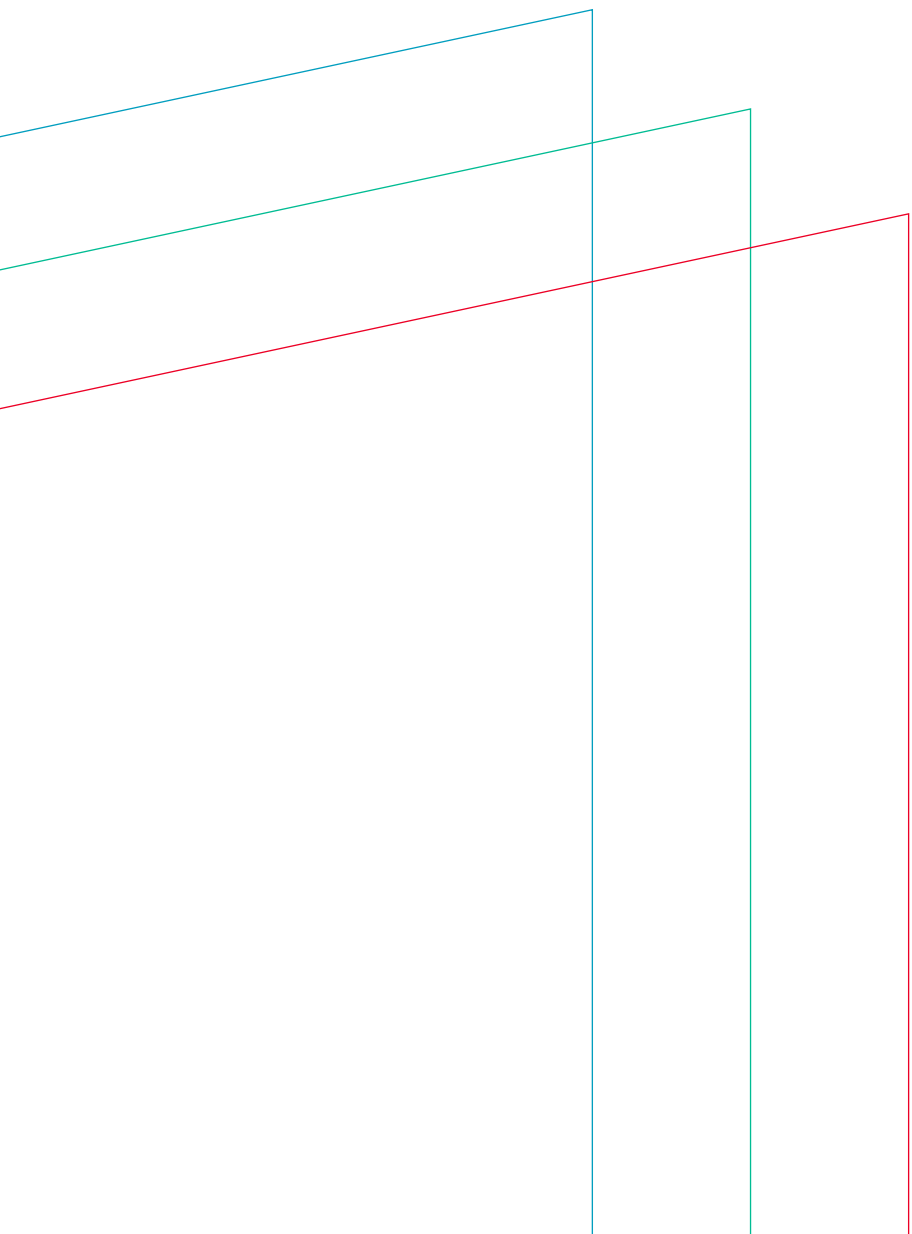
NEW ECONOMICS FOUNDATION

global action plan

I-SPY

THE BILLION DOLLAR BUSINESS OF SURVEILLANCE ADVERTISING TO KIDS



CONTENTS

EXECUTIVE SUMMARY

Today, one in three internet users is a child, but they are using a digital environment that was not designed with them in mind.[1] Unless we take active measures to limit it, our everyday activity on the Web, as well as that of our children, is recorded and tracked. Large multinational companies buy and sell this data to build detailed profiles that are used to target advertising.

Over the course of just 25 years, online advertising has evolved from a niche existence into a pre-eminent business model of the digital economy. Alphabet, the parent company of Google and YouTube, generated almost 84% of its 2020 revenue, around $135bn, from online adverts, while Facebook generated over 98.5% of its 2020 revenue that way, almost $70bn.[2] Despite being little more than a decade old, so-called surveillance advertising – targeted advertising using personal data provided by websites and platforms – has become the primary mode of monetising adverts for many of these major digital companies.[3]

This report explores the legitimate concerns around surveillance advertising and its use of large-scale data collection, profiling, and the sharing of children's personal information. Children have always been identified as being particularly vulnerable to the power of advertising. The advent of a new way to target individual people, with specific adverts based on their interests or personality, increases this vulnerability. Children are more susceptible to the pressures of marketing, less likely to recognise paid-for content, and less likely to understand how data is used for these purposes than adults.[4]

The online advertising industry, platforms, and tech giants claim that surveillance 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).

Surveillance advertising is demonstrably affecting social cohesion for both children and adults, helping to enable disinformation, clickbait, discrimination, and bias to survive and thrive. It makes disinformation websites much more economically viable than other modes of targeted advertising. Jake Dubbins, co-chair of the Conscious Ad Network, noted that"advertisers have helped fund the misinformation that stoked fires in the US Capitol",[5] while NewsGuard found that over 4,000 brands – including in some cases major pharmaceutical companies –"bought ads on misinformation websites publishing COVID-19 myths".[6]

Surveillance advertising also raises questions of legality. This includes how data is collected, acquired, or bought – especially where children have existing legal protection – as well as the aggregation of this data into profiles that are broadcast over advertisement auction networks. This is not surprising. The model pre-dates modern privacy legislation, like the General Data Protection Regulation (GDPR), and was therefore designed to work in a much looser regulatory environment.

Surveillance advertising is also failing to add proportionate value for advertisers themselves. A recent report by PriceWaterhouseCooper concluded that when considering the complexity of the online advertising ecosystem and the amount of money it pockets,"these challenges and complexities do not serve the principal interests of advertisers or publishers."[7] They found that publishers forgo 49p[8] of every £1 spent on online adverts in favour of online advertising intermediaries who each take a thin slice of the pie. In addition, major platforms, like Facebook[9] and LinkedIn,[10] have been caught defrauding advertisers by providing misleading metrics to boost the perceived impact of the adverts placed.

The dubious legality of surveillance advertising, along with the harm it causes, especially to children, as well as its failure to even support advertisers' and publishers' revenue, means that the current system is not fit for purpose. In this report,

we propose three recommendations to address these issues, each set at differing levels of ambition and effectiveness.

As an initial first step, policymakers could require platforms to use behavioural data that they have already collected to identify potential child users of their platform to ensure they are not served surveillance adverts. Any children identified on platforms with age restrictions would have had their data collected illegally and would need to be compensated and have their data deleted. However, reliance on this mechanism will likely prove inadequate on its own because it would legitimise ongoing data collection by tech companies and ultimately undermine hard-won data rights, where they exist.

A second proposal, which would go further in addressing the issues of surveillance advertising, is to implement a legal responsibility for information fiduciaries. This obligation would require companies to provide an active duty of care to data subjects. The basic concept is that when we give our personal information to an online company to get a service, that company should have a duty to do us no harm and exercise care towards us when using our information. Although it only offers partial protection from surveillance advertising, if implemented well, it could re-balance the power dynamic between a platform and its users and play a large part in helping to nurture new dynamics in the digital economy.

Finally, the most ambitious and effective solution would be to completely outlaw the practice of surveillance advertising. This would not ban advertising itself or the ability of websites to monetise their visitors' attention by showing them adverts. All that would change is that these adverts would no longer be targeted based on a user's personal data, but rather targeted on contextual data instead, based around the webpage and platform itself and the characteristics of their likely users.

Drafting new legislation would be the best way to achieve the ban. The new legislation could specify the limits on what information is permitted to be sent out by website owners seeking to have adverts placed on their site. It would prevent any personal information being sent to the real-time bidding (RTB) network (or other system) to provide an advert. We propose that nothing personally identifiable should be sent, with allowable permitted data limited to a new 'green list'. In addition, to ban surveillance advertising not done through online auctions, the legislation would also need to ban website owners (eg Facebook) from selling advertisement space on their sites using the user profiles they have built up using personal data.

1. INTRODUCTION

Today, one in three internet users is a child, but they are using a digital environment that was not designed for them specifically.[11] We now live in a world where, unless we take active measures to limit it, our everyday activities on the Web are recorded and tracked, with large multinational companies buying and selling this data, and compiling it into detailed profiles. Our digital selves then become marketable products, as advertisers pay tech giants and website owners to harness our attention and influence our decisions by placing adverts in front of us. This has created a strong incentive for companies to try and capture as much of our attention as possible, to gather as much information about us as possible, to show us as many adverts as possible.

This report explores the legitimate concerns around surveillance advertising and its use of large-scale data collection, profiling, and the sharing of children's personal information. It suggests ways that surveillance advertising systems could avoid targeting children, and so stop these harmful practices. These systems currently undermine the hard-fought regulation on advertising to children in place for traditional print and screen media. In this old world, there were limits around timing; certain adverts could not be shown before 9pm. There were limits to the volume of ads that could be shown in a given timeframe, and those ads were subject to a host of rules governing their content and message. These old rules no longer apply in the new online world. The current rules governing data privacy online do not protect children from surveillance advertising regulation, because regulation remains inadequate and poorly enforced.

Things are changing, however. Regulations, like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), are starting to impact company behaviour, as regulators and citizens begin to enforce compliance with the rules. At the same time, some major platform companies, like Google and Apple, are changing the rules that operate within their walled gardens. These changes are said to be focused on protecting people's privacy, but exactly how these new policies are going to operate remains uncertain. It is likely that how advertisers and publishers track users across websites in the future will be very different to how they do so today, but it is not possible to say exactly how. This report focuses on the problems of the current surveillance advertising system and proposes rules to ensure that the next-generation system is better for people, publishers, and the planet.

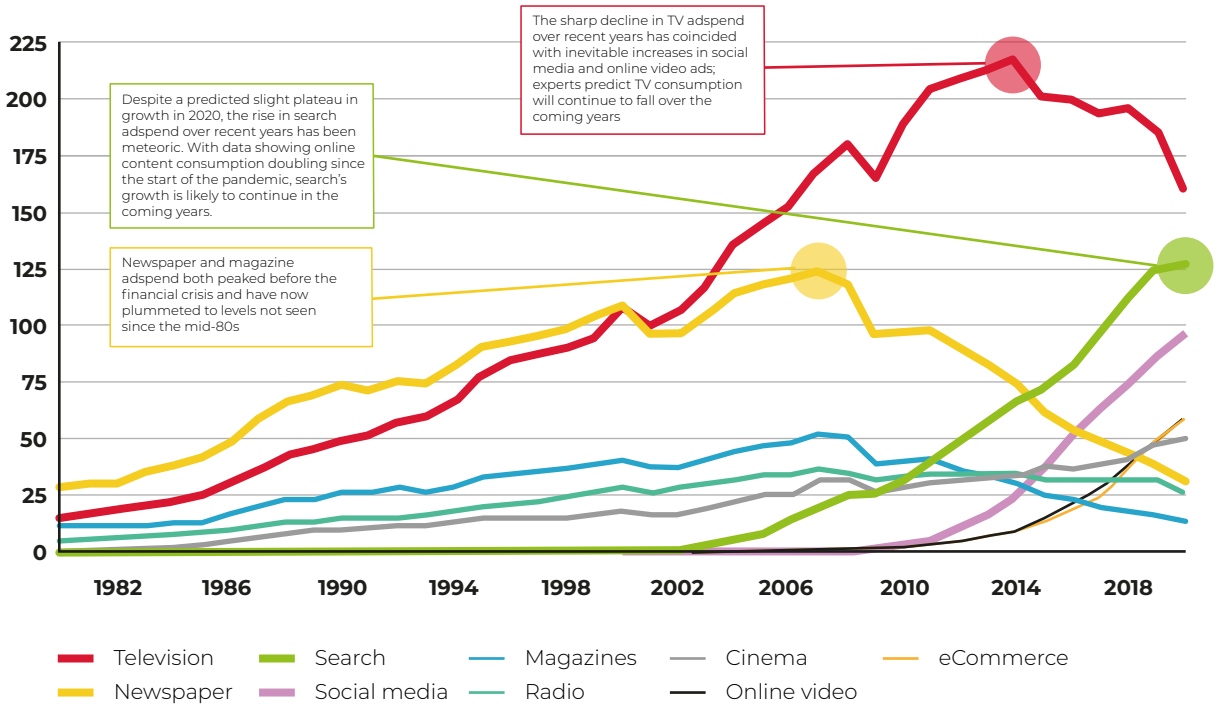
First, we explore the background context, including the growth in online advertising in recent decades, how surveillance advertising works, and how the pandemic has changed children's online habits. We then look at the multiple problems raised by the way that surveillance advertising works today. We examine surveillance advertising from social, environmental, and legal perspectives, and how it impacts society, and children specifically. We then discuss potential policy proposals and technical solutions that could resolve or mitigate problems with surveillance advertising to children. These broadly take two approaches: either a legal ban on surveillance advertising or a requirement that platforms understand the age of each user and ensure that children are not exposed to surveillance advertising. Before reaching the conclusions of the report, we outline a potential framework that could be used to score and compare different proposed solutions.

