Understanding the **digital media ecosystem**

How the evolution of the digital marketing ecosystem impacts tobacco, alcohol and unhealthy food marketing

Abstract

The digital ecosystem for tobacco, alcohol and unhealthy food marketing is complex and is changing quickly. Understanding the digital ecosystem is essential to being able to make decisions and advise policy-makers on what is needed to ensure that children are safe and not exposed to marketing of unhealthy foods – those high in fats, sugars and/or salt – which the evidence shows has a strong impact on children's eating behaviour. WHO has a key role to play in monitoring, measuring, educating and informing the policy debate on regulation and control of the digital media ecosystem. This paper summarizes recent changes in the digital ecosystem in detail, explains which factors and stakeholders are driving these changes and sets out the consequences for food digital marketing of these ongoing changes.

Understanding the **digital media ecosystem**

How the evolution of the digital marketing ecosystem impacts tobacco, alcohol and unhealthy food marketing

Contents

Acknowledgements

Abbreviations

AAID	Android advertising ID
API	application programme interface
ASA	Advertising Standards Authority (United Kingdom)
CAPTCHA	completely automated public Turing test to tell computers and humans apart
CCPA	California Consumer Privacy Act
CLICK	Comprehend the digital ecosystem; Landscape of campaigns; Investigative exposure; Capture on screen; and Knowledge sharing (framework)
CMA	Competition and Markets Authority (United Kingdom)
DCMS	Department for Digital, Culture, Media and Sport (United Kingdom)
DMP	data-management platform
DPIA	digital protection impact assessment
DSP	demand-side platform
DV360	Google Display & Video 360
EU	European Union
FAN	Facebook Audience Network
FCA	Financial Conduct Authority (United Kingdom)
FLoC	Federated Learning of Cohorts
GDPR	(European Union) General Data Protection Regulation
HFSS	foods that are high in fats, sugars and/or salt
ICO	Information Commissioner's Office (United Kingdom)
IDFA	Apple iOS ID for advertising
IP	Internet protocol
MAID	mobile ad identifier
NCDs	noncommunicable diseases
OECD	Organisation for Economic Co-operation and Development
OOH	out-of-home (advertising)
PECR	privacy and electronic communication regulation
PIGIN	private interest groups including noise
PII	personally identifiable information
SSP	supply-side platform
TURTLEDOVE	two uncorrelated requests, then locally executed decision on victory (Google)
VAN	vertical ad network
W3C	Worldwide Web Consortium

Glossary

Ad tech wiring/rails – the technology systems that allow the advertising ecosystem to operate.

Addressable media – digital media that can be targeted at an individual user and collect person-level measurement data.

Advanced targeting technologies – new technologies and approaches that enable contextual targeting instead of personalized ad targeting.

Advertiser ad server market – technology companies that provide advertising serving platforms (the technology that serves a specific ad creative to a specific advertising slot) to brands and agencies, as well as publishers.

Application programme interface – a connection between computers and computer programmes that enables interoperability between systems.

Attribution – the process of determining the user actions that led to the desired outcome between the click of the ad and the conversion on a website or app.

Authenticated web – any Internet site where a user's identity is verified by logging in to a publisher, producing an authentication token.

Big Tech – refers to the largest technology platforms that play a leading role in the Internet – usually Google, Apple, Facebook, Amazon and Microsoft.

Cookie – small blocks of data created by a web server while a user is browsing a website and placed on the user's computer or other device by the user's web browser.

Clean rooms – a secure, protected technology environment where personally identifiable information data are anonymized, processed and stored to be made available for analysis and measurement by third parties.

Consumer consent management solutions – software platforms that help publishers collect consumer opt-in consents to comply with data-protection laws, such as the European Union General Data Protection Regulation, by providing consumers with information about their privacy options and about the data types that will be collected when providing their consenting on the form.

Connected television – a device that connects to, or is embedded in, a television screen to support Internet access and streamed video content.

Contextual targeting – the selling of advertising audiences defined by the content or publication they are consuming.

Device fingerprinting – a process used to identify a device or browser based on its standard and bespoke configuration, to identify the device for future targeting of advertising. Device fingerprinting is a process used to identify a device or browser by determining which technology, such as the operating system and browser plugins along with other active settings, are present. It is used to track users and determine if they are unique or a known visitor (Netacea, 2021).

Data-management platforms – a software platform used for collecting, organizing and distributing data, allowing businesses to identify audience segments for targeting of advertising.

Demand-side platforms – technology platforms used by brands and agencies to buy targeted programmatic media.

DoubleClick for Publishers – Google's supply-side platform.

Display advertising – online advertising using banner ads and other visual ad formats.

Edge computing – a distributed computing architecture that brings computation and data storage closer to the sources of data.

First–party data – data that an entity (brands and publishers) have collected with permission from their own consumers. The permissions determine the rights of the entity for the use of the data.

Header bidding – a new approach to exchange transactions designed to improve yield for publishers in which to maximize the win and gain more control over the bidding process, publishers offer an ad impression to several ad exchanges simultaneously. By giving the chance to bid on an ad to multiple demand source bidders, the profit of the publisher can be increased by accepting the best offer (Morrisroe, 2020).

Identify graphs – a software system for resolving the identity of a consumer across disparate data sources, devices, channels and identity relationships.

Last or multi-touch attribution – an advertising effectiveness measurement technique which identifies and ascribes value to all customer touchpoints in a journey that lead to an outcome.

Mobile ad ID – the mobile ad ID (either the Apple iOS ID for advertising or the Android advertising ID) identifies phones and devices for advertising and is given by the device's operation system. The ID contains randomly selected numbers and letters and is used by advertisers to identify a device. The mobile ID can be used by free phone applications to understand the user and their choices and behaviour.

Native advertising – the use of paid ads that match the look, feel and function of the media format in which they appear. Native ads are often found in social media feeds, or as recommended content on a web page (Outbrain, 2021).

Non-personally identifiable information – any data that do not directly identify an individual. In the United States of America, this includes proxy identifiers such as cookies, mobile ad identifiers, Internet protocol addresses and other identifiers that may be unique but do not allow direct recognition of the individual. Under the European Union General Data Protection Regulation, it can still be classified as Personal Data that require explicit opt-in consent to be used for the targeting of advertising.

