or service.[58]

How would discriminatory practices be solved by a ban?

A general ban on surveillance-based advertising would make it easier to survey and sanction discriminatory and exclusionary marketing practices. This would contribute to an advertising market where discriminatory practices are more effectively sanctioned, which would help protect consumers' fundamental rights.[59]

---

[55] 'Discrimination through optimization: How Facebook's ad delivery can lead to skewed outcomes'. Muhammad Ali, Piotr Sapiezynski, Miranda Bogen, Aleksandra Korolova, Alan Mislove and Aaron Rieke. https://arxiv.org/abs/1904.02095

[56] 'Facebook (Still) Letting Housing Advertisers Exclude Users by Race'. Julia Angwin, Ariana Tobin and Madeleine Varner. https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin

[57] 'Leaked Location Data Shows Another Muslim Prayer App Tracking Users'. Joseph Cox. https://www.vice.com/en/article/xgz4n3/muslim-app-location-data-salaat-first

[58] 'Cookie monsters: why your browsing history could mean rip-off prices'. Arwa Mahdavi. https://www.theguardian.com/commentisfree/2016/dec/06/cookie-monsters-why-your-browsing-history-could-mean-rip-off-prices

[59] In order to constrain discriminatory practices through proxy attributes, restrictions on what categories or segments that can be used in marketing should be considered. For example, marketing to groups based on assumed health factors, or based on granular geolocation could be banned.

4.5 Disinformation

The lack of transparency in large parts of the surveillance-based advertising industry means that many advertisers do not know where their ads are being displayed. This creates reputational damage for brands and advertisers, as they lose control over whether their ads are displayed in conjunction with disinformation or otherwise problematic content.

The risk of reputational damage has led to some categories of websites or keywords being 'blacklisted', which has created new issues for serious content producers and publishers.[60] For example, this caused major problems and vast revenue losses for many publishers when a number of advertisers did not wish to place their ads on websites writing about COVID-19.[61] Similar practices have damaged publishers creating content for minorities and potentially vulnerable groups, for example through keywords related to LGBTQ+ being blacklisted.[62] This involves money being diverted from reputable publishers in favour of less reputable sources. Consequently, low quality content is incentivized, creating opportunities for fraud and scams.

Controversial content has been proven to create a high degree of engagement, leading many people to click on links to articles or content that are misleading or patently false.[63] This leads to advertising revenue for the actors creating and spreading such disinformation, meaning that surveillance-based advertising offers financial incentives to create such content.[64] The use of surveillance-based advertising is one, by not the only, business model incentivizing the creation and spreading of disinformation online.[65] Furthermore, the technology behind surveillance-based advertising can be used to spread disinformation, with potentially devastating effects on individuals and society.[66]

---

[60] 'The future of data-driven marketing'. World Federation of Advertisers. https://wfanet.org/knowledge/item/2021/03/10/WFA-report-The-future-of-data-driven-marketing

[61] 'Covid-19 heats up the race to combat advertising's keyword blocking problem'. Rebecca Stewart. https://www.thedrum.com/news/2020/04/30/covid-19-heats-up-the-race-combat-advertising-s-keyword-blocking-problem

[62] 'Vice slams brand safety keyword blacklists after alarming probe'. Oliver McAteer. https://www.campaignlive.com/article/vice-slams-brand-safety-keyword-blacklists-alarming-probe/1495610

[63] The Disinformation Index. https://disinformationindex.org/

[64] 'Targeted ads are one of the world's most destructive trends. Here's why'. Arwa Mahdavi. https://www.theguardian.com/world/2019/nov/05/targeted-ads-fake-news-clickbait-surveillance-capitalism-data-mining-democracy

[65] 'How the Adtech Market Incentivizes Profit-Driven Disinformation'. Joshua Braun. https://promarket.org/how-the-adtech-market-incentivizes-profit-driven-disinformation/

[66] 'Facebook Said It Would Stop Recommending Anti-Vaccine Groups. It Didn't'. Corin Faife and Dara Kerr. https://themarkup.org/citizen-browser/2021/05/20/facebook-said-it-would-stop-recommending-anti-vaccine-groups-it-didnt

How will the prevalence of disinformation online be solved by a ban?