2. THE GROWTH OF SURVEILLANCE ADVERTISING

Over the course of just 25 years, online advertising has evolved from a niche existence into a booming economic sector with high growth rates. It is the pre-eminent business model of the digital economy. Alphabet, the parent company of Google and YouTube, generated almost 84% of its 2020 revenue, around $135bn, from online adverts, while Facebook generated over 98.5% of its 2020 revenue this way, almost $70bn.[12] Figure 1 shows that revenue for all forms of traditional advertising, such as television or newspapers, has been in decline since at least 2013, with some starting to decline in 2007. On the other hand, we see 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. The UK online advertising market generated £15.7bn in 2019 (Figure 2).[13] A recent report by Ofcom, the UK's communications regulator, estimates that the online advertising industry has grown at a compound growth rate of 20% for the past five years.[14]

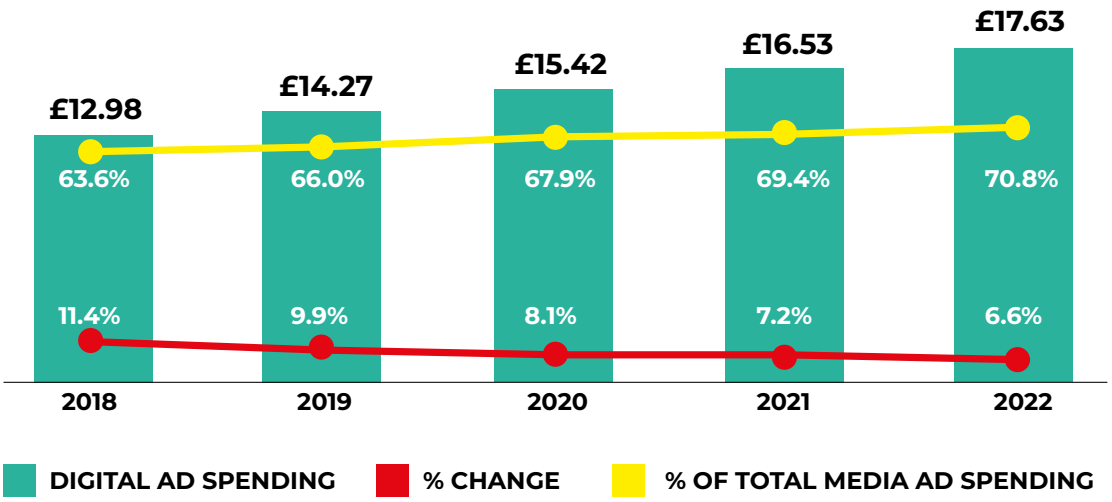
Initially, the emergence of the digital space did not significantly change the way that adverts were placed and delivered. Advertisers still went to where they thought their audience was and bought space, often through brokers and other intermediaries. Today, however, the picture is radically different. Advertising has migrated online in a remarkably short space of time. But what is more remarkable is that advertisers can now track and target individuals wherever they are on the internet, and that three digital giants, Google, Amazon, and Facebook, received 55.3% of the global digital ad spend in 2019.[15]

FIGURE 1: GLOBAL $BN SPENT ON ADVERTISING PER MEDIUM



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

FIGURE 2: UK DIGITAL AD SPENDING, 2018–2022
BILLIONS OF £, % CHANGE AND % OF TOTAL MEDIA AD SPENDING



Note: includes advertising that appears on desktop and laptop computers as well as mobile phones, tablets and other internet-connected devices, and includes all the various formats of advertising on those platforms.

Source: https://www.emarketer.com/content/more-than-60-of-uk-media-ad-spending-is-digital

The model of online advertising that dominates today is surveillance advertising, where adverts are placed in front of individuals based on personal data provided by the website and any adtech partners. This model is currently the primary business model of many digital companies.[16] It has been highlighted as troubling for a variety of reasons, from the way it invades our privacy, to the way it helps feed wider consumerism. Much of the analysis of surveillance advertising has been done in the context of thinking about how it affects adults. This report, as well as looking at the large systemic issues with surveillance advertising, will look more closely at the impacts on children.

In the UK, those under 13 benefit from some additional protection under the Data Protection Act (DPA), whereby those wishing to collect their data must obtain specific consent from a responsible adult.[i] There is, however, a challenge afoot about whether the law is being followed, with the case of McCann v Google[17] alleging that YouTube, the number one destination for children online,[18] does not obtain the necessary consent. Another case has also been initiated against TikTok, also alleging that it does not have the necessary consent to process children's data.[19] Consent for processing data for the over 13's is subject to different legal requirements, and many companies rely on other legal justifications instead of consent, such as 'necessary for performance of a contract' or 'necessary for your legitimate interests or the legitimate interests of a third party'.[20] A challenge for companies relying on consent is that, even if it has been validly given, it can be withdrawn at any time, which makes it very complicated to manage a data-intensive business. We are now in a situation where the global adtech industry holds 72 million data points on the average child by the time they reach the age of 13.[21] While digital platforms and companies are gathering more data on our children, our children are also spending more and more time online, a long-term trend that has been turbo charged by the Covid-19 pandemic. This dynamic means that children are being exposed to more data collection, more profiling, and more surveillance adverts. The data collected also informs the recommendation algorithms used by many digital companies to keep children online for longer, which leads to more ads and yet more data being collected.

i The protection comes from the implementation of GDPR which allowed countries to choose the age range where special protection arises. The GDPR allowed countries to set the upper limit between 13 and 16. The UK chose the very bottom of the range whereas many other countries, such as Germany and France chose the upper limit

3. HOW SURVEILLANCE ADVERTISING WORKS

The online ad world has evolved dramatically since the first banner ad appeared in 1994 on HotWired.com advertising AT&T (Figure 3). 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 notably changed. In these early days, internet users were interested in the novelty of online ads. This led to a high click rate. The percentage of those who saw the ad and clicked on it was an incredibly high at 44%.[22]

Since then, a new form of advertising has taken over the internet, one based on ubiquitous surveillance and profiling. The power of this new model has been accentuated and amplified by the automation of ad sales through what are known as real-time bidding (RTB) systems, first deployed in 2009.

This report does not look at all online advertising techniques, which include many forms of ads, different technical methods for delivering them, and different actors who take part in this process. It focuses specifically on the surveillance-driven open display[ii] advertising models sold via automated online auctions, variously called Online Targeted Advertising, Personalised Advertising, and Behavioural Advertising. Throughout the rest of this report, we will refer to these collectively as surveillance advertising.

This model of online advertising is complex and involves a large number of intermediaries between the advertiser on one side and the website and visitor on the other, each with their own interests and claim on some of the advertiser spend (Figure 4).

3.1. HOW AN ADVERT APPEARS ON A WEBSITE USING SURVEILLANCE ADVERTISING

1. When we click on a webpage, the page does not necessarily come pre-loaded with adverts that have already been placed. As we click, the website we are visiting identifies the number of advertising slots for sale and starts to compile a bid request.

2. To compile this bid request, the website collates as much information about us as possible, including the webpage we are visiting, our IP address (from which our location can be inferred), and our device details. It also sends various identifying information about us (the user) from previously collected data, through cookies and other mechanisms, or profile data bought from brokers, forming a detailed profile of us.

    a. A standard bid request contains the following:

        i. A user ID set by the supply-side platforms (SSPs).

        ii. A so-called full referral URL, meaning the link to the website where the ad is supposed to appear, a phrase or the link from and a category assigned to the website that, although relating to the content of the website, can reveal features of people visiting it and be highly sensitive (e.g. support for victims of abuse).

        iii. Year of birth.

        iv. Gender.

FIGURE 3: FIRST EVER ONLINE BANNER AD

ii Advertising served on publishers' websites or in their mobile apps.

v. Location.

vi. IP address (some systems truncate it).

vii. Interests or segments previously assigned to the user.

viii. Other information the SSP might hold, which can include any data they have collected directly, bought via data brokers or inferred.

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

4. The winning bidder gets to place the ad on the page we are viewing and to keep a copy of the data in the bid request.

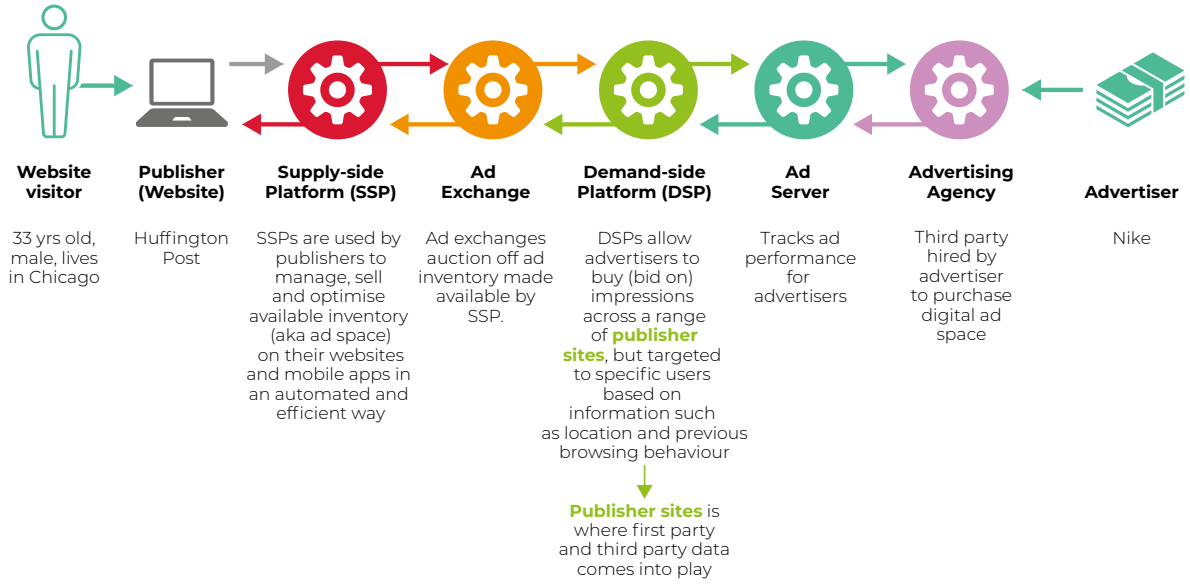
This auction process happens repeatedly every time we surf the Web. Although the total number of bid requests being sent daily is not public, we do know that "a single ad exchange using the Interactive Advertising Bureau (IAB) RTB system now sends 120 billion RTB broadcasts in a day."[23]

The New Economics Foundation estimated in *Blocking the Data* Stalkers,[24] that bid requests on UK users, containing our personal information, are being sent out at a rate of almost 10 billion a day[iii] or 164 per person per day across all the ad exchanges. They are seen by hundreds, if not thousands, of adtech companies, who could all be illegally collecting that data without us being aware of it. Using these very conservative figures, 820 million profiles of our children are being broadcast via RTB systems every day.

This whole process is automated from start to finish, with computers compiling the bid requests, artificial intelligence (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, in reality, the RTB sector is dominated by just two organisations – Google and the IAB – responsible for systems respectively known as Authorized Buyers and OpenRTB.

FIGURE 4: THE SURVEILLANCE ADVERTISING VALUE CHAIN



Source: Ankura Hogan Lovells presentation on AdTech and Privacy: Managing Risk in a Complex and Evolving Digital Economy https://f.datasrvr.com/fr1/120/19153/Ankura_-_Hogan_Lovells_-_AdTech_and_Privacy_Webinar_PPT.pdf

iii Based on own calculations multiplying the number of UK Internet users X average number of page visits per day X average number of ads per page X prevalence of ad blocking X use of real time bidding system

3.2. WHY CHILDREN SEE SURVEILLANCE ADVERTISING

Not all surveillance advertising is deliberately placed in front of children. Indeed, as we explore further in the next section, the targeting is not as precise as many would like us to believe. Finding out exactly who has seen a particular ad can actually be very difficult. There are broadly three ways in which advertisers can place a surveillance advert in front of a child, each of which we cover in turn:

1. Unintentionally, despite advertisers' best efforts

2. Carelessly

3. Intentionally

3.2.1 Unintentionally, despite advertisers' best efforts

A child may have a surveillance advert placed in front of them because of limitations in the ability of the surveillance advertising system to only target specific people or groups of people, in our case children. Some advertisers want to avoid their adverts appearing in front of children. This could be because of an explicit corporate strategy, as is the case with Mars Wrigley, or because the product or service being marketed is not appropriate for under 18s, such as alcohol or gambling.

Advertisers that want to avoid targeting children with their online adverts must work hard to achieve their goal. Evidence shows that it is impossible to ensure that 100% of surveillance advertising is not seen by children.[25] Even where a company communicates a clear desire to their adtech partners that they want to avoid any of their adverts being placed in front of children, they will find it an impossible goal to achieve; the techniques and tools are just not available.

3.2.2 Carelessly

A child may also be subjected to a surveillance advert because the company is either careless, or simply not caring about whether its adverts are placed in front of children.

When even a company that takes proactive steps to ensure that no surveillance advertisements are placed in front children fails, then those who make no effort to explicitly rule out advertising to children will naturally see a higher percentage of their ads being seen by children, even if this is not the intention of the campaign.

3.2.3 Intentionally

A child may also be targeted simply because they are a child, possibly also paired with specific characteristics.

3.3 SURVEILLANCE ADVERTISING V CONTEXTUAL ADVERTISING

Contextual advertising, another form of online advertising that pre-dates surveillance advertising, is enjoying a resurgence. 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. Google search ads continue to be among the most expensive adverts with some of the best click-through rates on the internet. However, since the emergence of the adtech ecosystem that can theoretically target individuals with tailored content based on their actual interests and immediate needs, the received wisdom has been that using that new model must be better and more lucrative.

From both academic studies of the area and real-world examples of companies changing their models, evidence is now starting to show that, at best, surveillance advertising brings in only marginally more revenue.[26]

As shown in Case Study 1, there is also emerging evidence that contextual advertising can be more profitable for publishers, while reducing the margins that adtech intermediaries extract, because advertisers are no longer reliant on additional personal data, analysis, and matching from adtech intermediaries.

CASE STUDY 1: NPO

In January 2020, one of the major Dutch public broadcasters, NPO, decided to switch their whole advertising model to contextual advertising. Received wisdom was they would see a dramatic fall in revenue as advertisers were no longer able to target people specifically. In reality, their revenue increased by 76% in February 2020 compared with the previous year.[27] Even while the pandemic led to significant drops in publishers' revenue generally, NPO's revenue from contextual ads not only did not fall but was higher in March–May 2020 than in the same period in 2019.

As the narrative around surveillance versus contextual advertising shifted, specific platforms and companies emerged to focus on the latter. One such platform, Kobler, recently released data showing that advertisers were prepared to pay 3.4 times more to place a contextual advert than the average price for a behavioural ad.[28] As well as seeing more revenue per ad, Kobler has also been growing quickly, with ad spend through the platform increasing by 400% in just six months. More companies are either experimenting with contextual advertising or moving their entire business over.[29]

There are myriad benefits from the widespread adoption of contextual advertising over surveillance advertising. Contextual advertising is genuinely privacy protecting because it does not involve the collection, processing, or broadcasting of personal data. It therefore eliminates any regulatory risk associated with data protection legislation and is one of the reasons why contextual targeting is increasingly gaining popularity. As well as eliminating legal risk, it also vastly reduces the internal administration required to manage consent and other user preferences.