Open Bidding – a form of programmatic advertising now provided by Google that allows ad sources to bid on each advertising impression in real time. Unlike traditional mediation that uses historical data to prioritize networks and call them one at a time, Open Bidding calls all participating networks simultaneously, enabling them to compete equally in a single, unified auction (Google Ad Manager, 2021).

Open ecosystem – the independent publishers and technology platforms that sit outside of the Big Tech walled gardens owned by, for instance, Facebook, Google and Microsoft.

Over-the-top television – a media service offered directly to viewers via the Internet, bypassing cable, broadcast and satellite television platforms.

Personal data – the term used under European Union General Data Protection Regulation that has a much wider scope than "personally identifiable information" because it includes data attributes that may single out and identify individuals when combined with personal data. This means that Internet Protocol addresses, mobile ad identifiers, specific latitude/longitude elements, cookies and device IDs generally are classified as Personal Data under the legal remit of the General Data Protection Regulation.

Personally identifiable information – elements that directly identify a person, such as a name, address, phone number, email address and a limited range of other identifiers.

Programmatic advertising value chain – the integrated system of technology platforms and connectivity that enables advertising to be bought and sold in real time through advertising exchanges.

Second-party data – data that are shared by a brand with a partner (the second party) in a dedicated environment with a clearly defined set of permissions and rights sent between each of the parties, frequently with a third-party provider managing the environment.

Supply-side platforms – technology platforms that enable publishers to sell their advertising inventory in the programmatic advertising ecosystem.

Third-party cookie – cookies that are placed on an Internet user's web browser by a domain that is not the site that is being visited, usually placed on a website through a script or tag. When a user accesses a website with third-party cookies, information and data bits about the user's behaviour are saved and shared with the company owning the cookies. Third-party cookies normally are owned by advertisers or social media sites.

Third-party data – data collected by an entity that does not have a direct relationship with the end-user (data subject) whose data are being collected.

Vertical ad networks – businesses that aggregate online publisher inventories of a specific genre or type (travel, sports, finance, health and beauty) and sell aggregated contextual audiences to agencies and brands.

Walled gardens – large technology companies that provide a full-service publisher, advertising technology and data solution to advertisers (usually Google and Facebook, but also Snapchat and TikTok). In the digital world, a walled garden is a closed ecosystem in which all the operations are controlled by the ecosystem operator (de Poulpiquet, 2017). The main platforms with walled gardens are Facebook, Google, Amazon, Microsoft and Apple.

Waterfall bidding – a prevalent methodology for programmatic advertising transactions on exchanges which contrasts with Open Bidding, in which a publisher (seller) offers ad impressions to predetermined ad networks (buyers) for a fixed minimum price per impression (floor bid) in sequential order. That means if the publisher offers an ad impression for a minimum price of US$ 0.02, it will be sold to the first ad network to which it is offered that meets the floor bid (Zeropark, 2021).

References[1]

de Poulpiquet P (2017). What is a walled garden? And why it is the strategy of Google, Facebook and Amazon Ads platform? In: mediarithmics_what is? [website]. San Francisco (CA): Medium (https://medium.com/mediarithmics-what-is/what-is-a-walled-garden-and-why-it-is-the-strategy-of-google-facebook-and-amazon-ads-platform-296ddeb784b1).

Google Ad Manager (2021). How Open Bidding works. In: Google Ad Manager [website]. Mountain View (CA): Google (https://support.google.com/admanager/answer/7128958).

Morrisroe B (2020). What is header bidding and why should you care? In: Publift [website]. Sydney: Publift (https://www.publift.com/adteach/what-is-header-bidding-and-why-should-you-care).

Netacea (2021). What is device fingerprint? In: Netacea (website). Manchester; Netacea (https://www.netacea.com/glossary/device-fingerprint/).

Outbrain (2021). Native advertising. In: Outbrain [website]. Manchester: Outbrain (https://www.outbrain.com/native-advertising/).

Zeropark (2021). Waterfall vs. header bidding for web & in-app advertising. In: Zeropark [website]. Cracow: Zeropark (https://zeropark.com/blog/waterfall-vs-header-bidding-web-in-app-advertising/#Waterfall_bidding_explained).

---

1   All references accessed 8 March 2022.

Executive summary

Noncommunicable diseases (NCDs) such as cardiovascular disease, cancer, chronic respiratory disease and diabetes are responsible for 86% of deaths and 77% of the disease burden in the WHO European Region. Unhealthy diet is a major risk factor for NCDs. Exposure of children and adolescents to marketing for foods high in fats, sugars and/or salt (HFSS) increases the likelihood that they will agitate for, buy and consume these foods and encourages establishment of unhealthy dietary patterns. Any attempt to tackle childhood obesity should therefore include measures to reduce exposure of children to marketing of HFSS foods.
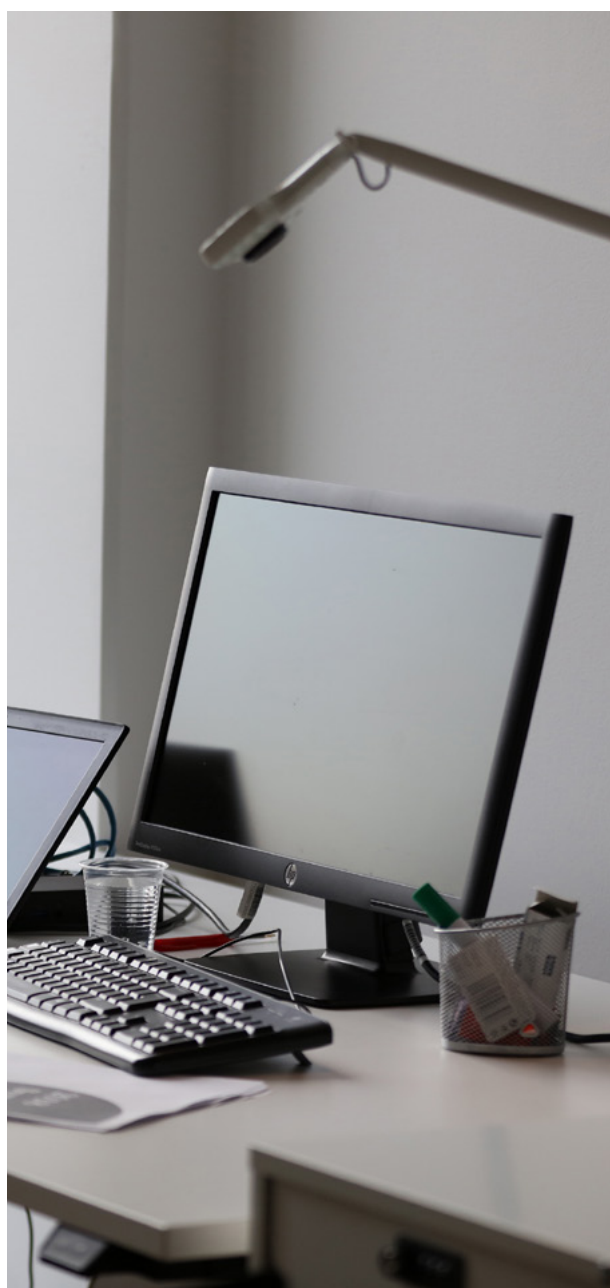
As digital media consumption grows, children increasingly are being exposed regularly to digital marketing of many unhealthy products. Time spent online is shifting increasingly to social media, mobile devices and gaming consoles, where personalized and targeted advertising predominates. Despite industry voluntary efforts to control marketing, exposure to the marketing of unhealthy foods remains a major issue throughout the European Region. This situation demands change that will protect all children equally from the harmful impacts of food marketing.