A ban on surveillance-based advertising will not be a perfect remedy for the prevalence of disinformation online. However, a general ban will disrupt the business models of a large number of websites and other actors that create and spread disinformation.

A more transparent supply chain will make it easier for advertisers to know where their ads are displayed. This means that brands can have more control over whether their ads are used to fund disinformation. A ban should nevertheless be complemented by consistent and strong enforcement of data protection, competition and consumer law.[67]

4.6 Anti-competitive effects

In the surveillance-based advertising model, a few actors can obtain competitive advantages by collecting data from across websites and services.[68] The increasing concentration of the digital advertising market is diminishing the value of publishers' first-party data and creating a race to the bottom. In practice, adtech companies can collect data about consumers on one website (e.g. an online newspaper), combine it with the data they have about that user within its own services (e.g. social media) and then use the data to target ads toward those consumers on other websites that offer a lower price for ad placements.[69]

Even though ad revenue from surveillance-based advertising has grown during the past few years, most of the revenue went to only a few platforms.[70] Platforms such as Google and Facebook are estimated to account for about two-thirds of the digital ad market in the United States[71] and around 80% in the

[67] 'What is the link between behavioural advertising and fake news?'. BEUC. https://www.beuc.eu/publications/beuc-x-2018-036_what_is_the_relation_between_behavioural_advertising_and_fake_news.pdf
[68] 'Google stymies media companies from chipping away at its data dominance'. Paresh Dave. https://www.reuters.com/article/tech-antitrust-google-idINKBN2410ZD
[69] 'Lousy ads are ruining the online experience'. Walt Mossberg. https://www.theverge.com/2017/1/18/14304276/walt-mossberg-online-ads-bad-business
[70] 'Google's digital ad dominance is harming marketers and publishers, says new study'. Ad Age. https://adage.com/article/digital/googles-digital-ad-dominance-harming-marketers-and-publishers-says-new-study/2257576
[71] 'Google, Facebook, and Amazon will account for nearly two-thirds of total US digital ad spending this year'. Mariel Soto Reyes. https://www.businessinsider.com/google-facebook-amazon-were-biggest-ad-revenue-winners-this-year-2020-12

UK.[72] This means that money has been moved away from publishers and potential competitors.

Dominant actors can abuse their positions in the digital advertising market by giving preference to their own services.[73] For example, Google controls many aspects of the value chain, and operates as both a buyer, seller and marketplace.[74] If Google manipulates its tools to favour its own online ad services and to stifle competition from rival technologies, these anti-competitive effects would not only harm potential competitors but also lead to less choice and higher prices for consumers.[75]

These anti-competitive effects may be further entrenched if the dominant platforms move away from using and enabling the collection of third-party data. Even if such measures limited the number of actors that can access personal data, which would be positive from a privacy perspective, it may also contribute to a small number of dominant actors further entrenching their position as gatekeepers.[76]

In today's situation, it is difficult for alternative business models of digital advertising to compete with the dominant actors. This has many causes, including network effects, anti-competitive behaviour from dominant players,[77] and because most advertisers already rely on surveillance-based advertising as their main revenue stream for free content.[78] Furthermore, many technical solutions tied to surveillance-based advertising solutions may be incompatible with models that do not rely on processing personal data.

How will the anti-competitive effects be solved by a ban?