4. PROBLEMS WITH SURVEILLANCE ADVERTISING

Having explained how surveillance advertising works, we now explore some of the problems and issues that its widespread use raises for society, as well as for individual privacy and agency.

The adtech industry, many platforms, and tech giants claim that surveillance 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. As we show, however, individuals, publishers, and even advertisers are all, to a lesser or greater extent, losing their privacy, revenue, or autonomy. These effects also spill over into society.

A recent report by PriceWaterhouseCooper concluded that when considering the complexity of the online advertising ecosystem and the amount of money it pockets, "these challenges and complexities do not serve the principal interests of advertisers or publishers."[30] They found that publishers forgo 49p[31] of every £1 spent on online adverts in favour of online advertising intermediaries who each take a thin slice of the pie. In addition, major platforms, like Facebook[32] and LinkedIn,[33] have been caught defrauding advertisers by providing misleading metrics to boost the perceived impact of the adverts placed with them.

Beyond publishers and advertisers, children have always been identified as being particularly vulnerable to the power of advertising. The advent of a new way to target individual people, with specific adverts based on their interests or personality, increases this vulnerability. Children are more susceptible to the pressures of marketing, less likely to recognise paid-for content, and less likely to understand how data is used for these purposes than adults.[34] Surveillance advertising accentuates existing problems with marketing to kids and creates new issues. This report, however, does not deal with long-standing and well-documented concerns around advertising to kids, such as pester power[iv] or impacts on mental health. These issues are explored in more detail in Global Action Plan's report *Kids for Sale*.[35]

We now explore the many social and environmental issues that surveillance advertising produces and how they affect society, individuals, and especially children.

4.1 UNSUSTAINABLE AND UNHEALTHY CONSUMERISM

It has been said that "advertising is the art of convincing people to spend money they don't have for something they don't need."[v] Advertising rarely provides unadulterated facts to help people make good, informed choices. Instead, it seeks to persuade and elicit a specific response, usually a purchase or increased brand recognition.

An example of this is Coca-Cola, a product that has remained unchanged for over 100 years yet the company spends over $4bn a year on marketing.[36] This enormous expense is not to educate us about Coca-Cola and its contents, which is a commercial secret, but to compel consumers to buy the product, as well as create and maintain brand awareness and affinity.

To compel consumption, the advertising industry often utilises psychological studies, for example studies that link purchasable products to unconscious desires.[37] Advertisers also frequently promote unrealistic expectations, for example by featuring seemingly perfect people and their perfect lives. Such adverts can leave us feeling emotionally insecure and seeking the product or service so that we, too, can be happy.[38]

The advertising space is full of slick ad campaigns that, rather than meet consumers' needs, make them want things they never knew they wanted.[39]

iv 'Pester power' is the tendency of children, who are bombarded with marketers' messages, to unrelentingly request advertised items. The phrase is used to describe the negative connotations of children's influence in their parents' buying habits.

v Quotation attributed to Will Rogers.

If all this is true for adults, then the impact on children, especially young children, is likely to be much worse. There is growing evidence showing a positive relationship between the amount of advertising children see and their levels of materialism.[40] This is found across all age groups, from pre-school to teenagers. Studies have demonstrated that materialism also impacts other areas of children's lives. More materialistic children have been shown to have lower wellbeing,[41] perform worse academically,[42] be less generous towards others,[43] and care less about the environment.[44]

Children, especially young children, do not have the cognitive ability to fully understand the purpose of advertising, and so are particularly susceptible to the manipulation involved in surveillance advertising. For very young children, there are challenges in even identifying the difference between adverts and neutral information.[45] Only 25% of 8–15-year-olds, for example, were able to identify the top results from a Google search as adverts, despite them being clearly labelled with the term 'ad'.[46]

Even as their critical abilities and skills mature, children remain highly influenceable. These factors, combined with the modern power of surveillance advertising, mean that "there is simply an unprecedented degree of asymmetry between the persuasive tactics used and the ability of a child to comprehend and resist them."[47]

Marketing to children is, by intention and design, inherently manipulative. This manipulation is intensified by a huge asymmetry of ability and information. On the one side is the child, who does not have the full mental capacity to understand or resist, and on the other is a powerful ecosystem of companies, with vast troves of data about the child. This makes surveillance advertising inherently more manipulative than traditional advertising.

4.2 DISINFORMATION AND CLICKBAIT

The adtech ecosystem has enabled the monetisation of the internet in a way that was impossible prior to its invention. Although disinformation and clickbait have been a feature of the internet since its inception, being able to monetise such a site easily and lucratively is a newer development.

During the twentieth century, advertising centred on companies and organisations securing the best space to show off their wares, such as a prominent billboard, a popular magazine, or, more recently, a prime-time television slot. Advertisers had to buy space where they thought their target market might be and show their products to a large number of people in the hope that some would be their target audience. Companies who had particular audiences could charge advertisers for access to them. For example, if a company wanted to target well-off professionals, they would place an advert in *The Economist* or the *Financial Times*, while if they wanted to reach the archetypal 'man in a van', they'd approach *The Sun*.

The theory of the new adtech ecosystem is that advertisers no longer need to place adverts where they think their customers are. Today, advertisers can target their audience wherever they are online, thanks to a pervasive online tracking system, coupled with a new auction system for placing ads. In the past, brands would have been wary of placing adverts directly on misinformation or clickbait sites, as this could cause reputational damage and they would not know if they were targeting the right kind of people. Now these brands, working with demand-side platforms (DSPs) and others in the adtech ecosystem, can track specific users, or users with specific characteristics, around the web. Unsurprisingly, it is cheaper to advertise on disinformation or clickbait sites than on reputable sites.

The surveillance advertising system, which focuses on individuals over locations, therefore creates opportunities for publishers of misinformation and clickbait to participate in ad auctions. This can result in advertising money from some of the world's biggest brands supporting extremist and fake news content.[48]

The Global Disinformation Index has conservatively estimated that "$76 Million in ad revenues flow each year to disinformation sites in Europe."[49] In another case, an investigative journalist tracked down the owner of a network of fake news sites, who claimed to be making between $10k and $30k per month from surveillance advertising.[50]

Ad agencies buy ads on premium publishers' websites just long enough to begin tracking their target users. Once they have enough data

to track them, they then switch to placing ads in front of those same users but on cheaper sites, often without caring whether these sites promote disinformation.[51]

As Jake Dubbins, co-chair of the Conscious Ad Network, noted,"advertisers have helped fund the misinformation that stoked fires in the US Capitol."[52] The events of 6 January did a lot to push to the fore the role of platforms and their algorithms in spreading disinformation. Without lucrative revenue from targeted ads, such sites would be less prolific. As another example, NewsGuard found that"over 4,000 brands bought ads on misinformation websites publishing COVID-19 myths."[53] Amazingly, this even includes vaccine manufacturers like Pfizer.[54]

We should be especially worried about the effect of disinformation on children, especially the young, who often lack the abilities needed to evaluate and verify information provided online. Children are subjected to a large amount of disinformation, with more than 10% seeing it over six times per day, while almost half see it on a daily basis.[55] A survey, conducted by the Safer Internet Day, found that exposure to disinformation made children feel annoyed, upset, sad, angry, attacked, or scared.[56] This proliferation, at least partly fuelled by the adtech system, has forced the Department of Education to start teaching children how to spot disinformation, due to concerns that it will"destroy trust, damage learning culture, and sap curiosity".[57]

An advertising industry expert, Bob Hoffman, goes even further to present a plausible pathway that links the adtech industry and the wider radicalisation and polarisation of society (Figure 5).

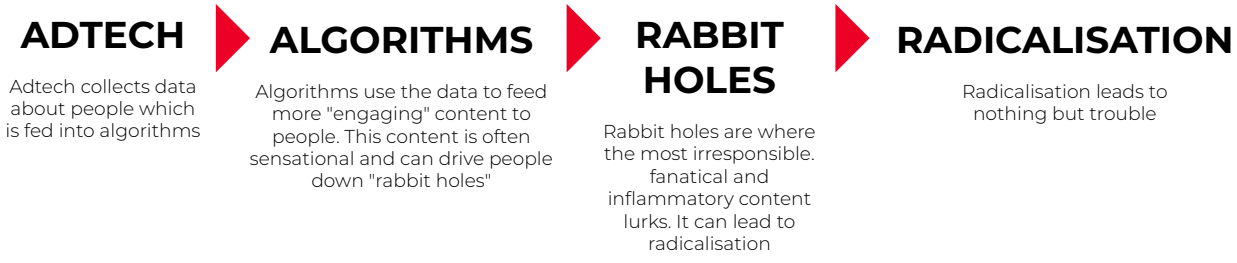
As Figure 5 shows, the large volumes of data collected by the adtech industry feeds into content recommendation algorithms, which can ultimately lead to radicalisation. Indeed, an internal Facebook study, reported in the *Wall Street Journal*, found that"64% of all extremist group joins are due to our recommendation tools... Our recommendation systems grow the problem."[58] As children are less able to rationally understand what is happening or to counter messages seen, we should be especially worried about their radicalisation.

4.3 DISCRIMINATION AND BIAS

The nature of surveillance advertising is that it can target individual people or people with specific characteristics. When advertising a product, say a ping-pong table, it makes sense to try and show the advert only to people who are likely to be interested, for example people who have a BT sport subscription or a tennis club membership. This system, however, can also be used for discrimination and bias. For instance, when placing job adverts, adtech tools can be used to help block certain groups, like women, migrants, or people of colour. They can also be used to exclude people with certain characteristics, such as race or location, from services. This discrimination is also hard to detect, as people generally do not know they are being discriminated against. They do not know what ads they haven't been shown.

The publication *ProPublica*, for example, bought dozens of house-for-rent adverts on Facebook.[59] When posting the adverts, they asked that they not be shown to certain categories of users, including African Americans, mothers of high school kids, people interested in wheelchair ramps, Jews,

FIGURE 5: THE STRAIGHT LINE BETWEEN ADTECH AND RADICALISATION



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

expats from Argentina, and Spanish speakers. This is illegal under the US federal Fair Housing Act, which prohibits discrimination. Facebook, however, approved the adverts within minutes, raising serious questions about its and the wider adtech ecosystem's compliance with anti-discrimination and anti-bias legislation.

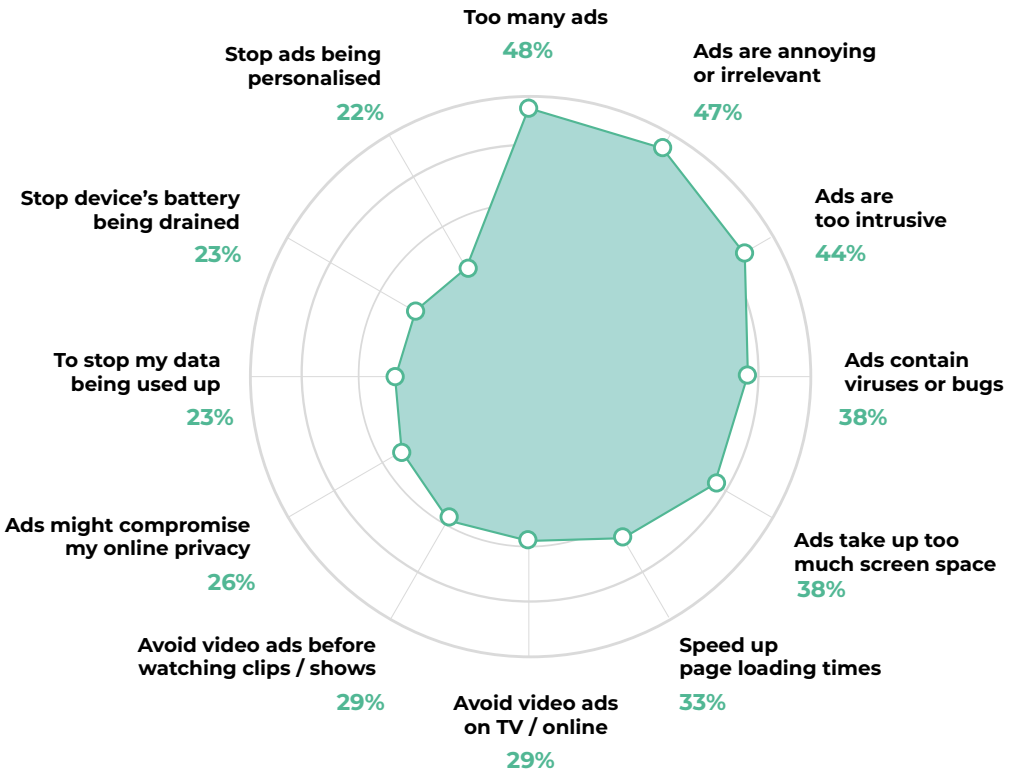
4.4 DISLIKE OF SURVEILLANCE ADVERTISING

For years, big tech companies and the adtech ecosystem have pointed to numerous industry funded surveys showing that people like personalisation and are willing to relinquish data and be shown ads in exchange for free online services.

An industry release from 2015, for example, proclaims that"consumers crave a personalized advertising experience and that 71% of respondents prefer ads tailored to interests and shopping habits."[60] The same report states that personalised adverts also boost engagement, noting that"people were almost twice as likely to clickthrough for an ad featuring an unknown brand if the ad was tailored to their preferences."[61] Finally, the study also found that 44% of those surveyed were willing to give up personal information to get more personalised adverts.[62]

The consultancy Harris International conducted research for the UK's Information Commissioner's Office (ICO) on attitudes to personalised adverts in 2019, which highlighted that most people do not understand how personalised adverts work or the extent of the personal data about themselves which is collected by these networks.[63] Without being given any explanation of how adtech works, people were asked whether they think it is okay for websites to display personalised adverts in return for the site being free to access; 63% responded that it was acceptable, while just 14% thought it unacceptable.[64] However, once people were told how adtech works and what data is used, a very different reception was found. Now 36% thought adtech was acceptable, whereas 43% thought it unacceptable. Another survey quizzed people's attitudes on the ethics of adtech:

FIGURE 6: TOP MOTIVATIONS FOR AD BLOCKING
% OF AD BLOCKERS WHO REPORT THE FOLLOWING AS THEIR MAIN REASONS FOR BLOCKING ADS



Source: https://www.digitalmarketingcommunity.com/indicators/ad-blocking-motivations-2019/

A mere 17 percent of respondents view tailored advertisements as ethical, and only 24 percent believe personalization to create tailored newsfeeds is ethical.[65]

Our growing antipathy towards surveillance advertising can be partly seen in the growth in the use of ad blockers. Over one-third of computer users apply ad blockers. These numbers reduce when applied to tablets and phones, but no region of the world sees less than 13% of users using ad blockers.[66]

There are many reasons why people choose to install and run ad blockers (Figure 6). The top reasons, 'too many ads' and 'ads are annoying', show that users are tired of adverts, while other core motivations speak directly to users' unease at the use of their data to provide advertising. For instance, 22% used ad blockers to stop ads being personalised, while 23% used them to stop their data being used, and 26% did so because ads could compromise their online privacy.