Digital advertising largely is bought and sold through a highly complex automated process known as programmatic advertising, involving real-time bidding. Without inside visibility of how the large so-called walled gardens operate, this process makes it almost impossible to predict or monitor exactly which adverts are served to whom. In 2018, WHO published a report to highlight the importance of the exposure of children and adolescents to digital media advertising of HFSS foodstuffs and to help countries understand the programmatic advertising system. The report also presented the CLICK framework (Comprehend the digital ecosystem; Landscape of campaigns; Investigative exposure; Capture on screen; and Knowledge sharing) for monitoring children's exposure to digital marketing.

The digital advertising ecosystem is evolving constantly, and there have been significant changes in how digital advertising is bought and sold since 2018. The pressures facing global digital advertising – further complicated by changes due to the COVID-19 pandemic – have impacted on the ecosystem in multiple ways. The future of digital media advertising is both **clear** (money will continue to follow eyeballs online, and new formats and technologies will continue to be invented) and **uncertain** (regulatory and commercial factors are changing the way the digital media ecosystem works). Going forward, brands, publishers and technology providers all face challenges and will be required to make significant changes.

The COVID-19 pandemic has increased governments' focus on health and the obesity crisis. Two areas of government policy – health (specifically tackling overweight and obesity) and regulation of major technology companies (so-called Big Tech) – are aligning, presenting a window of opportunity for coordinated policy action. Currently, technologies are being used for targeting HFSS advertisements at children or adolescents. In theory, the same technologies could also be used to prevent HFSS advertising from reaching underage audiences, as long as it was possible to verify accurately the digital identity and age of an Internet user.

The key aspects of the recent changes can be summarized as follows.

- Digital advertising spend has now further consolidated onto the major technology platforms, with Google, Facebook, Amazon, Microsoft and Apple accounting for between 60% and 80% of digital media spending in key markets globally.

- There continues to be a lack of accurate and verified identity and age data that would allow children to be identified in the ecosystem as being under 18 years of age.

- Due to changes in the browser and mobile operating systems and the deprecation of the third-party cookie (controlled by Apple and Google), personalized targeting across the open anonymous web will not continue at the same scale. Ultimately, there may be less advertising-funded content for children and adolescents outside of Facebook and Google, and it will be easier to control advertising content in more vertically focused children's apps and social and video channels.

There are several important implications of these recent and ongoing changes for policy-makers and regulators.

- To be effective, WHO and national policy-makers will need to directly address the main Big Tech platforms to influence changes to the rules for advertising HFSS foods to children.

- Given the spectrum of regulatory and political pressures that these businesses are facing across the globe, the timing is good for more coordinated and direct discussions on future policies with the platforms. Without active participation from Facebook and Google in the programmes, coordinated at regional and global levels, national programmes are likely to fail to have significant impact on digital advertising to minors.

- On the positive side, changing policies within the closed ecosystems (walled gardens) of companies such as Google and Facebook is theoretically and technically easier than changing behaviour across the whole open advertising ecosystem. The new environment simplifies the process of data collection for national-level market-mapping – the long-tail open publisher ecosystem has become less relevant and the remaining large national publishers are easier to identify at source. This also facilitates discussions among global national health research partners.

- There will, however, continue to be a conflict between the platforms' commercial objectives and momentum around restricting advertisers on the platforms. Blanket bans on HFSS advertising (such as in the United Kingdom) are likely to be resisted by global platforms and national publishers and may prove difficult to implement fully in practice.

- A focus on national publisher consortia (such as Ozone (United Kingdom), Gravity (France) and NetID (Germany)) and the main walled gardens (Google, Facebook, TikTok and Snap) is recommended, with increased attention on identifying and authenticating audiences (by age) by child-focused content vertical ad networks (such as SuperAwesome/Epic).

- A coordinated WHO voice and more active participation in national and European Union-wide regulatory debate will be important.

Understanding the constantly evolving digital marketing ecosystem remains essential for health policy-makers and regulators intent on reducing children's exposure to marketing of HFSS foods. The recent significant changes, which are ongoing, require a shift in approach for policy-makers. It will be more important than ever to initiate meaningful dialogue with the major technology platforms to explore possibilities for harnessing the power of technology to protect children from marketing of unhealthy products.

01.

Why digital advertising matters to WHO

Noncommunicable diseases (NCDs) such as cardiovascular disease, cancer, chronic respiratory disease and diabetes are the major causes of death worldwide, accounting for 86% of deaths and 77% of the disease burden in the WHO European Region. Many cases of NCDs could be prevented or delayed by tackling major risk factors beginning in childhood, including poor diet, and alcohol and tobacco use.