---

[72] 'Online platforms and digital advertising market study'. Competition and Markets Authority. https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study#final-report

[73] 'Algorithms: How they can reduce competition and harm consumers'. Competition and Markets Authority. https://www.gov.uk/government/publications/algorithms-how-they-can-reduce-competition-and-harm-consumers

[74] 'Lack of competition in ad tech affecting publishers, advertisers and consumers'. Australian Competition and Consumer Commission. https://www.accc.gov.au/media-release/lack-of-competition-in-ad-tech-affecting-publishers-advertisers-and-consumers

[75] In 2021, the French competition authority fined Google € 220 for promoting its own advertising services over its rivals. .' Google fined €220m in France over advertising abuse'. Simon Read. https://www.bbc.com/news/business-57383867

[76] '4 Big Questions about Google's new privacy position'. Johnny Ryan. https://www.iccl.ie/digital-data/4-big-questions-about-googles-new-privacy-position/

[77] 'Google's advertising practices targeted by EU antitrust probe'. EURACTIV. https://www.euractiv.com/section/digital/news/googles-advertising-practices-targeted-by-eu-antitrust-probe/

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

A general ban on surveillance-based advertising could contribute to levelling the playing field between publishers and dominant platforms, which would stimulate a better competitive market for advertising. However, the dominant positions of Facebook and Google must also be addressed by other means, particularly through enforcement of antitrust regulation. Any regulatory intervention must be complemented with enforcement of competition law at the level of anti-competitive agreements (e.g. between different players in the advertising supply chain) and to prevent the abuse of dominant positions.

A ban on surveillance-based advertising could also serve consumers by contributing to greater freedom of choice and media plurality, and lay the ground for new innovation.

4.7 Fraud and lost revenue

Although proponents of surveillance-based advertising sometimes touts the ability to measure ad efficiency, such measurements are not necessarily accurate. Ad fraud is a widespread problem across the industry, which has been shown to heavily inflate the number of ad views and clicks. The automation and scale of the marketing, and the sheer number of middlemen, mean that there is very little transparency around where ads are shown, how many consumers are actually exposed to the ads, and where the money spent ends up.[79]

This lack of control also means that consumers can easily be exposed to fraud and scams through targeted ads.[80] This leads to consumers being harmed, financially and otherwise, and to reputational damage for publishers who end up hosting criminal ads.[81]

The complicated network of actors in the surveillance-based advertising industry has led to many advertisers and publishers having a limited overview of where their ad spend is going, which in turn has spawned a large industry based on ad fraud.[82] This kind of fraud is commonly committed by having ads shown to bots instead of humans, which in turn reduces the price that publishers can claim for ad space and makes advertisers pay for ads which no consumer is

[79] 'Ad Tech Could Be the Next Internet Bubble'. Gilad Edelman. https://www.wired.com/story/ad-tech-could-be-the-next-internet-bubble/
[80] 'Fake ads; real problems: how easy is it to post scam adverts on Facebook and Google?'. Andrew Laughlin. https://www.which.co.uk/news/2020/07/fake-ads-real-problems-how-easy-is-it-to-post-scam-adverts-on-google-and-facebook/
[81] 'AI & Advertising, a consumer perspective'. Harriet Kingaby. https://www.harrietkingaby.com/reports
[82] 'Report: Ad Fraud to hit $23 billion, isn't going down'. George P. Slefo. https://adage.com/article/digital/report-ad-fraud-hit-23-billion-isnt-going-down/2174721

actually seeing.[83] In other words, legitimate actors end up paying for advertising that never reaches an audience at all.

The use of middlemen has led to large amounts of advertising revenue going to third parties.[84] This means, for example, that money which otherwise would have reached a local newspaper is being gobbled up by third-party actors, and in some cases cannot be traced.[85] This has given rise to questions about whether surveillance-based advertising is financially sustainable for publishers.[86]

The rise of ad fraud has led to the emergence of a large market for fraud detection tools. This is technology that is used to verify that ads have been shown to actual human beings. There are different ways to do this, but these methods often involve collecting more information about consumers.[87] The development of such tools is a constant arms race against the fraudsters, which leads to increased costs for advertisers and to further privacy violations against consumers.

Similar tools are also used to track the number of ads shown to determine what the advertiser has to pay for the ad placement. Such numbers have been shown to be inaccurate or outright false, which may have serious consequences for businesses.[88] Other tools that are meant to prevent ad fraud and provide advertisers with security have also been found to have significant flaws.[89] The fight against ad fraud has turned into a negative spiral where advertisers, as well as publishers and consumers, are all losers.