Recent work by the ICO also revealed that people use other methods to block adverts, such as actively deleting marketing cookies (36%), changing browser settings (31%), and stopping visiting the website altogether (30%).[67]

4.5 ARMS RACE FOR OUR ATTENTION

Advertisers and the adtech ecosystem want to capture our attention and then influence our decisions and behaviour. We, however, have become accustomed to marketing tricks, and have learned how to consciously ignore them. Advertisers and their marketing consultants are, therefore, in an arms race for our attention. Companies 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%.[68]

As another example, pop-up ads were an adtech innovation that tried to ensure users paid attention after people had started ignoring banner ads. These ads would, as the name suggests, 'pop-up' and pretty much force the user to engage. Although this may have made short-term sense for advertisers, many users felt that a line had been crossed. Users have found ways to block pop-ups, first through customised plug-ins, but now as a standard feature of most browsers. As a response, websites partnered with adtech companies, which resulted in extensive additional data gathering about users and the sites they visit to create detailed profiles. The location of ads within websites also changed, with ads now appearing in the middle of articles, and video ads now often autoplaying.

We now explore four trends that are part of the ongoing arms race between the adtech industry and users.

4.5.1 Death of the third-party cookie

The arms race is presently in full swing as many of the major browsers and platforms get rid of third-party cookies. Third-party cookies are placed on your browser by a website other than the one you are currently visiting. Probably the most famous cookie is the Facebook 'like' button, which appears on many non-Facebook websites and will store a small piece of computer code on any visitor's computer, even if they do not click on the 'like' button. That cookie can later be accessed by Facebook to identify visitors and see which websites they visited. These invasive tracking devices, however, are on their way out, with Google giving a firm date of 2022. Regulations around the world had put their legal status at risk, and almost all non-Google browsers, from Safari to Firefox, already block most third-party cookies.

The end of third-party cookies means the adtech industry will need to find a new means of collecting the user data that has become so critical to fuelling the adtech ecosystem.

We are not going to see the death of first-party cookies, however, because they don't follow us around the web and are critical to the smooth operation of websites. For instance, without first-party cookies when online shopping we would need to login to each page we visit in order to add a product to our basket.

4.5.2 Birth of the unblockable trackers

The rise of ad blocking and the death of third-party cookies has resulted in what the open-source ad blocker uBlock Origin has dubbed an "unblockable tracker".[69] Although the uBlock Origin team has

managed to find a way to block the tracker in Firefox, this leaves Chrome and possibly other browsers susceptible. This tracker builds up profiles of users' interests and keeps track of pages they visit without being blocked by the browsers or ad blockers. This is a clear example of the dangers that result from an arms race between browser makers and adtech companies.

4.5.3 First- vs third-party cookies

With the writing on the wall for third-party cookies, innovative adtech companies are also starting to use a technique called DNS delegation or DNS aliasing. This involves a website owner giving an adtech company access to manage a subdomain of their website, basically another page on their website. This can trick browsers and adblockers into thinking that the external tracker is in fact coming from the website and is therefore allowed.

There is evidence that major adtech players, like Criteo, are already deploying this technique despite it being in clear contravention of Europe's General Data Protection Regulation (GDPR) and the UK's Data Protection Act (DPA). This also shows that the adtech industry is willing to engage in "deliberate action to make a third-party cookie appear to be first-party to skirt privacy regulations and consumer choice".[70]

4.5.4 Rise of digital fingerprinting

Another technique that has been on the rise is digital fingerprinting. This technique collects information about the settings that we have on our devices, such as what model and operating system we are using, and our device's screen resolution, to create a unique combination of settings that can then be used to track us around the net. In 2019, it was estimated that 3.5% of mobile apps were using this technique, double the figure from 2016.[71] The death of third-party cookies, however, is likely to accelerate their growth. For instance, it was recently revealed that Proctor and Gamble, among the world's largest advertisers, is actively working to develop robust fingerprinting technology so that it can continue to track users online.[72]

The privacy crowd has, thankfully, already developed techniques, plug-ins, and solutions to defend us against pervasive digital fingerprinting. This is not the end of the adtech arms race, however; it is just the start of the next step in the race.

4.5.5 Overpowers children's attention

In addition to the arms race for our children's attention, surveillance advertising is allowing advertisers to develop increasingly sophisticated strategies to capture their attention. As well as using traditional ways of getting children's attention, such as the use of cartoon and TV characters in adverts, they are also utilising the full power of surveillance advertising to do the following:

- Inundate kids with adverts across all of the technologies they use, such as TV, mobile phones, tablets and computers, even wearable technologies.[73]
- Target children, regardless of where they are on the internet.
- Create enticing and engaging opportunities for children to interact with their brands.

As children spend more time online, they are exposed to an almost limitless volume of advertising. Rules have long existed limiting TV ads to seven minutes per hour on Public Service Broadcast channels or nine minutes per hour on other channels.[vi] There is no online equivalent.

Data analysis by the digital monitoring agency Sprout Social reveals that one in every three Instagram posts is an advert.[74] A Global Action Plan survey of teenagers revealed that, on average, teens see one ad every ten seconds while scrolling through their feeds, equivalent to 420 adverts per hour.[vii] Based on average online time, this means that "a third of 14 year olds could be exposed to 1,260 adverts a day – ten to twenty times as many adverts as children see on TV alone."[75]

---

vi The amount of advertising UK television broadcasters are allowed to show is determined by regulation at a European level through the AVMS Directive, which is implemented in the UK by Ofcom's Code on the Scheduling and Amount of Advertising (COSTA). https://www.ofcom.org.uk/__data/assets/pdf_file/0014/32162/costa-april-2016.pdf

vii Global Action Plan survey of 102 teenagers using Instagram, 12 January 2020. Of 102 surveyed, they saw an average of 7.4 ads in one minute scrolling their Instagram feeds. 74% said they found advertising on social media either sometimes or very annoying.

Finally, persuasive design, which creates experiences that nudge users to take certain actions, encourages children to spend more and more time online. Persuasive design is fundamental to the success of surveillance advertising, as its goal is to keep people online for as long as possible, to increase platform revenue from surveillance advertising.

4.6 CARBON EMISSIONS

All actions involving the processing, analysis, and use of data, and transferring it around the world, consumes energy, not only where you physically are to power your computer or tablet, but all over the networks utilised across the world. For instance, Google calculates that an average user's searching on Google for a year generates CO_2 emissions equivalent to one washing machine cycle.[76] Now this is not much when considered individually, but when multiplied by Google's billions of users, it becomes considerable, especially when you consider that we are only talking about the energy for one small part of our online/digital life.

Surveillance advertising also has a carbon cost, which will only increase as more data is collected, stored, processed, and analysed, and as the number of internet users and internet pages increase. A 2016 study evaluated the global carbon footprint of online advertising at 60m metric tons,[77] which is the same as one-fifth of the UK's 2019 emissions.

Today, the total is likely to be much higher for three reasons. First, we have seen a large increase in the volume of digital advertising, with spending having increased significantly since 2010 (Figure 1). Second, the study does not include the carbon impact of data collection, processing, analysis, the creation of detailed profiles based on that information, the further data bought from other companies who have collected and processed it, and the impact of the storage and management of all this information. Finally, there has been an increase in the use of complex machine learning algorithms to process raw data into actionable and valuable insights for advertisers. Machine learning systems are often very energy intensive.[78]

As countries around the world coalesce around the need for concerted action to mitigate the worst impacts of climate change, we should not ignore the contribution of surveillance advertising.

4.7 LEGAL ISSUES

Beyond some of the social and environmental issues that surveillance advertising raises for us as individuals and as part of wider society, it also has serious legal issues. In this section, we examine how surveillance advertising is built on very shaky legal ground, and explore some of the ways that it almost certainly already contravenes existing legislation. We also expose the various ways in which ad fraud can be used to deceive and defraud advertisers.

4.7.1 Potential illegality at the heart of surveillance advertising

This report articulates some of the main problems with the surveillance advertising system. There is, however, potentially a larger issue: the adtech world is alleged to be rife with illegal practices, including the processing of personal data in the RTB system in contravention of the GDPR. There is potential illegality not only by companies breaking the rules of the system as well as those following them. We believe 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, especially in the case of children.

2. Profiles of individuals (especially children) 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 necessary legal justification.

3. The broadcasting[viii] of bid requests, containing our personal data, over the RTB network to hundreds, maybe thousands, of adtech companies, without adequate legal justification or protection. Once again, this is particularly concerning regarding children's data.

viii 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.

This is not surprising, because the adtech model pre-dates modern privacy legislation, like the GDPR, and was therefore designed to work in a much looser regulatory environment. We now take a more detailed look at each of the three potential legal issues.

In 2018, a complaint was lodged with the ICO claiming that the RTB system resulted in systemic breaches of the DPA. As interest and awareness of the issues increased, similar complaints were lodged in 17 other European jurisdictions.[79] In 2019, the ICO issued a report that confirmed many of the issues raised in the complaints and concluded:

> *Thousands of organisations are processing billions of bid requests in the UK each week with, at best, inconsistent application of adequate technical and organisational measures to secure the data in transit and at rest.*[80]

They also found that neither legitimate interest nor consent could be used as a legal justification for broadcasting data through the RTB system.[81] However, the ICO has taken no enforcement action to date and is now being taken to court by the Open Rights Group and others for their failure to do so.[82] In 2020, the Belgian DPA, which is the lead EU enforcer on adtech,"found serious GDPR infringements in the system Google and others use to legitimise online tracking".[83] This clearly demonstrates that allegations of illegality at the heart of surveillance advertising are real and they should therefore provide another serious catalyst for wholesale change in the surveillance advertising industry. A recent US settlement forced Disney, Viacom, and 10 adtech companies to remove specific advertising software from their children's apps because they violated the privacy of children.[84]

Illegal data collection

Personal data collection across the digital economy in the UK and EU requires an approved legal basis. Although consent is often sought through lengthy terms and 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.

Whereas for some data processing these legal bases may be wholly appropriate, the UK's ICO has been clear that when placing cookies on people's browsers (or using other techniques like digital fingerprinting) to gather their personal data, "consent is the most appropriate legal basis."[85] Once the data processing is based on consent, other problems then appear.

First, regarding the collection and processing of children's data. Article 8 of the GDPR provides that if an online service is provided to a child (in the UK, defined for data protection purposes as under 13) such consent must be given by the person with parental authority for the child. The recently launched case of McCann v Google,[86] initiated by the author of this report, will be the first major case to test the notion of consent as the legal basis for processing children's data. The case alleges that YouTube, owned by Google (in turn owned by the holding company Alphabet), has not received meaningful consent from the legal guardians of the children that it proceeds to collect data on systematically.

Second, there is a more general concern that the kind of consent that is given online when accepting terms and conditions does not meet the GDPR's definition:

> *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.*[ix]

It is clear that the way most consent is obtained would struggle to meet these conditions. Many websites are evolving to allow users to access their site while rejecting data processing, which is a welcome advance, but too many websites, apps, and services still only allow us to accept or reject the terms – with a rejection meaning no access. In addition, rather than collecting data for specific limited purposes many sites feel that they can use our personal data as they see fit. Finally, because so few people read the terms and conditions, it is hard to say how the consent is informed.

The large-scale collection of personal data, at least some of which is likely to have been illegally collected, also creates a risk to everyone due to the potential of this data being leaked to, shared by, or stolen by actors who wish to use this data against

ix GDPR art 4(11).

the data subject. This could be sensitive data that could be used to blackmail people and companies, as in the Ashley Madison leak,[87] or used to steal people's identities.[88]

Illegal profiling

All this data processing is done, in part, with the intention of creating detailed profiles of people and their interests to enable advertisers to specifically target them. There are currently thousands of digital profiles of each of us, collated from our vast data trails online. Some contain rich histories with thousands of data points collected over many years; others are just single data points.

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 of 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.

Even if we could somehow get easy access to all our profiles, including being able to amend and correct them, there remains another important issue: to be meaningful, we must have some control over the inferences these companies are making about us. Our digital profiles are full, not just of objective and verfiable facts (age, place of birth, address, etc.) but also of inferred characteristics. In fact, many of the most 'useful' and monetisable aspects of our profiles are inferred data, including data that has been inferred from other inferred data points. Examples could be our interest in a certain topic or product, inferred from our interest in similar products; whether we are getting married or having a child in the near future, inferred through social media messages; or our mental health and imminent suicide risk or attempts, inferred from web searches and the websites that we visit. Many children, and adults, are unaware of this practice.[89]

These inferences are currently made mainly to target advertising, but also to personalise what we see on each website. Facebook's profiling system was found to have labelled over 740,000 children as "interested in gambling" and over 940,000 children "interested in alcohol", attributes which advertisers could then target.[90] Current data protection legislation does not grant us the same protections and rights over inferred data as over personal data that we have actively provided in the course of our interactions with digital platforms.

Another core problem with 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 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 buy our data.

Finally, despite all these attempts to collect and compile data about us, our profiles are full of incorrect and inaccurate data. Acxiom, one of the largest data brokers, concedes that about 30% of the data held in each profile is incorrect.[91] This has potentially huge implications, as it means that many of the 'interests' or 'characteristics' attributed to us will be false, and therefore any advertiser using that information to bid at auction to show us an advert will have been defrauded, since the premise on which they made a bid was not accurate. Also, since these profiles are not built in collaboration with us, neither we nor the companies will ever know what is inaccurate and why. Sometimes the consequences of inaccurate profile data can be relatively innocuous, like seeing an advert that does not interest you. However, there can also be serious real-world implications to incorrect data being assigned to your digital profiles as Case Study 2 demonstrates.