Exposure of children and adolescents to marketing for foods high in fats, sugars and/or salt (HFSS) increases the likelihood that they will agitate for, buy and consume those foods (Hastings et al., 2003; McDermott et al., 2006; Cairns et al., 2009; Boyland et al., 2016). Marketing influences food preferences and encourages establishment of unhealthy dietary patterns, leading to development of overweight, obesity and diet-related NCDs. Marketing of unhealthy products to children therefore is a significant concern for health professionals, governments and parents. Despite an increasing number of voluntary efforts to control marketing by the consumer goods and media industries, exposure to the marketing of unhealthy foods remains a major issue in all markets. This situation demands change that will protect all children equally from the harmful impact of food marketing. Any attempt to tackle childhood obesity should therefore include a reduction in exposure of children to marketing.

Marketing has become more powerful and pervasive since 2010, with digital media and data-targeting techniques boosting the amount of advertising images seen and increasing their impact. As digital media consumption grows (also boosted in 2020 by the COVID-19 pandemic), children are being exposed even more regularly to digital marketing of many unhealthy products; time spent online is shifting increasingly to social media, mobile devices and gaming consoles, where personalized and targeted advertising predominates.

Global digital media and advertising is now huge business, with the largest and most valuable companies in the world (Amazon, Apple, Facebook, Google and Microsoft) playing a significant role in how adults and children consume media content and determining the advertising and products to which they are exposed. Emerging platforms (such as TikTok, Snap and Roblox) and local and national publishers, platforms and broadcasters continue to play an important role as brands constantly seek new channels for marketing. While commercial, consumer and regulatory forces are shaping the future of the digital media ecosystem, given the elevated importance of the global health crisis, WHO has a key role to play in monitoring, measuring, educating and informing the policy debate on regulation and control of the digital media ecosystem going forward into the 2020s.
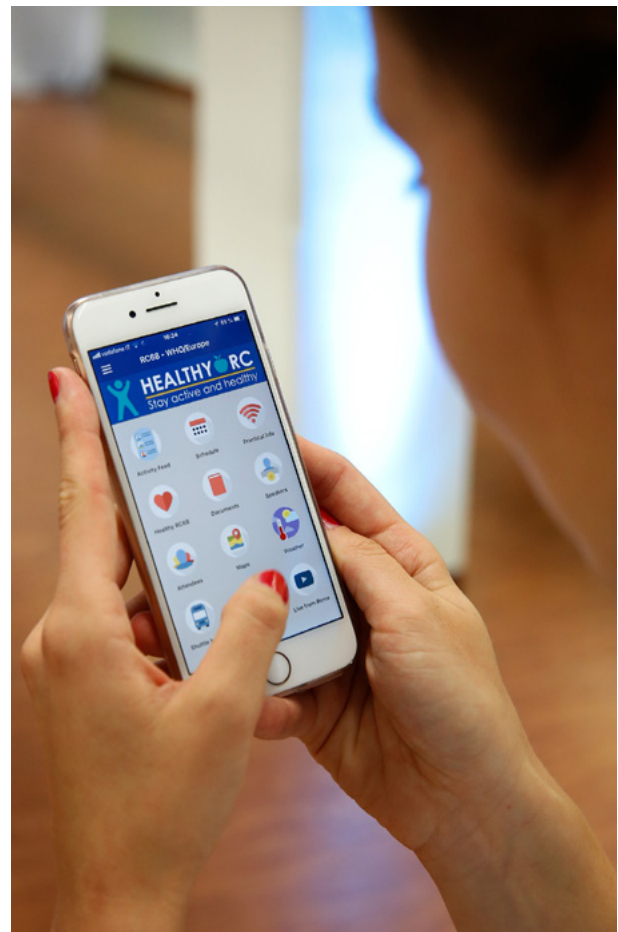
◆ There is unequivocal evidence that the marketing of unhealthy foods and sugar-sweetened beverages is related to childhood obesity. Marketing has become more powerful and pervasive over the last 10 years, with digital media and data-targeting techniques boosting the amount of advertising images seen and increasing their impact.

02.

Overview of the digital marketing ecosytem

The WHO European Office for the Prevention and Control of Noncommunicable Diseases published its report on the monitoring and restricting of digital marketing of unhealthy products to children and adolescents (the CLICK report – Comprehend the digital ecosystem; Landscape of campaigns; Investigative exposure; Capture on screen; and Knowledge sharing) in 2019 (WHO Regional Office for Europe, 2019). It highlights the importance of exposure of children and adolescents to digital media advertising of HFSS foodstuffs. An overview of how the digital media advertising industry was structured and behaved at that time was presented as part of the report, with a detailed explanation of the data- and technology-enabled programmatic advertising value chain. This overview is summarized briefly below.

The original digital marketing system

Early digital advertising was not targeted at individual users. Rather, as with broadcast and print advertising, agencies bought large-scale audiences, often chosen by the content (websites and webpages) they were consuming, and all consumers of that content would see the same advertisement at the same time. This original form of audience media-buying still predominates in some less developed advertising markets with less sophisticated publishers. The advent of data-driven advertising in the last 10–15 years brought the technical capability to send a different advertisement to each consumer and to target additionally by, for instance, context and time based on the individual characteristics (the data) of individual customers.

Programmatic advertising system

The last 10 years have seen a significant global shift towards automated buying and selling of targeted advertising, known as the programmatic system of advertising, as it has proven the most effective way of buying and selling media. The programmatic ecosystem is supported by numerous technology companies that connect publishers and brand/agency campaigns in real time. The system uses data about individuals to target appropriate advertisements and has the potential to be much more efficient from an advertiser's perspective. The profits in programmatic advertising rely on successfully matching advertisements to individuals' data, so accurate personal information has become more valuable in the digital advertising ecosystem (Fig. 1a, Fig. 1b).

The supply side: how an advertisement reaches people

When people click through to a publisher's website, as the page loads a request is sent from the website to one of the publisher's chosen supply-side platforms (SSPs), which manage selling of the publisher's advertising space (Fig. 1a). This request is known as an ad request and carries a cookie or an advertising identifier that often links to data held on the person or device. The SSP then submits the ad request to an ad exchange, and the process of selling the ad impression begins.