How will issues related to fraud be solved by a ban?

---

[83] 'The Cost-Performance Paradox Of Modern Digital Marketing'. Augustine Fou. https://www.forbes.com/sites/augustinefou/2020/08/18/the-cost-performance-paradox-of-modern-digital-marketing/

[84] 'In Digital, 'Wanamaker's 50%' Is Known. It's Also Worse Than That.'. Augustine Fou. https://www.forbes.com/sites/augustinefou/2020/12/19/in-digital-wanamakers-50-is-known-its-also-worse-than-that/

[85] 'Time for change and transparency in programmatic advertising'. ISBA. https://www.isba.org.uk/article/time-change-and-transparency-programmatic-advertising

[86] 'Behavioral Ad Targeting Not Paying Off for Publishers, Study Suggests'. Keach Hagey. https://www.wsj.com/articles/behavioral-ad-targeting-not-paying-off-for-publishers-study-suggests-11559167195

[87] For example, the data broker Tamoco claims to use location data to detect ad fraud. 'What Is Ad Fraud? How Location Data Can Detect Ad Fraud'. Tamoco. https://www.tamoco.com/blog/location-digital-ad-fraud-detection/

[88] 'Facebook knew for years ad reach estimates were based on 'wrong data' but blocked fixes over revenue impact, per court filing'. Natasha Lomas. https://techcrunch.com/2021/02/18/facebook-knew-for-years-ad-reach-estimates-were-based-on-wrong-data-but-blocked-fixes-over-revenue-impact-per-court-filing/

[89] 'Breitbart.com is Partnering with RT.com & Other Sites via Mislabeled Advertising Inventory'. Zach Edwards. https://medium.com/@thezedwards/breitbart-com-is-partnering-with-rt-com-other-sites-via-mislabeled-advertising-inventory-6e7e3b5c3318

A general ban on surveillance-based advertising would lead to more transparency in the supply chain and likely reduce the amount of ad fraud. This would in turn diminish the need for costly and invasive fraud detection tools, which would be a boon to publishers' and advertisers' bottom lines as well as to consumer privacy and security. A ban should be complemented by other measures to reduce fraud, such as obligations on online marketplaces to verify traders' legitimacy, as proposed in the Digital Services Act.

4.8 Security risks

As many systems used in surveillance-based advertising involve data being shared and spread amongst potentially thousands of actors, there is a significant risk that at least one of these actors seize the opportunity to sell or share data sets to other companies that have business models outside of advertising.[90]

In these systems, there is no real distinction between 'regular' consumers and individuals in critical roles. For example, the Norwegian public broadcaster NRK has revealed how personal data collected from popular apps could be used to track the movement of military personnel.[91] In a 2021 report, NATO announced that this form of collection and sharing of personal data constitutes a serious threat to national security.[92]

The collection and storage of information also create a risk of personal data being spread as a result of hacking or data breaches. This means that criminals may be able to access information that can be used for identity theft, fraud, and blackmailing purposes. Data that has been leaked can also be misused to identify, track down and harm vulnerable individuals and groups[93] or in attempts to influence or interfere in democratic elections.

[90] 'Telefonen spionerte på meg. Slik fant jeg overvåkerne'. Martin Gundersen. https://nrkbeta.no/2020/12/03/telefonen-spionerte-pa-meg-slik-fant-jeg-overvakerne/
[91] 'Når mobilen blir fienden'. Martin Gundersen, Øyvind Bye Skille, Henrik Lied, Mari Grafsrønningen, Harald K.Jansson. https://www.nrk.no/norge/xl/norske-offiserer-og-soldater-avslort-av-mobilen-1.14890424
[92] 'Data Brokers and Security'. NATO STRATCOM. https://stratcomcoe.org/publications/data-brokers-and-security/17
[93] 'Egyptian police 'are using Grindr to find and arrest LGBT people''. Matt Payton. https://www.independent.co.uk/news/world/africa/egyptian-police-grindr-dating-app-arrest-lgbt-gay-anti-gay-lesbian-homophobia-a7211881.html

In addition to data breaches leading to security risks, digital advertising has become a vector for the spread of malicious code such as malware or viruses.[94] This means that some advertising banners may include scripts that infect the consumer's device, which can lead to hackers accessing the device, damaging the device or otherwise interfering with device operations.