CASE STUDY 2: HOW INCORRECT DATA CAN RUIN LIVES[92]

Catherine Taylor's world was turned upside down when a data broker, ChoicePoint, incorrectly linked her to a criminal charge of intention to supply methamphetamines.[93] The data broker then sold her file on many times so that the original error was replicated widely across the many digital profiles maintained about her.

Luckily for Catherine, she was able to find this incorrect data and communicated with ChoicePoint so that they could remove the record. This did not, however, rectify the error in all the systems that had bought the incorrect data. Catherine was forced to personally contact all the other brokers and even file lawsuits to get the offending data removed.

The error cost her job interviews, as employers were scared away by the black mark against her name. It took over four years for her to find a job. In the meantime, she was rejected for an apartment she wanted to buy and couldn't even get credit for a new washing machine.

Although Catherine was able to remove almost all the incorrect data, it took a huge toll on her, consuming lots of time and effort while exacerbating health problems. But at least Catherine was aware of the offending data. Many people could be affected by this problem without knowing the reason or having the time and patience to resolve the issue.

Illegal broadcasting of personal data

The adtech industry is potentially exposing every person who uses the internet not only to fraud but also 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.[94]

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.[95,96] Because of the obvious challenge of identifying if and when adtech companies are actually recording the data they receive, we believe that the case against Vectaury represents only the very tip of a sizable iceberg.

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 link to a page, 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.

If all this is true for the data of adults, then the case for the RTB system violating data protection laws is even stronger when the data is of children, who are better protected by the law.

Ad fraud

Three key fraudulent advertising practices are click fraud, domain spoofing, and unviewable ads.

Click fraud involves the widespread practice of using bots and automated scripts, and occasionally armies of paid humans, to click on adverts. This results in the advertiser paying 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,[97] while another study suggested that $1 in every $3 spent was lost to it.[98]

Domain spoofing uses an unknown website that is made to look like a high-value website to get ads placed by legitimate advertisers. The website owners then use botnets[x] and other tricks to drive traffic to the spoof site and generate ad revenue. The ease of using ad-fraud techniques, and the very low risk of getting caught or sanctioned, means that organised crime is diversifying its operations to take advantage of this sizable opportunity. This led the World Federation of Advertisers to predict that by 2025, ad fraud would be worth over $50bn a year, representing the second highest source of income for organised crime, after drug traffic.[99]

Another way the adtech ecosystem is accused of unfairly pocketing too much of the ad spend is in how **rebates**, ie discounts for the bulk purchase of ad placements, are passed back through the system. For instance, a report by K2 Intelligence found that in 83% of adtech companies "rebates were not disclosed to advertisers or were not passed through to advertisers."[100] The Association of National Advertisers similarly stated:

Advertising agencies defrauded their own customers by failing to disclose rebates they received from vendors, and also routinely act as principals in buying ad impressions and then reselling them to clients at 30–90% markups.[101]

x Collections of computers controlled by malicious code.

5. EVALUATING POTENTIAL SOLUTIONS

Stopping targeting advertising to kids may sound simple, but it is a complex technical task, especially because many of the potential solutions create additional problems, such as requiring additional data to be collected about the child, the use of biometrics, or the proliferation of insecure age-gates.

There are two over-arching strategies to achieve our goal.

1. Institute a legal ban on surveillance advertising.

2. Establish whether the user is over or under 18 and adjust the surveillance advertising practices for the user accordingly.

We explore both of these routes, noting that there is a multiplicity of ways the second option could be achieved.

5.1 LEGAL BAN ON SURVEILLANCE ADVERTISING

The dubious legality of surveillance advertising, along with the harm it causes, especially to children, as well as its failure to even support advertisers' and publishers' revenue, means that the current system is not fit for purpose. The system fails to ensure the protection of personal data against unauthorised access, and creates large incentives for a digital panopticon, as companies collect every data point that we produce to build extensive profiles of us to show us adverts. The large risks to us and society are not worth the substantial rewards that a relatively small number of adtech companies and intermediaries are receiving. Although some believe, as we saw in section 4.7, that current legislation already outlaws surveillance advertising, at least for certain users and data that require special protection, new legislation would be the best way to completely outlaw the practice.

Such legislation could specify the limits on what information is permitted to be sent out by website owners seeking to have adverts placed on their site. The legislation would prevent bid requests containing personal information being sent to the real-time bidding (RTB) network (or other system). We propose that nothing personally identifiable should be sent and that a 'green list' of data permitted to be sent be generated. To ensure that the advertisers still have enough relevant data to allow them to decide whether to place a bid to show an ad, the bid request should still contain some contextual information, such as data about the website and the specific page the user is on. To develop the framework for what data should be shared for advertising purposes, an extensive public engagement exercise should be undertaken to ensure there is broad informed support for the new advertising regime. Successfully implementing this would immediately prevent platforms using surveillance advertising on children.

In addition, to ban surveillance advertising not done through online auctions, the legislation would also need to ban website owners from selling ad space on their sites using the user profiles they have built up using personal data. A complete ban is the best way to ensure that the most vulnerable are protected as well as many other benefits (Box 1).

Sensing that change is on the horizon, the industry is already developing other means to provide adverts that are not as problematic. While some are starting to use the contextual targeting that we explore in Section 3.3, adtech giants, like Google and Criteo, are pushing for a form of collective targeting (Box 2).

BOX 1: WIDER BENEFITS OF ELIMINATING SURVEILLANCE ADVERTISING

- **Tackle data leaks.** One of the largest potential sources of personal data leaks would be instantly stopped. Since no personal data would be transmitted during the bid request, there would be no opportunity for those receiving the bid requests, such as companies like Cambridge Analytica, to harvest that data and link it to profiles.
- **Reduce the commodification of personal data.** It would diminish one of the major reasons for collecting personal data, ie to sell it on to brokers and platforms, who develop sophisticated profiles to enable advertisers to target us.
- **Force tech giants to diversify their business models.** Since the largest tech companies also hold some of the most detailed profiles about us and dominate the adtech space, they would need to find other ways to monetise their services, not based on constant surveillance.
- **Redistribute power away from the tech giants.** It would return some power to those sites and companies who have spent time producing content and have a dedicated user base. In this new world, advertisers would once again be buying space based on the destination rather than the individual.
- **Fight back against ad fraud.** Post-reform, adverts on fraudulent sites would hardly generate any revenue, since the price paid for adverts would be driven by the site quality and not by tracking users, thereby reducing the incentive to engage in these kinds of scams.

BOX 2: COLLECTIVE TARGETING

The adtech giants' preferred proposal is collective targeting. It allows continued data gathering and profiling, but no longer broadcasts this data to the wider adtech network. Under this proposal, adverts are targeted to cohorts, 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 over ad auction networks.

Under such proposals, a central gatekeeper (eg a browser) would be in control of individuals' data and assign them to relevant groups. Personal data would not be shared directly with advertisers. Ad auctions, which would normally operate by broadcasting data across multiple servers, would be designed to run locally, again minimising the opportunity for personal data escaping.

Proposals by adtech giants like Google[102] and Criteo[103] resolve some of the issues with surveillance advertising, such as preventing individualised targeting and the large-scale sharing of personal data with numerous adtech intermediaries. The grouping, however, would still expose people to potentially harmful ads, and would still require large-scale data collection and profiling of individuals. In addition, adding further technical complexity to the system would increase the reliance of advertisers and publishers on the adtech ecosystem.

Such proposals appear to be a move in the right direction, but many questions remain. For example, in a recent article, Johnny Ryan, of the Irish Council of Civil Liberties, notes that "Google has 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."[104]

FIGURE 7: A FRAMEWORK FOR UNDERSTANDING AD PERSONALISATION
SEGMENTING AUDIENCES BY THOSE WHO ARE LIKELY TO ENAGAGE WITH TAILORED ADS AND THOSE WHO SAY ADVERTISING HELPS THEM CHOOSE WHAT TO BUY.

Source: YouGov – https://yougov.co.uk/topics/consumer/articles-reports/2018/03/26/targeting-personalised-ads-right-audience

5.1.1 Make surveillance advertising illegal without age verification

A variation on a total prohibition of surveillance advertising that protects children but opens up the possibility of adults opting in to data collection, profiling, and surveillance advertising, is to allow adults to explicitly consent to this.

Of course, people are not one homogenous group but instead are diverse in nature and personality and therefore react differently to personalisation. Research by YouGov developed a framework that divides us into seven groups depending on whether we are more likely to engage with personalised adverts and whether we think that adverts help us choose what we want to buy (Figure 7).[105] In their model, over half (55%) of British adults say personalised adverts "creep them out" and so advertisers would be wise to avoid personalisation with them. However, the 9 million "personalised pioneers", representing 13.4% of the UK population, seek personalisation and consciously allow it to impact their decisions.

Under this option, we would legislate in the same way as for a total ban on surveillance advertising. This ensures that both adults and children are protected by default. As with the total ban, when we enter a website, it will not use any personal data or data profiles to serve surveillance advertising. However, those who can 'prove' themselves to be over 18, using one of the age-verification or age-assurance methods that we discuss in the next section, could switch on data gathering and personalisation.

This recognises that surveillance advertising can be harmful by design, and so only adults over the age of 18 should be able to consent to being subject to that potential harm. We already use this approach with other potentially harmful activities/substances that we prohibit for children, such as tobacco, alcohol, and gambling.

There was a similar proposal in the UK that adults would need to prove that they were over 18 to access adult material online. There were many concerns with the implementation of this policy: it did not include social media sites,[106] which are widely accepted to be where most underage porn viewing occurs[107]; it potentially creates a highly sensitive database of people's identities linked to their porn habits; and it was so easily circumventable that it was almost useless. The policy was, unsurprisingly, pulled at the last minute.[108]

The failure of this porn age-verification policy, however, is not a death knell for the proposal to ban surveillance advertising by default, while allowing some people to opt in. First, our policy will not include any loopholes for key companies. Second,

it will protect the majority of users by default, and for those who want to turn on data collection and personalisation, the net impact of having to provide data to prove their age to activate the functionality is less of an issue because the point is to opt into a digital world of data collection and surveillance adverts. In this case, providing a small amount of data to validate that they are over 18 is not a major concern. Third, it would not leave as dangerous a data trail, since all sites would have to operate this model, not just sensitive sites like pornography sites.

Finally, unless being exposed to personalisation and the full impact of the data collection economy becomes highly desirable for the under 18s, it would seem quite unlikely that we would see hordes of under-18-year-olds using virtual private networks (VPNs) and other more sophisticated tools to circumvent the protection. Indeed, the problem may in fact be reversed, as millions of people from around the world join the internet through a UK VPN service to take advantage of the enhanced privacy.

This section has provided two options which completely protect children from the harms of surveillance advertising. Where we make an exception, by allowing adults who can prove their age to opt into their data being used for surveillance advertising, we ensure that it is adults who take affirmative action. In the next section, we explore policies that fail to tackle the core problem of surveillance advertising, but still acknowledge the need for additional protection for children. In doing so, we shift the burden of taking responsibility onto our children.

5.2 ASSESSING AGE TO CUSTOMISE

In this section, we consider policy proposals that would require platforms to identify who is a child, so they can customise the user's experience to either allow surveillance advertising, or not, depending on their age. First, we explore the different ways in which age can be assessed and/or verified. Second, we look into how these practices could be adopted by companies either voluntarily or through regulation.

5.2.1 Age assurance and verification

There are three broad categories of data that can be used to help verify age. The first is to get the user to submit information, either through a self-assurance process or by providing some form of ID. It is important to distinguish here between verification, meaning actual hard proof of age, and seeking softer assurance, which can range from asking for our birthday to seeking parental consent. The second is the use of biometrics, with facial analysis being the most widely used of these services. Finally, there is behavioural analysis of user data, which the vast majority of platforms collect.

ID

Many systems have been developed that use ID to prove age, although the vast majority used today focus on enabling people to prove that they are an adult, rather than under 18 (or 13). The landscape is, however, broadly divided into two camps, namely those seeking some kind of soft assurance of age, generally suitable for content that poses low relative risk if exposed to the wrong age group, and verification backed up by hard facts that can be checked for more high-risk areas of the digital economy.

Where the risk is deemed low and soft assurance is an acceptable way forward, then there are a number of different ways to proceed. In the most basic, the user is asked to manually input their age. This is a system often used to validate the age requirement for creating an online account. Soft assurances, however, will not stop children accessing services like YouTube, Facebook, or Instagram. Research has shown that as many as 40% of 9–12-year-olds had lied about their age to gain access to an online service.[109] Some services, like Youtube, then use this information to decide whether to restrict harmful content such as adverts for high fat, sugar, or salt products (Case Study 3).

Although this is the age-verification system that most websites and platforms use, outside of heavily regulated sectors, like gambling, the European Data Protection Working Party has advised that self-declaration is not a sufficient proof of age to meet the requirements of the General Data Protection Regulation (GDPR). It goes on to clarify that if a child gives consent while underage, and the platform or website undertakes no verification, this would render the data processing unlawful.[xi]

xi Article 29 Data Protection Working Party Guidelines on consent under Regulation 2016/679, adopted on 28 November 2017 (17/EN, WP259 rev.01)

CASE STUDY 3: BLOCKING HFSS (HIGH FAT SUGAR SALT) ADVERTS TO UNDER 18s – YOUTUBE

YouTube, owned by Google, has initiated a policy to block junk food adverts for under 18s in the UK amid government efforts to tackle obesity. Under the policy, advertisers will be required to declare whether the advert is for a HFSS product, with failure to do so resulting in the adverts being pulled from YouTube.

Those adverts that are flagged will then not be shown to users that YouTube determines to be younger than 18. YouTube will calculate the user's age based on the self-entered birth date associated with the account. YouTube has stated that those who access videos without logging in will, by default, not be shown HFSS adverts.[110] The advertising restrictions will come into force in the UK and the EU in October 2021.

Despite extensive evidence of people lying about their age when creating accounts,[111] especially when being truthful would severely reduce or block access to the site or material, YouTube made no commitment to verify the self-assured age. This means that a 10-year-old who creates an account, lies about their age, then goes on to watch lots of cartoons and slime videos, will still be shown HFSS adverts on the platform.