Fig. 1a. Programmatic ecosystem: supply side

USER → WEBSITE/APP → SSP → AD EXCHANGE
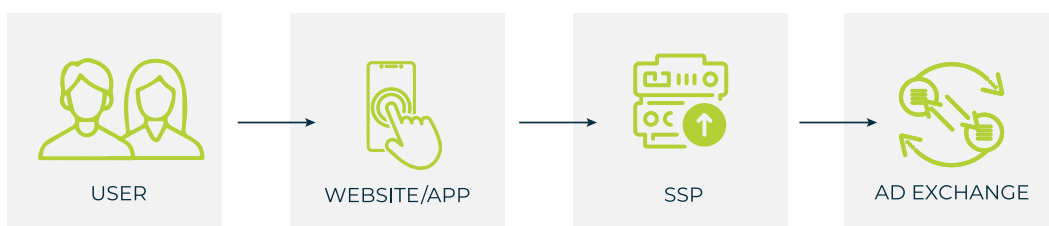
Source: WHO Regional Office for Europe (2019).

The demand side: where an advertisement comes from

Brands use media agencies to design their creative content, buy the media and operationally run their advertising campaigns. Trading desks at these agencies ensure that ad impressions are bought from different ad exchanges and publishers as cheaply and efficiently as possible, using technical tools called demand-side platforms (DSPs) to buy, serve and track advertisements (Fig. 1b). The DSP allows an ad campaign to be tagged with information to ensure that it is sent only to users with the data attributes that predict they are likely to be interested in buying the product. Once the advertisement has been tagged and the ad impression bought from the publisher, the decision is made about which campaign to send to that device/ad impression by comparing the campaign with the data known about that device or user. These data on the device/individual to be targeted are stored within a data-management platform (DMP). Once the ad impression has been bought and the data crunched to work out the best advertisement to send – that is, to the device whose profile best matches the tags on the ad – an ad server sends the advert to the device. Given its complexity and a lack of transparency in the systems, it is not always possible to track this exact process of delivering the brand's advertisement to the publisher's webpage and measurement remains a key feature of the industry.

Fig. 1b. Programmatic ecosystem: demand side
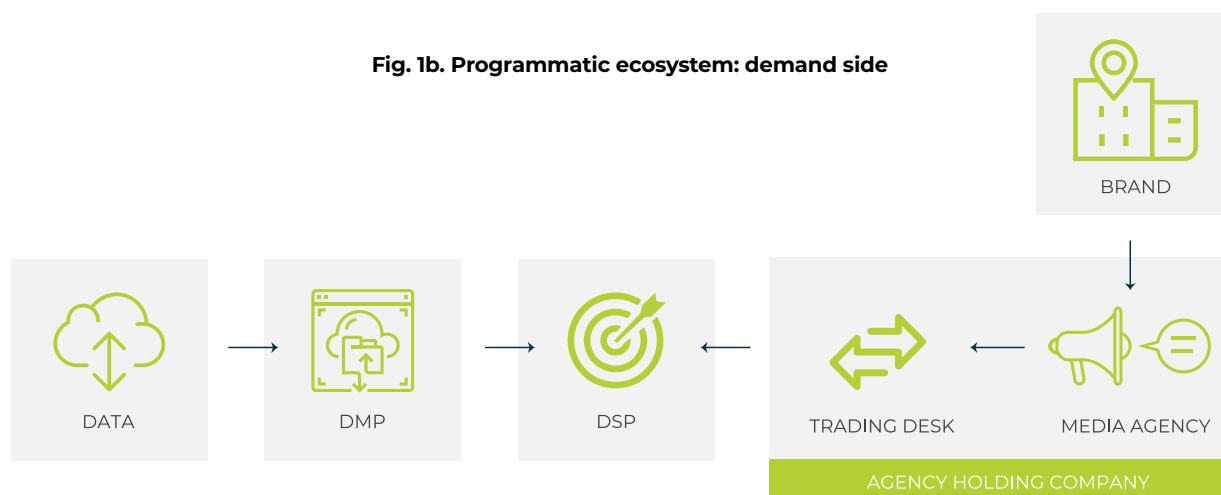
Source: WHO Regional Office for Europe (2019).

The bidding process

The process described above is further complicated by a bidding process in which the advertisement the user sees on their device is selected. There are multiple intermediaries at many steps of this process, and it is almost impossible to monitor or predict exactly where an advert will actually be shown. Although theoretically possible, the data process tends to be fragmented and neither the brand, the media agency nor the publisher can say with certainty which advertisements have been served to which device. The whole complex process – requesting content, choice of content and identifying to whom it will go and at what price – takes less than 250 milliseconds to complete and is known as real-time bidding.

◆ Digital advertising is bought and sold through a highly complex automated process known as programmatic advertising involving real-time bidding. This process makes it almost impossible to predict or monitor exactly which adverts are served to whom. The CLICK report (WHO Regional Office for Europe, 2019) highlights the importance of exposure of children and adolescents to digital media advertising of HFSS foodstuffs to help countries understand the programmatic advertising system.

03.

Why understanding the digital ecosystem matters to countries

The CLICK report also explains how brands and agencies use these technologies to target specific advertising campaigns to specific audiences for maximum effect, and recommends the CLICK monitoring framework to help countries address the challenge of digital marketing of unhealthy products to children (Fig. 2).

Fig. 2. The CLICK tool for monitoring children's exposure to marketing of unhealthy products online

C	Comprehend the digital ecosystem	Map the global, regional and national digital marketing ecosystem and children's website/app usage; alongside this work, set up focus groups to gauge children's and parents/guardians' experience and awareness of marketing techniques and campaigns
L	Landscape of campaigns	Assess campaigns run by leading national brands by collecting information from advertising agencies and by sampling whole-country social media for relevant content to ascertain what is viewed by different age groups
I	Investigate exposure	Map exposure to some paid-for digital marketing experienced by a panel of children in each age bracket using an installed smartphone app that (with consent) monitors and aggregates data on children's interaction with advertisements in some websites and social media
C	Capture on-screen	Use real-time screen capture software on a panel subgroup to assess what a representative sample of children actually sees online on their devices, in order to better understand wider marketing techniques, including user-generated content and product placement
K	Knowledge sharing	Create user-friendly materials from the research data and develop partnerships with young people, parents, policy-makers and civil society, who together can advocate change, raise awareness and influence policy

Source: WHO Regional Office for Europe (2019).