How will security risks be solved by a ban?

A general ban on surveillance-based advertising would throttle large parts of the data flow and collection of personal data. This would help scale down the potential for security breaches and misuse of this data. Simply put, if the data is not collected or stored, it cannot be used to harm consumers or institutions.

4.9 Lack of trust

Although issues regarding violations of privacy and security online have received significant public attention in the past few years, consumers are often left with few alternatives but to continue using the problematic services. Some platforms have no competitors, which means that consumers cannot switch to a different service even if they would like to. In other cases, the complexity and scale of the problematic practices are so vast that consumers cannot realistically understand the harms, protect themselves or take preventive action. This leads to disillusionment, fatigue, and a lack of trust in digital service providers, impacting the digital economy beyond advertising.[95]

Although most consumers have few or even no ways to protect themselves against commercial surveillance online, and cannot be expected to take action, a lack of trust in digital services has been an important factor in the rise of tracking and blocking tools. Such tools are used by many consumers, and are pre-installed on several popular web browsers such as Safari, Firefox and Brave. Although this strengthens consumer protection, it also means that ads from legitimate actors are blocked, which leads to both advertisers and publishers losing revenue.

All of these choices presuppose that the consumer has an unrealistic level of power, technological and legal competence. If the consumer were to make a truly informed choice, she would have to spend hundreds of hours every year

[94] 'Protect Yourself From Ad Threats And 'Malvertising''. Michelle Drolet. https://www.forbes.com/sites/forbestechcouncil/2020/02/03/protect-yourself-from-ad-threats-and-malvertising/
[95] 'Deloitte Global Mobile Consumer Survey 2019: The Nordic cut'. Deloitte. https://www2.deloitte.com/no/no/pages/technology-media-and-telecommunications/topics/global-mobile-consumer-survey.html

reading legal documentation and combat dark patterns designed to influence her autonomy, decisions and choices.

The use of dark patterns to nudge consumers into accepting tracking further shifts the balance of information and power to the disadvantage of the consumer.[96] The sum of these practices means that consumers are constantly asked to make choices which they have no practical or realistic way of controlling, understanding or relating to. This absurd situation also contributes to a lack of trust in digital services.

Due to the opaque supply chains of surveillance-based advertising systems, it is also difficult for advertisers to have control of where their ads are displayed. This has led to a large number of cases where ads are displayed next to and used to finance extreme or hateful content, leading to negative brand associations.[97]

Furthermore, the general lack of trust may reduce the spread and uptake of useful services, and have a negative effect on companies who take privacy and security seriously.[98] This can have serious chilling effects on consumer behaviour, which may prevent consumers from using important services related to mental health[99] or seeking help through public services.[100]

Consumers have few ways to distinguish between serious and unserious actors in the digital space, which is likely to negatively impact small and medium sized-enterprises wanting to compete on factors such as development of privacy preserving technologies.

How will the lack of trust in digital services be solved by a ban?

A general ban on surveillance-based advertising will not be a cure-all to restore trust in digital services. The scandals are too numerous, and have taken place

[96] 'Deceived by Design: How tech companies use dark patterns to discourage us from exercising our rights to privacy'. Forbrukerrådet. https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/

[97] 'Google's bad week: YouTube loses millions as advertising row reaches US'. Olivia Solon. https://www.theguardian.com/technology/2017/mar/25/google-youtube-advertising-extremist-content-att-verizon

[98] See, for example, the European Commission's white paper 'On Artificial Intelligence - A European approach to excellence and trust'. https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

[99] 'Your mental health for sale'. Privacy International. https://www.privacyinternational.org/campaigns/your-mental-health-sale

[100] 'Surveillance on UK council websites'. Johnny Ryan. https://brave.com/ukcouncilsreport/

repeatedly over a long period. It will take time to restore trust. However, a ban would contribute to a level playing field where ad revenues would to a greater extent reach serious actors. This may contribute to consumers no longer feeling as if service providers and brands are looking over their shoulder online and being treated as commodities that are sold to the highest bidder. It may also restore trust by reassuring consumers that brands are not sponsoring hateful content.