Where the risk is deemed more serious, then the platform will want, and sometimes be required by law, to ensure that only people of the right age profile can access the service. Services that use this form of verification have for the most part arisen to verify that only adults access certain services, like gambling sites. Whereas soft assurance systems are mainly run by the platforms themselves, hard verification has spawned an age-verification industry. In this industry, there are two main ways that data can be submitted or assessed: utilising a large publicly held dataset, such as the electoral register, or ID that can be validated, such as a passport or driving licence. The benefit of using this kind of age verification is that it offers high certainty, but this comes at a cost. First, there is an increased risk to the individual of fraud, because our passports, if accessed without our consent, can help hackers steal our identity. Second, reliance on official data sources disadvantages those who, for various reasons, are not present in government databases or do not have a passport. The last UK census revealed that only 76% of people had a UK passport, and 17%, 9.5 million people, had no passport at all.[112] These systems are also expensive to maintain. Although, in some cases, like the electoral register, this arguably has to be done in any case, and the work to provide access to verify is not a significant extra burden.

However, the ability to use ID to prove that one is a child is much more limiting. Although many, but not all, will have passports, the information contained is valuable to hackers and would have to be treated with extreme care. Where someone has a mobile phone, this could be used to provide some age verification through new services being deployed by mobile operators. Providers already provide a service that blocks unsuitable sites by default, until the owner of the phone proves they are over 18.[113] A child who owns their own phone could use this to show that they are a child. A recent report found that, in the UK, 90% of children over 11 own a phone.[114]

What is perhaps most interesting is to consider whether soft age assurances might be sufficient in the case of surveillance advertising. In most areas where age verification occurs, there is a highly desirable forbidden fruit that minors seek to access. However, when providing an age to decide whether personal information and profiles are used for surveillance advertising, this is arguably not a highly desirable service that children will want to access. Would children lie to get surveillance advertising served to them?

CASE STUDY 4: AGESCAN BY YOTI

AgeScan is a service offered by Yoti that can estimate a person's age by scanning their face. The service was designed with user privacy and data minimisation in mind. It can be embedded into web pages or incorporated into apps, and only requires a webcam or mobile camera.

To use the service, users are not required to register with Yoti, nor do users need to provide any documentary evidence or otherwise of their identity. The service does not retain any information about users, nor any images of them that are used to estimate their age. Yoti claims that the images are not even stored, and so cannot be re-shared, re-used, or sold on. The image is also not stored locally on the terminal; it is securely transmitted to the Yoti backend server, currently hosted in the United Kingdom. To estimate age, it is compared against images in its own database. After the age estimate is performed, the captured facial image is deleted from Yoti's backend servers.

Currently, the service can only identify adults, and so can be used to help adults prove they are over 18 or, as in the case of the Yubo social networking platform, help identify adults in spaces designed for teenagers and young people, which when identified are flagged to a Yubo moderation team.

The service has been criticised by Privacy International for not treating user-provided data, such as passports and pictures, with the level of protection that their messaging implies.[115] Previously, photos submitted through the app (different to the photos received to do an AgeScan) were used to train its facial analysis algorithm, without this being clear. The terms of service have now been improved and made clearer, thanks to the issues publicly raised by Privacy International.[116]

In reality, the strong incentive to lie about their age during the sign-up process to get access to the platforms, such as YouTube or TikTok, would remain, since access to the site would trump any potential extra protection they could get from being truthful about their age. It is therefore doubtful whether reliance on soft assurances of age will offer much additional protection, while, at the same time, requiring ID or other firm validation on every site that operates surveillance advertising would not be practical or desirable.

Biometrics especially facial analysis

The potential for incorrect self-assurance, coupled with the problems raised around hard verification, has led to the rise of a new sector, where age verification is based on biometric data. Biometric data is defined in GDPR as follows:

Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic[xii] data.[xiii]

Because our biometric data cannot lie (even though we may not be assessed correctly by the system) and everyone has it, by default, this potentially makes it a good choice for industry. The use of biometrics to prove identity is becoming increasingly common. Many problems have been highlighted, with most attention placed on facial recognition technology (FRT) systems. Case study 4 above highlights one example of efforts to deliver a privacy respecting biometric system.

xii Dactyloscopy relies on the analysis and classification of patterns observed in individual finger prints.
xiii GDPR, Chapter I, Article 4, paragraph 14.

The proliferation of FRT systems is a danger. Any initiative that seeks out 'good' uses of the technology also feeds the wider industry. Broad adoption of FRT is likely to transform society and could enable large-scale abuse of human rights. Many activists contend that FRT is not just an iteration of CCTV technology, but something fundamentally different. Many are calling for a total ban, or at least a moratorium so that society can debate the "profound threat to human rights and to human society".[117] In addition, FRT systems, worryingly, do not have a legislative framework within which to operate. The Chair of UK Parliament Science and Technology Committee stated:

> *A legislative framework on the use of these technologies is urgently needed. Current trials should be stopped, and no further trials should take place until the right legal framework is in place.*[118]

Studies have found that these systems perform worse on any group that is not white male, in terms of correct matches and false positives.[119] As these systems are rolled out more broadly, we not only run the risk of using up police time verifying innocence, but we also risk creating a situation where non-white males are all disproportionately at risk of false positives. Recent work by the National Institute of Science and Technology in the USA "saw noticeable surges in false positives based on gender, age and racial background".[120]

The 2016 Annual Fraud Indicator report shows that identity fraud already costs the UK £5.39bn with the bulk of the fraud occurring online.[121] As criminal networks become more sophisticated, detailed, and ubiquitous, FRT systems may make us more vulnerable to fraud, rather than protect us. We would therefore caution whether the use of biometrics, and the serious dangers that it poses for individuals and society, make it the right tool to use to protect children from the impacts of surveillance advertising.

Behavioural data

The final category of data that could be used to identify who is over and under 18 is behavioural data. This is data that is generated as people use specific platforms. As noted in section 4.7.1, in many cases, especially when the data is of under-13-year-olds, this data will have been collected and processed without the required explicit consent.

The large platforms have long been challenged that they must know that there are myriad under-age users on their websites. Facebook, for example, was confronted with this in 2018, when an undercover reporter, training to be a moderator, was told to ignore users flagged as potentially underage. "We just like pretend that we are blind and that we don't know what underage looks like."[122] This embarrassing revelation led to Facebook changing their policy, and committing to locking "the accounts of users its moderators encounter and suspect are below the age of 13".[123] They stopped short, however, of using the data they already held on their users to identify underage users, presumably because they knew that such an exercise would reveal millions of underage users, and their removal would reduce their key success metric, the number of daily unique visitors, and their ad revenue.

The big platforms could easily enforce their own age policies. Taking the example of Facebook, the first thing a new user does is put up a profile photograph, and then makes 'friends', many of whom you would expect to be of the same age. They then go on to post pictures and comments about their school, classmates, and extracurricular activities. This gives plenty of information to figure out the rough age of platform users. Artificial intelligence (AI) surely can identify that serial Peppa Pig and Paw Patrol video watchers are likely to be under 13? The truth is that it is not in the interests of the platform to eject millions of users because this is how they monetise their product.

Although behavioural data is plentiful and already being gathered, this does not necessarily make it a good long-term solution to the problem of how to protect children and only allow actual adults to access age-restricted content or settings. For example, it would actively require the platforms to continually gather and process as much data as possible on all of their users. This would cement in ubiquitous surveillance, without the need for consent, across the whole internet and do away with important rights won by the implementation of the GDPR and similar legislation around the world.

On the other hand, it is undeniable that platforms, especially the big ones, have already collected and analysed vast quantities of personal data about almost all of their users. Platforms could, therefore,

potentially be required to use data that they already have in order to estimate age. This should not result in people being summarily evicted from their social media account, but instead would be a prompt for the user to provide additional evidence to prove their age. In addition, any data found for users under the age of 13 would have to be deleted, since it would not have been legally collected and processed, and compensation would have to be be paid to the child.

Internal documents leaked from TikTok indicate the platform is already using this data to estimate age. The documents show that more than 43% of UK users are deemed to be under 14.[124] This age has likely been selected because it includes 13/14-year-olds who are allowed on the platform, but the statistic clearly includes many who are under that age. There is no evidence that TikTok used this data to prompt additional age checks on any of their users, or used it to pre-emptively eject them from the site. Employees from TikTok have revealed that users' behavioural data, including online activity and social connections, is compared with others to establish an age.[125] They also confirmed that this can be merged with third-party data, as well as facial analysis of photos that are posted.

The TikTok insiders additionally claim that this sort of age estimation "is standard practice across our industry to use high-level age-modelling to better understand our users".[126] They also reveal that the main purpose of this data is not to protect their users or police their policies but instead "to inform corporate strategy" and they did not "use the classifications to automatically restrict or take down videos that might be from users under 13, or to secure permission from those users' parents or guardians".[127]

Therefore, while using behavioural data could be a useful tool to use as a transition mechanism, we do not recommend that platforms ubiquitously collect children's data to protect them from harm. There are better methods that do not come with associated data collection problems.

5.2.2 Implementation options

In the previous section, we analysed key age-assurance methods. We now look at how these approaches could be implemented. We explore two different options: voluntary commitments, either individual or collective, and legal obligations, including bans and fiduciary obligations.

Individual and collective voluntary agreements and commitments can be a good way to make progress on an issue when there is a lack of wider agreement or political avenue to implement legislative change. Throughout the report, we have highlighted companies, such as NPO, who have all departed from the accepted strategy and narrative around surveillance advertising and radically changed their behaviour. We are also seeing examples around marketing directly to children; for example, Mars' strategy as detailed in Case Study 5.

Such voluntary commitments take important steps towards stopping targeted advertising to children. Getting more large brands to make similar public commitments would send a powerful message around the acceptability of using surveillance advertising to target children.

CASE STUDY 5: MARS

Mars Wrigley is an industry leader in its approach to marketing to children online. It has committed to not using surveillance advertising, or other processes, to target children under 13, and will not collect and process any data from under-16-year-olds.

However, Mars, as the advertiser, does not have access to the exact age profile of every internet user. Instead, Mars assesses the user demographic of the platforms where it seeks to place adverts and does not advertise on platforms where over 25% of users are assessed to be under 13. Third-party auditing of Mars' online advertising shows that 98.4% comply with their guidelines.[128]

There remain serious limitations, however, to relying on voluntary action. If any company fails to achieve their stated goal, there is no recourse that individuals or society could take to enforce compliance or seek compensation. In addition, it is currently almost impossible for an advertiser to actually stop surveillance advertising to kids, because of the imperfect tools available for them to identify children in the mass of users. Voluntary commitments will therefore always fall short and would need the involvement and collaboration of adtech intermediaries and publishers to maximise impact.

Rather than rely on voluntary actions from corporations, legal restrictions, ie prohibiting any platform or website from providing a surveillance advert to children, could be introduced. This proposal is different to a total legal ban on surveillance advertising where adults could opt in. Here, surveillance advertising would be legal, but the platform would have to identify children and protect them, whereas the option discussed in section 5.1 starts from all surveillance advertising being illegal, unless the user opts in and proves they are over 18.

Another way to create legal obligations, without strict rules about what data can be used for which purpose, is to impose fiduciary obligations on companies that hold data about us (Box 3). This obligation would require companies to provide an active duty of care to data subjects. The basic concept is that when we give our personal information to an online company to get a service, that company should have a duty to do no harm and exercise care towards us when using that information.

Doctors, lawyers, and pension fund trustees are examples of professionals that (in many parts of the world) are bound by fiduciary obligations to serve patients' or clients' interests, rather than their own, especially where those interests may conflict. This is because in such professions, the professional has far greater expertise than the client, and therefore could exploit the information asymmetry for their own gain. Such information asymmetries are currently exploited in the digital economy.

BOX 3: INFORMATION FIDUCIARY

The concept of an information fiduciary was first articulated by Jack Balkin and Jonathan Zittrain in a paper published in 2016 highlighting the large conflicts of interest inherent to a digital surveillance economy, and how this dysfunctional relationship could be mended, and trust increased.[129] Their paper focuses on the similarities between professions, like lawyer or doctor, and new digital economy companies seeking to collect and monetise our personal data. They all involve a direct contractual relationship, either as a customer or a user. They all collect sensitive data about their customers or users, and they use that information to advise their customers or users on future courses of action. Finally, the power is one-sided in both cases. For example, online businesses can monitor their customers' activities, but those customers don't have reciprocal power.

This proposal is being examined with interest. The originators note that the "proposal has bipartisan appeal in [the US] Congress, because it protects consumers and corrects a clear market failure without the need for heavy-handed government intervention."[130]

Zittrain, however, notes that "a fiduciary duty wouldn't broadly rule out targeted advertising — dog owners would still get dog food ads — but it would preclude predatory advertising, like promotions for payday loans."[131] When applied to children, it would likely mean that although the majority of adverts would be deemed not in the child's best interests, some might still be allowed. This proposal, therefore, offers some protection, but with no examples of data fiduciary obligations, it is not yet possible to say how well they would operate. This is in large part because the harm of having the wrong medical operation or following inappropriate legal advice is obvious, whereas whether a particular advert is against our best interests is likely to be much more contested.

Our analysis shows we should proceed carefully before using age-verification systems to protect our children from surveillance advertising.[xiv] The children's digital rights charity, 5Rights, recently published an excellent proposal for a statutory code of practice for age-assurance technology (Box 4), which illuminates the challenges and sets the bar for how the technology should be used to protect children online.[132]

BOX 4: PROPOSED STATUTORY CODE OF PRACTICE FOR AGE ASSURANCE, 5RIGHTS

1. Age assurance must be privacy preserving.

2. Age assurance should be proportionate to risk and purpose.

3. Age assurance should be easy for the child to use.

4. Age assurance must enhance children's experiences, not merely restrict them.

5. Age assurance providers must offer a high level of security.

6. Age assurance providers must offer routes to challenge and redress.

7. Age assurance must be accessible and inclusive.

8. Age assurance must be transparent and accountable.

9. Age assurance should anticipate that children don't always tell the truth.

10. Age assurance must adhere to agreed standards.

11. Age assurance must be rights-respecting.

xiv This paper does not seek to say whether age-verification systems are appropriate in circumstances other than for the purpose of disabling surveillance advertising.

6. FRAMEWORK TO EVALUATE FUTURE PROPOSALS

This section proposes a framework to help policymakers and campaigners assess the merits of proposals to curb surveillance advertising to children. It does not, however, analyse the categories of solutions already presented to determine an optimal policy. This is because the framework can only be applied to concrete and specific solutions, not broad solution categories, as design and implementation have a large impact on outcomes. For instance, whether a particular solution creates an activity log or whether it is enforceable makes a big difference to the ultimate score, but these are not generic design choices.

We propose using six criteria to assess proposals to stop surveillance advertising to children, against which low and high scores will respectively represent low and high risks, as detailed in Table 1.