Some key terms

Advanced targeting technologies – refers to new technologies and approaches that enable contextual targeting instead of personalized ad targeting.

Data-management platforms (DMPs) – a software platform used for collecting, organizing and distributing data, allowing businesses to identify audience segments for targeting of advertising.

Demand-side platforms (DSPs) – technology platforms used by brands and agencies to buy targeted programmatic media.

Mobile ad IDs (MAIDS) – the mobile ad ID (either the Apple iOS ID for advertising or the Android advertising ID) identifies phones and devices for advertising and is given by the device's operation system. The ID contains randomly selected numbers and letters and is used by advertisers to identify a device. The mobile ID can be used by free phone applications to understand the user and their choices and behaviour.

Programmatic advertising value chain – the integrated system of technology platforms and connectivity that enables advertising to be bought and sold in real time through advertising exchanges.

Supply-side platforms (SSPs) – technology platforms that enable publishers to sell their advertising inventory in the programmatic advertising ecosystem.

Walled gardens – large technology companies that provide a full-service publisher, advertising technology and data solution to advertisers (usually Google and Facebook, but also Snapchat and TikTok). In the digital world, a walled garden is a closed ecosystem in which all the operations are controlled by the ecosystem operator (de Poulpiquet, 2017). The main platforms with walled gardens are Facebook, Google, Amazon, Microsoft and Apple.

The first step in the CLICK framework is the C for Comprehend the Digital Ecosystem. The recommendation was that Member States need to complete a national mapping of the digital media ecosystem to identify the scale of reach and usage of the major platforms (Google/YouTube, Facebook/

Instagram/WhatsApp, Twitter, Snapchat and TikTok) in child and adolescent age brackets. The mapping exercise should also identify the local ecosystem players that complete the picture, including major agencies, brands and publishers and the technology partners they use to target and serve their digital media advertising (including DSPs, SSPs and DMPs). Although many of the main platforms are global, their use and adoption vary across markets. With a more accurate picture of the landscape of the national digital media ecosystem, local health agencies can begin to identify with which major players in their ecosystem they should engage and assess how new guidelines could be implemented. Given the fast pace of development of the digital media ecosystem in all markets, there is a great deal of complexity that is not well understood or researched at local level outside of the main global digital media markets (such as China, the United Kingdom and the United States of America), so some primary research is often required.

The recommendations of the CLICK report were based on the idea that better understanding of the local ecosystem would be the first step in determining how to influence changes to the local advertising ecosystem to help prevent the advertising of HFSS foodstuffs and non-alcoholic beverages to children and adolescents under 18. Currently, the technologies are being used for targeting adverts that deliver the highest commercial returns to brands, which often includes the specific targeting of HFSS advertisements at vulnerable children or adolescents. In theory, the same technologies can also be used for good or negative targeting (under certain conditions and industry guidelines) to prevent HFSS advertising from reaching underage audiences.
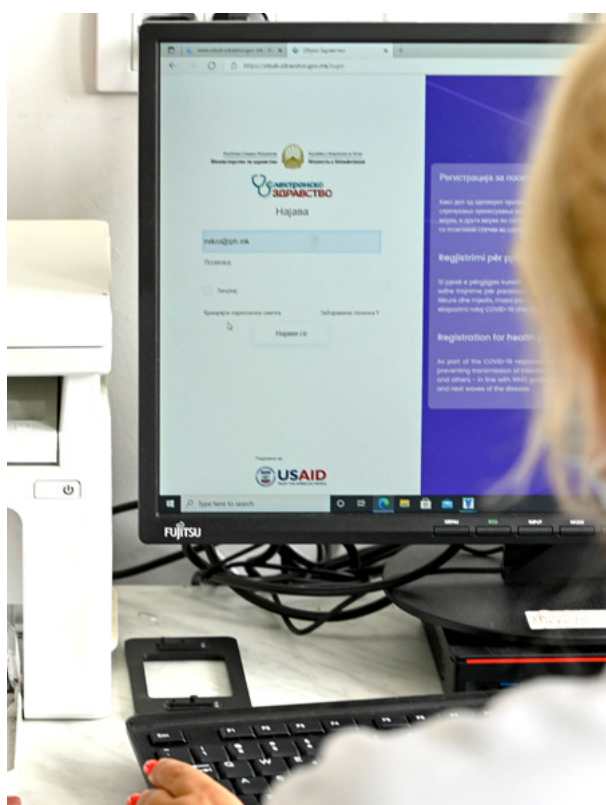
This ray of light comes with three caveats:

- the industry lacks a consistent and accurate digital identity or age dataset that verifies accurately the age of the child;

- many children consume content in adult settings or by using false declared logins that hide their true age; and

- a high proportion of advertising content is consumed on the major walled-garden portals (Facebook, Google/YouTube, Snapchat and TikTok) where deeper engagement with the platforms on their advertising targeting policies needs to be coordinated at regional or global level.

As countries grapple with the complexity of their advertising ecosystems and the lack of available local data and research, the global digital advertising ecosystem continues to evolve at a very rapid pace. Specifically, since 2018, the changes predicted in the industry in response to consumer privacy concerns and regulation have become more real, and significant changes in how digital advertising is bought and sold and the underpinning technologies are occurring. These changes have been accelerated by moves by Google and Apple to change the structure and performance of the underlying identifier technologies (third-party cookies and mobile ad identifiers (MAIDs)) that underpin digital media advertising in response to consumer, commercial and regulatory pressure.

The future of digital media advertising is both clear (money will continue to follow eyeballs on mobile devices, and new formats and technologies will continue to be invented) and uncertain (regulatory and commercial factors are changing the way the digital media ecosystem works). Usage will continue to grow, and money will continue to flow. Exactly how the digital advertising ecosystem can best be monitored, controlled and directed in the future is still to be determined.

The remaining chapters of this report outline the changes in the digital ecosystem since 2018 and explore their implications for health policy-makers who are seeking to restrict children's exposure to marketing of unhealthy products.