4.10 Inefficient technology

It is contested whether, in addition to creating and exacerbating a number of serious problems, the technology behind surveillance-based advertising is actually effective as a marketing tool. Even though innovation in areas such as artificial intelligence is often presented as revolutionary for the advertising industry, it is worth questioning whether the marketing effects of the technology are being oversold.[101] This is exemplified by studies showing that surveillance-based advertising have in many cases had no beneficial effects on conversion rates or publisher revenues.[102]

Studies have shown that companies that sell advertising technology are significantly exaggerating the effectiveness of the technology and that the actual targeting is far from accurate.[103] Although profiling based on data collection may be accurate in certain circumstances, in other cases the inferences drawn can be inaccurate or flat out wrong.[104]

There are also challenges related to advertisers reaching consumers who were already planning on purchasing or who have already purchased the product being advertised. It can be difficult or even impossible for an advertiser to distinguish between a sale made because of an ad or whether the ad was displayed to a consumer who would have made the purchase regardless.[105] Furthermore, online advertising is often dependent on consumers actually

---

[101] 'The new dot com bubble is here: it's called online advertising'. Jesse Frederik, Maurits Martijn. https://thecorrespondent.com/100/the-new-dot-com-bubble-is-here-its-called-online-advertising/13228924500-22d5fd24

[102] 'Digiday Research: Most publishers don't benefit from behavioral ad targeting'. Mark Weiss. https://digiday.com/media/digiday-research-most-publishers-dont-benefit-from-behavioral-ad-targeting/

[103] 'Frontiers: How Effective Is Third-Party Consumer Profiling? Evidence from Field Studies'. Nico Neumann, Catherine E. Tucker, Timothy Whitfield. https://pubsonline.informs.org/doi/pdf/10.1287/mksc.2019.1188

[104] 'I asked an online tracking company for all of my data and here's what I found'. Privacy International. https://privacyinternational.org/long-read/2433/i-asked-online-tracking-company-all-my-data-and-heres-what-i-found

[105] 'Overvurdering av digital reklameeffekt'. CPM Analytics. https://www.cpm.no/wp-content/uploads/2019/06/Overvurdering-av-digital-reklameeffekt-PDF-28062019.pdf

clicking on the ads, and the sheer volume of advertising may lead to most marketing material turning into background noise.[106]

Although a large portion of digital advertising technologies may have limited effects, this does not mean that decisions based on bad technology will be better for consumers than decisions based on accurate technology. The inaccuracy of technology is not a mitigating factor if consumers are subjected to discrimination, manipulation or exclusion.

There are also serious inefficiencies in computing power and the energy usage of surveillance-based advertising. Although the energy consumption of data centres is not a problem unique to advertising, studies have shown that digital advertising technologies have significant carbon footprints.[107] The environmental impact of surveillance-based advertising is exacerbated by the use of artificial intelligence and the prevalence of bots used for ad fraud.[108]

How will the inefficient technology be solved by a ban?

A general ban on surveillance-based advertising will limit the opportunities to sell 'snake oil' technologies that promise far more than they can deliver to advertisers and publishers. This can reduce revenue loss for advertisers and publisher and help protect consumers against decisions based on faulty technologies and assumptions.

The environmental impact of surveillance-based advertising may curb some of the excessive carbon footprint, but other complementary measures are necessary in order to handle the emission levels of data centres and artificial intelligence.