The first criterion is whether the proposed solution would lead to additional data being stored about the child. Given that our goal is to protect children and their data online, the best proposals will not lead to any additional data gathering. On the other hand, proposals based on platforms using behavioural data would score poorly.

The second criterion is whether the proposed solution would create an activity log, which links a specific user to all the sites that they have accessed. Activity logs are a form of data collection that pose significant risks because they provide detailed pictures of users' digital habits. The best proposals, therefore, will not create an activity log. Some may create an activity log but encrypt it, which is not ideal but better than creating a non-encrypted centralised database.

The third criterion is whether the solution requires access to sensitive public or private databases, such as a school's database and its unique child identifiers. Any solutions that use sensitive databases increase the risk of sensitive data being leaked, either on purpose or accidentally. The best solutions, therefore. will not access any sensitive data. Those accessing such databases remotely will receive a mid-range score to reflect the relative risk, while solutions that use a stored copy of a sensitive database will receive the poorest scores.

The fourth criterion is whether the proposed solution uses biometric data and whether it is stored. The use of biometric data, especially facial recognition technology (FRT), is fraught with risks, and our analysis suggests it should be heavily restricted. The framework therefore gives the best scores to solutions that do not use biometrics. We acknowledge that solutions, such as AgeScan, that scan faces to estimate their age, but do not store the images, are less problematic than many other biometric-based systems. Therefore, solutions that match users to created biometric databases are given the poorest scores.

The fifth criterion is enforceability. As we have seen throughout this report, there is lack of enforcement in many areas of the data economy and specifically within surveillance advertising. The best scores will therefore be given to solutions that would be directly enforceable in the courts. Proposals that place enforcement within bodies like the Information Commissioner's Office (ICO) receive mid-range scores, to reflect that, while this is better than no enforcement, national data protection authorities are often under-resourced. Finally, voluntary agreements score worst, as these are not enforceable.

The final criterion looks at who is responsible for ensuring that no surveillance advertising is shown to children. The best solutions are those that put responsibility onto the platforms themselves, because they have the resources and technical capabilities. A mid-point solution could be to put the responsibility onto internet service providers (ISPs), who act as our gateway to the internet. Finally, the worst scores were awarded to solutions that place the burden on parents, guardians, and children themselves.

One proposal discussed in this report is specific enough to be assessed against our framework – a total ban on surveillance advertising. This proposal would achieve a low (good) score in all categories, because it would not lead to additional data collection, would not create an activity log, would not use any sensitive data, would not use any biometrics, would be legally enforceable, and would place the responsibility with the tech companies and platforms. It thus provides a baseline standard that other proposals could be compared against.

TABLE 1: FRAMEWORK TO EVALUATE FUTURE PROPOSALS

Framework		
Criteria	**Explanation**	**Scoring**
Additional data collected and stored	Does the proposed solution lead to additional data being stored about the child?	1 – No additional data stored 3 - Some additional data stored 5 – Significant additional data stored
Activity log	Does the solution create a database of users and the sites that they access?	1 – No activity log 3 – Encrypted activity log 5 – Activity log
Use of sensitive data	Does the solution require access to sensitive public or private databases (ie a school's database for unique child identifiers)?	1 – Does not access any sensitive data 3 – Remotely accesses sensitive data 5 – Uses stored copy of database
Use of biometrics	Does the proposed solution use biometric data? Do they store the biometric data?	1 – No use of biometrics 3 – Use of biometrics 5 – Use of stored biometrics
Enforceability	How enforceable is the proposal if not followed?	1 – Legally enforceable 3 – Enforceable by regulator 5 – Not enforceable
Responsibility	Who is responsible for ensuring that the child does not see adverts?	1 – Platform 3 – ISP 5 – Parent/guardian

7. CONCLUSION

We are frequently told that surveillance advertising is vital because it is the best way to keep large parts of the digital economy 'free' to access, as website publishers can earn revenue through advertising rather than charging. Supposedly everyone wins. This report has shown that there are in fact many losers when it comes to surveillance advertising, both at the individual level and for wider society. The only entities really benefiting from surveillance advertising are the adtech companies.

For years, there has been a growing chorus of voices describing the dangerous consequences of surveillance 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.*[133]

On 3 March 2021, Google, a company at the heart of creating and promoting surveillance advertising, published a blog confirming that it would change its online advertising system, and that it now opposes "any technology used for tracking individual people as they browse the web".[134]

We therefore must take action to guide tech companies and communities to create a new digital environment that protects people, and particularly children, from the harms of surveillance advertising. This report sets out a six-criteria framework against which reform proposals could be assessed: additional data collection and storage, activity log, use of sensitive data, use of biometrics, enforceability, and responsibility. A total ban on surveillance advertising scores well against all six criteria. It would do the most to ensure children are no longer subject to surveillance advertising, reduce data leaks, force tech companies to diversify their business models, redistribute power away from the tech giants, and fight back against ad fraud. It also avoids issues introduced by the implementation of age-assessment or age-verification methods such as additional data gathering, activity logs, and the use of biometric data. Finally, it changes the very nature of the data economy because it decommodifies our personal data and greatly reduces the incentive to collect, store, sell, and share it.

This would be a seismic shift in the foundations of the digital economy; however, some of the other proposals discussed in this report are also worth considering. For instance, requiring platforms to use their existing behavioural data to identify potential child users of their platform could be implemented as a transition mechanism.

In addition, the concept of information fiduciary is very promising, even though it only offers partial protection against surveillance advertising. If implemented well, it could re-balance the power dynamic between a platform and its users and play a large part in helping to nurture a new digital economy.

The framework proposed in this report could be used to explore the relative pros and cons of these alternative policies. This has not, however, been done in this report. The framework can only be applied to concrete and specific solutions, not the broad solution categories presented, as design and implementation have a large impact on outcomes.

ENDNOTES

1 Livingstone, S., Byrne, J., & Carr, J. (2016). *One in three: Internet governance and children's rights*. Unicef. Retrieved from https://www.unicef-irc.org/publications/795-one-in-three-internet-governance-and-childrens-rights.html

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

3 Brownlow J., Zaki M., Neely A. & Urmetzer F. (2015). *Data and analytics - data-driven business models: A blueprint for innovation - The competitive advantage of the new Big Data world*. Cambridge Service Alliance. Retrieved from https://cambridgeservicealliance.eng.cam.ac.uk/resources/Downloads/Monthly%20Papers/2015MarchPaperTheDDBMInnovationBlueprint.pdf

4 Lapierre, M. A., Fleming-Milici, F., Rozendaal, E., McAlister, A. R., & Castonguay, J. (2017). The effect of advertising on children and adolescents. *Pediatrics*, 140 (2) S152-S156; DOI: 10.1542/peds.2016-1758V

5 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

6 Skibinski, M. (n.d.). *Advertising on COVID 19 misinformation*. NewsGuard. Retrieved from https://www.newsguardtech.com/special-report-advertising-on-covid-19-misinformation/

7 Pidgeon, D. (2020). *15% of programmatic supply chain hosts unattributable*. Mediatel News. Retrieved from https://mediatel.co.uk/news/2020/05/06/isba-pwc-third-of-programmatic-supply-chain-costs-unattributable/

8 *Ibid*.

9 Lomas, N. (2021). F*acebook knew for years that ad read estimates were based on the wrong data but blocked fixes over revenue impact, per court filing*. Extra Crunch. Retrieved from 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/

10 Sloane, G. (2020). *LinkedIn discloses inflated metrics glitch 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

11 Livingstone, S., Byrne, J., & Carr, J. (2016). *One in three: Internet governance and children's rights*. Unicef. Retrieved from https://www.unicef-irc.org/publications/795-one-in-three-internet-governance-and-childrens-rights.html

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

13 IAB. (2019). *Total UK digital ad spend, full year 2019.* Internet Advertising Bureau. Retrieved from https://www.iabuk.com/sites/default/files/public_files/Digital-Adspend-2019-One%20Pager.pdf

14 Ofcom Online nation 2020 report - Oliver & Ohlbaum estimates and analysis, based on data from AA/WARC, PwC Global Entertainment and Media Outlook, Enders Analysis (based on company data and AA/WARC), Zenith, Statista, the e-Commerce Foundation, company reporting and public filings. UK adjusted for CPI at 2019 prices by Ofcom.

15 Enberg, J. (2019). *Global digital ad spending 2019.* eMarketer. Retrieved from https://www.emarketer.com/content/global-digital-ad-spending-2019

16 Brownlow J., Zaki M., Neely A. & Urmetzer F. (2015). *Data and analytics - data-driven business models: A blueprint for innovation - The competitive advantage of the new Big Data world.* Cambridge Service Alliance. Retrieved from https://cambridgeservicealliance.eng.cam.ac.uk/resources/Downloads/Monthly%20Papers/2015MarchPaperTheDDBMInnovationBlueprint.pdf

17 McCann v Google. (n.d.). *McCann v Google* [webpage]. Retrieved from https://www.youtubedataclaim.co.uk/ [accessed 6 May 2021].

18 Worledge, M. & Bamford, M. (2019). *Adtech market research report*. ICO. Retrieved from https://ico.org.uk/media/about-the-ico/documents/2614568/ico-ofcom-adtech-research-20190320.pdf

19 BBC News. (2021). *TikTok sued for billions over use of children's data.* BBC News, 21 April. Retrieved from https://www.bbc.com/news/technology-56815480?at_custom1=%5Bpost+type%5D&at_medium=custom7&at_campaign=64&at_custom2=twitter&at_custom4=E1932048-A260-11EB-AD9C-3A914744363C

20 ICO. (n.d.). *Lawful basis for processing.* Information Commissioner's Office. Retrieved from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/ [accessed 6 May 2021].

21 Collins, D. (2017). *How much data to adtech companies collect on kids before they turn 13?* SuperAwesome. Retrieved from https://www.superawesome.com/blog/how-much-data-do-adtech-companies-collect-on-kids-before-they-turn-13/

22 Lafrance, A. (2019). *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/

23 Ryan J. (2020). *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*. Submission to the Irish Data Protection Commission. Retrieved from https://www.iccl.ie/wp-content/uploads/2020/09/1.-Submission-to-Data-Protection-Commissioner.pdf#page=9

24 McCann, D. & Hall, M. (2018). *Blocking the data stalkers.* London: NEF. Retrieved from https://neweconomics.org/uploads/files/NEF_Blocking_Data_Stalkers.pdf

25 Mars. (2020). *Mars Marketing Code for Human Food 2020 Governance Report*. Retrieved from https://lighthouse.mars.com/adaptivemedia/rendition/id_7877ef09282bd16de184fb74c1193ffa83363c1f/name_out/MMC%20Governance%20Report%20-%202020.pdf

26 Lomas, N. (2019). *Targeted ads offer little extra value for online publishers, study suggests.* Tech Crunch. Retrieved from https://techcrunch.com/2019/05/31/targeted-ads-offer-little-extra-value-for-online-publishers-study-suggests/

27 Brave. (2020). *NPO* [webpage]. Retrieved from https://brave.com/npo/

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

29 *Ibid*.

30 Pidgeon, D. (2020). *15% of programmatic supply chain hosts unattributable*. Mediatel News. Retrieved from https://mediatel.co.uk/news/2020/05/06/isba-pwc-third-of-programmatic-supply-chain-costs-unattributable/

31 *Ibid*.

32 Lomas, N. (2021). *Facebook new for years that ad read estimates were based on the wrong data but blocked fixes over revenue impact, per court filing.* Extra Crunch. Retrieved from 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/

33 Sloane, G. (2020). *LinkedIn discloses inflated metrics glitch 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

34 Lapierre, M. A., Fleming-Milici, F., Rozendaal, E., McAlister, A. R., & Castonguay, J. (2017). The effect of advertising on children and adolescents. *Pediatrics*, 140 (2) S152-S156; DOI: 10.1542/peds.2016-1758V

35 Hayes, O. & Parker, N. (n.d.). *Kids for sale.* Global Action Plan. Retrieved from https://www.globalactionplan.org.uk/files/kids_for_sale.pdf [accessed 6 May 2021].

36 Lee Reynolds, L. (2019). Marketing, technology, and consumerism. *The Ecologist*. Retrieved from https://theecologist.org/2019/feb/26/marketing-technology-and-consumerism

37 Abu-Saud, Z. (2013). *The dogma of advertising and consumerism*. The Huffington Post. Retrieved from https://www.huffingtonpost.co.uk/ziad-elhady/the-dogma-of-advertising-_b_2540390.html

38 WARC. (2019). *Ads are unrepresentative and set unrealistic expectations.* World Advertising Research Center. Retrieved from https://www.warc.com/newsandopinion/news/ads-are-unrepresentative-and-set-unrealistic-expectations/42684

39 Brusseau, J. (2012). *Business Ethics.* Retrieved from https://2012books.lardbucket.org/books/business-ethics/s16-03-we-buy-therefore-we-are-consum.html

40 CCFC. (n.d.). *Marketing and materialism*. Retrieved from https://commercialfreechildhood.org/wp-content/uploads/2019/10/materialism_fact_sheet.pdf

41 Easterbrook, M., Wright, M., Dittmar, H., & Banerjee, R. (2014). Consumer culture ideals, extrinsic motivations, and well-being in children. *European Journal of Social Psychology*, 44(4), 349–359. doi: 10.1002/ejsp.2020

42 Ku, L., Dittmar, H., & Banerjee, R. (2014). To have or to learn? The effects of materialism on British and Chinese children's learning. *Journal of Personality and Social Psychology*, 106(5), 803–821. doi: 10.1037/a0036038

43 Kiang, L., Mendonça, S., Liang, Y., Payir, A., O'Brien, L., Tudge, J., & Freitas, L. (2016). If children won lotteries: materialism, gratitude and imaginary windfall spending. *Young Consumers*, 17(4), 404–418. doi: 10.1108/yc-07-2016-00614

44 Kasser, T., Moore, K., & Lippman, L. (2005). *Frugality, generosity, and materialism in children and adolescents. In What do children need to flourish? Conceptualizing and measuring indicators of positive development, Vol. 3.* The Search Institute Series on Developmentally Attentive Community and Society, pp. 357–373. Boston, MA: Springer US.