◆ WHO recommended the CLICK monitoring framework to help countries monitor children's exposure in 2019. Through better understanding of the local ecosystem, it may be possible to adapt the advanced targeting technologies in place to prevent HFSS advertising from reaching underage audiences. The global digital advertising ecosystem continues to evolve at a very rapid pace and very significant changes in how digital advertising is bought and sold have occurred and continue to change since then.

04.

United Kingdom basis for the underlying analysis

Much of the data in this report emerge from published data on the United Kingdom market, which is the largest and best researched digital media market in the European Region. Specifically, the United Kingdom's Competition and Markets Authority (CMA) issued a comprehensive report on the structure and conduct of the United Kingdom digital media advertising ecosystem in July 2020 (Competition and Markets Authority, 2020). As the major technology companies operate primarily global platforms, most of the same observations and effects will apply to countries in the Region at varying levels of digital media penetration and ecosystem maturity. The unbridled success of the major advertising platforms and the development of technology solutions for publishers are global phenomena, based on the power of data and the advantages of operating technology platforms at large scale.

Digital media regulation in the United Kingdom

There are good reasons to choose the United Kingdom as the example reference market for the assessment of understanding of what could be done to control the distribution of HFSS advertising to children/adolescents. The market is one of the most developed digital media markets in the world. Along with European Union (EU) markets, it has been at the forefront of data-privacy regulation through the early impact of the EU General Data Protection Regulation (GDPR). Following the United Kingdom's departure from the EU, the country has had to think through its approach and role in the regulatory debate as an independent sovereign state. As a result, much work and research has been done recently on the structure of the online market and likely needs for regulatory interventions.

The United Kingdom construct also provides an example of how online harm regulation is fragmented and multi-faceted, involving six of the main government and regulatory bodies in one market. This complexity is matched in other regional markets, resulting in great complexity of policies and regulatory approaches being developed and taken at national, regional and global levels. This fragmentation creates a huge amount of complexity – and perhaps confusion – in the major technology platforms about what changes to advertising policies and processes they actually are being asked to prioritize. Fragmentation of voice is one of the key

barriers to working effectively with the major technology platforms to reduce the exposure of unhealthy food marketing to children.

Since 2019, significant research has been published by the six main Government agencies that are shaping the agenda for big technology in the United Kingdom: the Information Commissioner's Office (ICO), Ofcom, the Advertising Standards Authority (ASA), the CMA, the Financial Conduct Authority (FCA) and the Government's Department for Digital, Culture, Media and Sport (DCMS) (Fig. 3).

The DCMS, which gives devolved responsibility to the ICO, Ofcom, the ASA and the CMA, led on the new Digital Services Tax that was introduced in April 2020 (Her Majesty's Revenue and Customs, 2020). This measure applied a new 2% tax on the revenues of search engines, social media services and online marketplaces (including adjacent online advertising businesses) above an annual limit of GB£ 25 million revenue. Revenues are usually derived from users in the United Kingdom if the revenue arises by virtue of a user using the service. Where one of the parties to a transaction on an online marketplace is a user in the United Kingdom, all of the revenues from that particular transaction will be treated as derived from United Kingdom users. When the transaction involves accommodation, land or buildings in the United Kingdom, revenue from that transaction will be treated as derived from United Kingdom users. Advertising revenues are derived from United Kingdom users when the advertisement is viewed or otherwise consumed by a United Kingdom user.

In November 2020, the DCMS and the Department of Health and Social Care launched a consultation on proposals to ban online adverts for HFSS foods in the country as part of a raft of measures to tackle obesity. The total ban on online HFSS advertising was proposed to future-proof how obesity is tackled and to help address the lack of transparency, noting the paucity of independent public data to reliably monitor the extent to which children are exposed to HFSS adverts online (United Kingdom Government, 2020). In June 2021, the United Kingdom Government launched its Tackling Obesity Strategy, which includes the requirement for a full ban on advertising for HFSS foodstuff on TV and online, following concerns about the effectiveness of implementing a 21:00 online advertising watershed. Ofcom will have a statutory role in overseeing the

Fig. 3. Arrangements for digital media regulation in the United Kingdom

Digital Regulators Forum					
Department for Digital, Culture, Media and Sport (DCMS)	**Ofcom (Telecoms regulator)**	**Competition and Markets Authority (CMA)**	**Information Commisioners Office (ICO)**	**Financial Conduct Authority (FCA)**	**Advertising Standards Authority (ASA)**
Goverment ministry with oversight of the media industry Gives devolved regulatory responsibility to Ofcom, ICO and ASA Decides what policies should be put into law	Telecom and broadcast regulator Appointed as Online Harms regulator Wide agenda for protection of consumers online Delegates authority for advertising to ASA	Major competition and antitrust regulator Responsible for antitrust rulings against major tech companies Reports on market structure and anticompetitive conduct	Enforces compliance with the United Kingdom version of the GDPR Development of Age Appropriate Design Code to protect children and adolescents	Regulator for financial services Involvement highlights interdependencies on use of data and algorithms	Regulator for advertising Applies advertising codes written by committees of advertising practice Oversees implementation of Government ban of HFSS advertising under Ofcom delegated authority

regulation of the restriction, and the ASA will have day-to-day responsibility for applying the new rules, which currently are planned to be implemented in 2023 (Department for Digital, Culture, Media and Sport and Department of Health and Social Care, 2021a).

The CMA, as the major competition and antitrust regulator in the United Kingdom, completed a comprehensive report on the market structure and the potentially anticompetitive practices of major tech companies in July 2020. As a result of the report's recommendations, a specialist Digital Markets Unit was established in April 2021 to further progress the competition agenda in the digital media and advertising industry.

Ofcom was appointed as Online Harms Regulator in December 2020. The scope of this role is still to be defined but will encompass a wide agenda, touching the major technical platforms on the Internet, including the protection of children online, and will involve close coordination with the ICO, CMA and DCMS.

A recent ICO survey into people's biggest data-protection concerns ranked child privacy second only to cyber security. Data-protection law at European level is rooted in the United Nations Convention on the Rights of the Child, which recognizes the special safeguards children need in all aspects of their life and provides its own additional safeguards for children.