5 Current legislation

As outlined above, a ban on surveillance-based advertising is not a cure-all solution. Digital services are already subject to a number of rules and regulations in the EU, and a ban would be complementary to the existing legal framework. In the following section, existing European data protection and

[106] 'Banner Blindness Revisited: Users Dodge Ads on Mobile and Desktop'. Kara Pernice. https://www.nngroup.com/articles/banner-blindness-old-and-new-findings/
[107] 'Environmental impact assessment of online advertising' M. Pärssinena, M.Kotilab, R.Cuevasc, A.Phansalkard, J.Mannere. https://www.sciencedirect.com/science/article/pii/S0195925517303505
[108] 'AI & Advertising, a consumer perspective'. Harriet Kingaby. https://www.harrietkingaby.com/reports

consumer law is assessed in relation to the harms stemming from surveillance-based advertising.

5.1 EU privacy and data protection law

The General Data Protection Regulation (GDPR) regulates the processing of personal data. The protection of personal data is regarded as a fundamental human right, and the GDPR primarily aims to give individuals control over their personal data and prohibit the processing of personal data without a valid legal basis. As a general rule, the use of personal data for profiling and tracking, especially when this involves onward sharing of personal data, requires a valid consent.[109] This has also been affirmed by European data protection authorities.[110]

The work done by the Norwegian Consumer Council in the field of digital advertising shows that the surveillance-based advertising industry operates in ways that involve illegal collection, sharing and use of personal. These practices are widespread and complicated to understand, even for experts. The sum of these practices is that all consumers become vulnerable by default in the face of surveillance-based advertising. It is therefore unreasonable to claim that consumers understand what they are consenting to if they accept tracking and profiling for advertising purposes. If this is the case, the processing of personal data for surveillance-based advertising purposes has proven in most cases not to be compliant with the GDPR. This was further affirmed by the Norwegian Data Protection Authority (*Datatilsynet*) when it announced its intention to fine the dating app Grindr for processing personal data for advertising purposes.[111]

Even if the GDPR is adequate to address a number of privacy-related issues regarding surveillance-based advertising, the regulation is limited to cases where personal data is being processed.

As shown above, many of the potential harms of surveillance-based advertising endure even if personal data is not transferred from the end user's device. In these cases, both the GDPR and the ePrivacy Directive may be insufficient to deal with the problems. Hence complementary measures, such as a general ban

[109] 'Adtech and Real-Time Bidding under European Data Protection Law'. Michael Veale and Frederik Zuiderveen Borgesius. https://osf.io/preprints/socarxiv/wg8fq/
[110] See for example 'Update report into adtech and real time bidding'. Information Commissioner's Office. https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf
[111] 'Intention to issue € 10 million fine to Grindr LLC'. Datatilsynet. https://www.datatilsynet.no/en/news/2021/intention-to-issue--10-million-fine-to-grindr-llc2/

on surveillance-based advertising, may be needed to tackle these broader issues.

5.2 The Unfair Commercial Practices Directive

The Unfair Commercial Practices Directive (UCPD) establishes a European framework for what marketing, commercial practices and terms of use commercial actors are allowed to engage in across different markets. Consumer protection authorities are responsible for enforcing this law and for ensuring that consumers are protected.

The UCPD is technology-neutral, and can in theory be used in cases that concern surveillance-based advertising. Marketing directed at individuals in the form of surveillance-based advertising can give rise to questions about whether the technology that is used to influence the receiving party crosses the boundaries for what constitute unfair and illegal influencing or pressure.

Questions can be raised about whether certain forms of surveillance-based advertising meet the criteria for aggressive commercial practices under the Marketing Control Act.[112] This provision is aimed at marketing that employs measures that are considered offensive to acknowledged and widespread societal norms.

However, the UCPD is predominately concerned with the content and form of marketing activities and materials. The numerous problematic issues arising from the use of surveillance-based advertising are not necessarily tied to the content of the marketing, but rather to the means of delivering ads, including the process of deciding which ad to show to what person at what time. This, in addition to the fleeting nature of surveillance-based advertising, may mean that the UCPD is not fit for purpose to regulate this particular area.