45 Jalbro, G. (2002). *Children and advertising on television: A survey of the research, 1994–2000.* Nordicom. Retrieved from https://www.nordicom.gu.se/sites/default/files/kapitel-pdf/34_Jarlbro.pdf

46 Ofcom. (2019). *Children and parents: media use and attitudes 2019*. Office of Communications. Retrieved from https://www.ofcom.org.uk/__data/assets/pdf_file/0023/190616/children-media-use-attitudes-2019-report.pdf

47 Hayes, O. & Parker, N. (n.d.). *Kids for sale*. Global Action Plan, p. 5. Retrieved from https://www.globalactionplan.org.uk/files/kids_for_sale.pdf [accessed 6 May 2021].

48 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

49 Fagan ,C. & Wright, L. (2020). *Ad tech fuels disinformation sites in Europe: the numbers and the players.* Global Disinformation Index. Retrieved from https://disinformationindex.org/wp-content/uploads/2020/03/GDI_Adtech_EU.pdf

50 Sydell, L. (2016). *We tracked down a fake news creator in the suburbs: This is what we learned*. NPR. Retrieved from https://text.npr.org/503146770

51 Silber, A. (2002). *Clickbait and traffic laundering: How ad tech is destroying the web.* The Guerrilla Agency. Retrieved from https://theguerrilla.agency/clickbait-and-traffic-laundering-how-ad-tech-is-destroying-the-web

52 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

53 Skibinski, M. (n.d.). *Advertising on COVID 19 misinformation.* NewsGuard. Retrieved from https://www.newsguardtech.com/special-report-advertising-on-covid-19-misinformation/

54 *Ibid*.

55 Bateman, C. (2021). *Fake news: Half of UK kids saw more online misinformation in 2020, survey finds.* Sky News. Retrieved from https://news.sky.com/story/fake-news-half-of-uk-kids-saw-more-online-misinformation-in-2020-survey-finds-12213722

56 *Ibid*.

57 Cockburn, H. (2019). Schools to teach kids about fake news and confirmation bias, government announces. *The Independent*. Retrieved from https://www.independent.co.uk/news/education/education-news/fake-news-schools-education-online-risks-confirmation-bias-damian-hinds-government-a9004516.html

58 Horwitz, J. & Seetharaman, D. (2020). Facebook executives shut down efforts to make the site less divisive. *Wall Street Journal*. Retrieved from https://www.wsj.com/articles/facebook-knows-it-encourages-division-top-executives-nixed-solutions-11590507499

59 Angwin, J., Tobin, A., & Varnet, M. (2017). *Facebook (still) letting housing advertisers exclude users by race.* ProPublica. Retrieved from https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin

60 Kirkpatrick, D. (2016). *71% of consumers prefer personalized ads.* Marketing Dive. Retrieved from https://www.marketingdive.com/news/study-71-of-consumers-prefer-personalized-ads/418831/

61 *Ibid*.

62 *Ibid*.

63 Worledge, M. & Bamford, M. (2019). *Adtech market research report*. ICO. Retrieved from https://ico.org.uk/media/about-the-ico/documents/2614568/ico-ofcom-adtech-research-20190320.pdf

64 *Ibid*.

65 RSA. (2019) *The dark side of consumer data*. Retrieved from https://www.rsa.com/en-us/company/news/the-dark-side-of-customer-data

66 Global Web Index (2019) *Ad-blocking behaviour around the world.* Retrieved from https://www.globalwebindex.com/reports/global-ad-blocking-behavior

67 Worledge, M. & Bamford, M. (2019). *Adtech market research report.* ICO. Retrieved from https://ico.org.uk/media/about-the-ico/documents/2614568/ico-ofcom-adtech-research-20190320.pdf

68 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

69 Claburn, T. (2019). *Bad news; Unblockable web trackers emerge. Good news: Firefox, with uBlock Origin can stop it, Chrome not so much*. The Register. Retrieved from https://www.theregister.com/2019/11/21/ublock_origin_firefox_unblockable_tracker/

70 *Ibid*.

71 Mass News. (2019). *The rise of digital fingerprinting.* Retrieved from https://www.massnews.com/the-rise-of-digital-fingerprinting/

72 Terlep, S., Higgins, T., & Haggin, P. (2015). P&G worked with China trade group on tech to sidestep Apple privacy rules. *Wall Street Journal.* Retrieved from https://www.wsj.com/articles/p-g-worked-with-china-trade-group-on-tech-to-sidestep-apple-privacy-rules-11617902840

73 Kasser, T., & Linn, S. (2016). Growing Up under Corporate Capitalism: The Problem of Marketing to Children, with Suggestions for Policy Solutions. *Social Issues and Policy Review*, 10(1), 122 150.

74 Barnhart, B. (2021). *The most important Instagram statistics you need to know for 2021*. Sprout Social. Retrieved from https://sproutsocial.com/insights/instagram-stats/

75 Hayes, O. & Parker, N. (n.d.). *Kids for sale*. Global Action Plan. Retrieved from https://www.globalactionplan.org.uk/files/kids_for_sale.pdf [accessed 6 May 2021].

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

77 Pärssinen, M., Kotila, M., Cuevas, R., Phansalkar, A., & Manner, J. (2018). Environmental impact assessment of online advertising. *Environmental Impact Assessment Review*, 73, 177–200. Retrieved from https://www.sciencedirect.com/science/article/pii/S0195925517303505

78 Le Page, M. (2018). AI's dirty secret: Energy guzzling machines may fuel global warming. *New Scientist.* Retrieved from https://www.newscientist.com/article/mg24031992-100-ais-dirty-secret-energy-guzzling-machines-may-fuel-global-warming/

79 Delli Santi, 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/

80 ICO. (2019). *Update report into adtech and real-time bidding.* Information Commissioner's Office. Retrieved from https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf

81 *Ibid*.

82 Open Rights Group. (n.d.). *Help us protect your data from illegal ads.* Retrieved from https://action.openrightsgroup.org/help-us-protect-your-data-illegal-ads [accessed 6 May 2021].

83 Irish Council for Civil Liberties. (n.d.). *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/ [accessed 6 May 2021].

84 Singer, N. (2021). Disney and ad-tech firms agree to privacy change for children's apps. *New York Times*. Retrieved from https://www.nytimes.com/2021/04/13/technology/advertising-children-privacy.html

85 ICO. (2019). *Update report into adtech and real-time bidding.* Information Commissioner's Office. Retrieved from https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf

86 McCann v Google. (n.d.). *McCann v Google* [webpage]. Retrieved from https://www.youtubedataclaim.co.uk/Home/Faq [accessed 6 May 2021].

87 Bolton, D. (2015). Ashley Madison leak: The personal details of 32 million users might not all be genuine. *The Independent.* Retrieved from https://www.independent.co.uk/life-style/gadgets-and-tech/news/ashley-madison-hack-live-email-verification-10461653.html

88 Lockert, M. (2021). *How hackers use your information.* Credit Karma. Retrieved from https://www.creditkarma.com/id-theft/i/how-hackers-use-your-information

89 5Rights Age (2021) *But how do they know it is a child.* Retrieved from https://5rightsfoundation.com/in-action/but-how-do-they-know-it-is-a-child-age-assurance-in-the-digital-world.html

90 Hern, A. & Ledegaard, F. H. (2019). Children interested in gambling and alcohol, according to Facebook. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2019/oct/09/children-interested-in-gambling-and-alcohol-facebook

91 Hicken, M. (2013). *Find out what Big Data knows about you (it may be very wrong)*. Money. Retrieved from https://money.cnn.com/2013/09/05/pf/acxiom-consumer-data/

92 McCann, D. & Hall, M. (2018). *Blocking the Data Stalkers.* London: NEF. Retrieved from https://neweconomics.org/2018/12/blocking-the-data-stalkers

93 Pasquale, F. (2018). *Our lives in a scored society*. Retrieved from https://mondediplo.com/2018/05/05data

94 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

95 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

96 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

97 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

98 Slefo, G. (2015). *Report: For every $3 spent on digital ads, fraud takes $1.* Adage. Retrieved from https://adage.com/article/digital/ad-fraud-eating-digital-advertising-revenue/301017

99 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

100 Smiley, M. (2016). *ANA report finds rebates to be widespread in US media landscape*. The Drum. Retrieved from https://www.thedrum.com/news/2016/06/07/ana-report-finds-rebates-be-widespread-us-media-landscape

101 Leathern, R. (2016). *The subprime ad crisis is here*. Medium. Retrieved from https://medium.com/@robleathern/the-subprime-ad-crisis-is-here-6ac028133c93

102 Tingleff, S. (2020). *Explaining the privacy sandbox explainers*. IAB Tech Labs. Retrieved from https://iabtechlab.com/blog/explaining-the-privacy-sandbox-explainers/

103 Criteo. (n.d.). *Glossary of terms* [webpage]. Retrieved from https://www.criteo.com/digital-advertising-glossary/sparrow/ [accessed 6 May 2021].

104 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/

105 Sevak, T. (2018). *Targeting personalised ads to the right audience.* YouGov. Retrieved from https://yougov.co.uk/topics/consumer/articles-reports/2018/03/26/targeting-personalised-ads-right-audience

106 Manavis, S. (2019). The government's age restrictions on porn create more problems than they solve. *New Statesman.* Retrieved from https://www.newstatesman.com/politics/uk/2019/04/governments-age-restrictions-porn-create-more-problems-they-solve

107 The Scotsman. (2019) *Social media gives children access to porn, claims new documentary.* Retrieved from https://www.scotsman.com/news/politics/social-media-gives-children-access-porn-claims-new-documentary-1413591

108 BBC News. (2019). *The UK's controversial 'porn blocker' plan dropped*. BBC News. Retrieved from https://www.bbc.co.uk/news/technology-50073102

109 Aiken, M. (2016). *The kids who lie about their age to join Facebook*. The Atlantic. Retrieved from https://www.theatlantic.com/technology/archive/2016/08/the-social-media-invisibles/497729/

110 Pinkstone, J. (2020). YouTube block junk food adverts. *The Daily Mail.* Retrieved from https://www.dailymail.co.uk/sciencetech/article-8599571/Google-YouTube-BLOCK-junk-food-adverts-18s.html

111 Young, S. (2019). Social media being used by a growing number of children under 11 despite age limits. *The Independent.* Retrieved from https://www.independent.co.uk/life-style/children-social-media-use-age-limit-facebook-instagram-profiles-a8756096.html

112 ONS. (2013). *Detailed country of birth and nationality analysis from the 2011 Census of England and Wales.* Office for National Statistics. Retrieved from http://webarchive.nationalarchives.gov.uk/20160107124139/http://www.ons.gov.uk/ons/dcp171776_310441.pdf

113 O2. (2011). *Mobile phones and age verification: your questions answered*. Retrieved from https://news.o2.co.uk/2011/03/03/mobile-phones-and-age-verification-your-questions-answered/

114 PA Media. (2020). Most children own mobile phones by the age of seven, study finds. *The Guardian.* Retrieved from https://www.theguardian.com/society/2020/jan/30/most-children-own-mobile-phone-by-age-of-seven-study-finds

115 PI. (2020). *Identity gatekeepers and the future of digital identity.* Privacy International. Retrieved from https://privacyinternational.org/long-read/3254/identity-gatekeepers-and-future-digital-identity

116 PI. (2019). *Yoti Letters.* Privacy International. Retrieved from https://privacyinternational.org/node/3266

117 Buncombe, A. (2019). Facial recognition: Activists call for ban of government use of technology that is a 'profound threat to humanity'. *The Independent*. Retrieved from https://www.independent.co.uk/news/world/americas/facial-recognition-technology-ban-us-government-privacy-ice-fight-for-the-future-a8997706.html

118 Hall, K. (2019). *Those facial recognition trials in the UK? They should be banned, warned Parliamentary committee.* The Register. Retrieved from https://www.theregister.co.uk/2019/07/18/uk_government_facial_recognition/

119 Singer, N. & Metz, C. (2019). Many facial-recognition systems are biased, says U.S. study. *New York Times.* Retrieved from https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html

120 Boutin, C. (2019). *NIST study evaluates effects of race, age, and sec on face recognition software*. National Institute of Standards and Technology. Retrieved from https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software

121 Experian *et al.* (2016) *Annual Fraud Indicator 2016.* Retrieved from https://ex.broxbourne.gov.uk/sites/default/files/meetings/Annual%20Fraud%20Indicator%202016.pdf

122 Hutchinson, A. (2018). *Facebook to expand efforts to detect underage users after reports of inaction.* Social Media Today. Retrieved from https://www.socialmediatoday.com/news/facebook-to-expand-efforts-to-detect-underage-users-after-reports-of-inacti/528230/

123 Constine, J. (2018). *Facebook and Instagram change to crack down on underage children.* Tech Crunch. Retrieved from https://techcrunch.com/2018/07/19/facebok-under-13

124 Zhong, R. & Frenkel, S. (2020). A third of TikTok's U.S. users may be 14 or under, raising safety questions. *New York Times.* Retrieved from https://www.nytimes.com/2020/08/14/technology/tiktok-underage-users-ftc.html

125 *Ibid*.

126 *Ibid*.

127 *Ibid*.

128 Mars. (2020). *Mars Marketing Code for Human Food 2020 Governance Report.* Retrieved from https://lighthouse.mars.com/adaptivemedia/rendition/id_7877ef09282bd16de184fb74c1193ffa83363c1f/name_out/MMC%20Governance%20Report%20-%202020.pdf

129 Balkin, M & Zittrain, J. (2016) *A grand bargain to make tech companies trustworthy.* The Atlantic. Retrieved from https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/

130 Zittrain, J. (2019). *How to exercise the power you didn't ask for*. Harvard Blogs. Retrieved from https://blogs.harvard.edu/jzwrites/2018/10/29/how-to-exercise-the-power-you-didnt-ask-for/

131 *Ibid*.

132 5RightsFoundation. (n.d.). *But how do they know it is a child?* [webpage]. Retrieved from https://5rightsfoundation.com/in-action/but-how-do-they-know-it-is-a-child-age-assurance-in-the-digital-world.html

133 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

134 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

WWW.NEWECONOMICS.ORG
info@neweconomics.org
+44 (0)20 7820 6300 @NEF
Registered charity number 1055254

COVER IMAGE BY:
NRuedisueli via iStockPhoto

PUBLISHED:
May 2021

Global Action Plan is a charity that is working for a green and thriving planet where people enjoy their lives within the Earth's resources. We do this by making connections between what is good for people and good for the planet.

Our *End Surveillance Advertising to Kids* campaign brings people together to challenge the tech platforms' surveillance advertising business model, which drives harmful consumerism and plummeting youth wellbeing.

WRITTEN BY:
Duncan McCann