To our knowledge, no decisions regarding surveillance-based advertising have been issued by consumer protection authorities.

5.3 Enforcement issues

Although the GDPR sets forth strict requirements for processing personal data, the regulation has not been sufficient to stop the widespread illegal data

[112] Marketing Control Act, section 9, cf. section 6.

collection and profiling of consumers. The reasons for this shortcoming are that companies have not complied with the rules and there have been serious cross-border enforcement bottlenecks and a lack of enforcement.

The GDPR introduced new enforcement mechanisms that sought to facilitate cross-border enforcement, but thus far this has not worked as intended. For example, a large number of legal complaints have been passed to the Irish Data Protection Commission, since many large tech companies have their European headquarters in Ireland. This has led to complaints not being handled and to serious delays in decisions.[113] Simultaneously, companies continue to operate even after large-scale violations of the GDPR, since the likelihood of a swift decision or administrative fine is relatively small.

Enforcement of the UCPD against infringements in the area of surveillance-based advertising has not, to our knowledge, taken place. Penalising isolated infringements is a time-consuming process, and happens only after the infringement has occurred and the damage has already been done. In practice, this means that a large number of companies are getting away with breaking the law. The fact that the marketing itself is tailored and fleeting, since it is only shown to particular people at certain points in time, makes control and enforcement difficult. Furthermore, invasive and problematic surveillance-based advertising may not necessarily be in breach of the UCPD, as the content and form of a certain ad may be outside the scope of the law yet still be harmful in the way the ad was delivered or how the recipient was chosen.

The lack of enforcement of the GDPR has also led to a situation where a large number of actors have been able to continue operating illegally without facing any significant consequences. Models where profiles are created and stored locally on consumer devices may or may not reduce privacy risks, but the use of personalization and individualization still carries problems related to discrimination, manipulation or exclusion, and is also very difficult to control or verify.

Since investigating individual cases of violations requires considerable time and resources and comes after the fact, it is pertinent to consider whether more overarching remedies are needed to halt the use of surveillance-based advertising. Rather than considering individual cases of marketing, a general ban on surveillance-based advertising should be considered. This would

[113] 'Commercial surveillance by Google. Long delay in GDPR complaints'. BEUC. https://www.beuc.eu/press-media/news-events/commercial-surveillance-google-long-delay-gdpr-complaints

contribute to more efficient and swift enforcement, and would send a strong signal to the marketing and adtech industry.

6 Conclusion

Surveillance-based advertising causes violations of fundamental rights, widespread fraud and revenue loss, and has contributed to a number of negative individual and societal effects. Despite repeated warnings, fines, scandals, and revelations, the industry has shown little willingness to significantly alter its practices, and it is questionable whether significant changes to parts of the industry are even possible without fundamental reform.

Legislation in this area is fragmented and largely based on enforcement after the damage has already been done. It is therefore timely to ask whether surveillance-based advertising should be banned outright so as to prevent the problems being caused in the first place. A ban would also contribute to levelling the playing field in digital advertising and maximise revenues for advertisers and publishers which currently are in the hands of a few players.[114]

A general ban on surveillance-based advertising will force many industry actors to change their business models. It would stimulate growth for technologies that respect consumer and fundamental rights. In a longer-term scenario, it would help restore consumer trust in digital services. This would be a net positive for consumers, for businesses and for society at large.

We urge policymakers on both sides of the Atlantic to enact strict regulations to curb the many harms of surveillance-based advertising. Effective policy, regulation and enforcement to address the commercial surveillance that pervades our everyday lives are long overdue. As we have argued throughout this report, any perceived benefits of surveillance-based advertising are far outweighed by the harms, and a ban is therefore the right solution.

[114] This point is also being made by major industry actors, including the CEO of Axel Springer: 'It's time for Europe to take private data from the hands of powerful tech monopolies and give it back to the people'. Mathias Döpfner. https://www.businessinsider.com/big-tech-private-data-facebook-google-apple-europe-eu-2021-1