As the United Kingdom regulator responsible for enforcing compliance with the GDPR regulation, the ICO published its guidance on data privacy for children and adolescents, *Age appropriate design: a code of practice for online services* (ICO, 2020). The Code came into force in September 2020, with a 12-month transition period requiring compliance by 2 September 2021. It is the first of its kind but reflects the global direction of travel, with similar reform being considered in the United States, Europe and globally by the Organisation for Economic Co-operation and Development (OECD).

The Code is not a new law, but it sets standards and explains how the GDPR applies in the context of children using digital services. It presents a set of 15 flexible standards that do not ban or specifically prescribe, but which provide built-in protection to allow children to explore, learn and play online by ensuring that the best interests of the child are the primary consideration when designing and developing online services (Box 1).

Organizations should conform to the Code and demonstrate that their services use children's data fairly and in compliance with data-protection law. If organizations do not conform to the standards in this Code, they are likely to find it more difficult to show that their processing is fair and complies with the GDPR and the Privacy and Electronic Communications Regulation (PECR). The ICO can take action against organizations that process a child's personal data in breach of the GDPR or PECR. Tools at ICO's disposal include assessment notices, warnings, reprimands, enforcement notices and penalty notices (administrative fines). For serious breaches of data-protection principles, the ICO has the power to issue fines of up to €20 million (GB£ 17.5 million) when

Box 1. The 15 principles of *Age appropriate design: a code of practice for online services*

Best interests of the child: the best interests of the child should be a primary consideration when you design and develop online services likely to be accessed by a child.

Data protection impact assessments (DPIA): undertake a DPIA to assess and mitigate risks to the rights and freedoms of children who are likely to access your service, which arise from your data processing. Take into account differing ages, capacities and development needs and ensure that your DPIA builds in compliance with this Code.

Age-appropriate application: take a risk-based approach to recognizing the age of individual users and ensure you effectively apply the standards in this Code to child users. Either establish age with a level of certainty that is appropriate to the risks to the rights and freedoms of children that arise from your data processing, or apply the standards in this Code to all your users instead.

Transparency: the privacy information you provide to users, and other published terms, policies and community standards, must be concise, prominent and in clear language suited to the age of the child. Provide additional specific bite-sized explanations about how you use personal data at the point that use is activated.

Detrimental use of data: do not use children's personal data in ways that have been shown to be detrimental to their well-being, or that go against industry codes of practice, other regulatory provisions or government advice.

Policies and community standards: uphold your own published terms, policies and community standards (including but not limited to privacy policies, age restriction, behaviour rules and content policies).

Default settings: settings must be "high privacy" by default (unless you can demonstrate a compelling reason for a different default setting, taking account of the best interests of the child).

Data minimization: collect and retain only the minimum amount of personal data you need to provide the elements of your service in which a child is actively and knowingly engaged. Give children separate choices over which elements they wish to activate.

Data sharing: do not disclose children's data unless you can demonstrate a compelling reason to do so, taking account of the best interests of the child.

Geolocation: switch geolocation options off by default (unless you can demonstrate a compelling reason for geolocation to be switched on by default, taking account of the best interests of the child). Provide an obvious sign for children when location tracking is active. Options which make a child's location visible to others must default back to "off" at the end of each session.

Parental controls: if you provide parental controls, give the child age-appropriate information about this. If your online service allows a parent or carer to monitor their child's online activity or track their location, provide an obvious sign to the child when they are being monitored.

Profiling: switch options which use profiling "off" by default (unless you can demonstrate a compelling reason for profiling to be on by default, taking account of the best interests of the child). Only allow profiling if you have appropriate measures in place to protect the child from any harmful effects (in particular, being fed content that is detrimental to their health or well-being).

Nudge techniques: do not use nudge techniques to lead or encourage children to provide unnecessary personal data or weaken or turn off their privacy protections.

Connected toys and devices: if you provide a connected toy or device ensure you include effective tools to enable conformance to this Code.

Online tools: provide prominent and accessible tools to help children exercise their data protection rights and report concerns.

Source: ICO (2020). Reproduced by permission of the Information Commissioner's Office, *Age appropriate design: a code of practice for online services*, 2020, licensed under the Open Government Licence v3.0.

the GDPR comes into effect or 4% of a company's annual worldwide turnover, whichever is higher, for infringements of the Code and standard GDPR infringements.

International coordination on policy following the United Kingdom's departure from the EU (Brexit)

The United Kingdom is now pursuing a full and holistic programme of regulation and policy on the operations of global technology companies. Bodies will continue to coordinate and align with their counterparts in Europe and work closely with regulatory bodies in key overseas markets such as Australia, Canada and the United States. Similar coordination continues within the EU for EU Member States.

Studies from other markets

Many similar studies have been, or are in the process of being, conducted in other markets. The global trends, issues and decisions of the global technology platforms will be the same in all markets, but how the local ecosystem adapts and how low regulation is formed to shape the right outcomes warrants specific and detailed studies. One of the challenges is that the ecosystem continues to move extremely quickly, so it is important for WHO to continue to share information, research and ideas.

◆ The United Kingdom market is presented as a case study because it is one of the most developed digital media markets in the world and, along with EU markets, has been at the forefront of data-privacy regulation. A new code of practice on age-appropriate design for online services that came into effect in September 2020 sets standards relating to data privacy for children and adolescents. The policy debate on online harms, however, remains fragmented across many bodies, which makes regulation and engagement with the major tech platforms more difficult. It is also difficult for WHO to engage with such a fragmented stakeholder landscape across the European Region.

05.

Three decades of digital advertising

Before looking forward and discussing the implications on the structure of the digital media ecosystem in the future on WHO and national health agendas, it is worth taking a step back and putting the last three decades of history of the digital media advertising industry into context. Digital/mobile advertising has now become big business, currently representing more than 60% of global advertising spend and growing faster than all spending on advertising on analogue media (Fig. 4). This extraordinary growth has been fuelled by scale of audience reach, technology investment and the power of data to drive better performance through personally targeted advertising. The mobile Internet initially was wired for performance, not for the protection of consumers' data, privacy or experience.

Fig. 4. Past, present and future of digital advertising: actual or projected global digital advertising spend (amount in US$ and percentage of total global advertising spend) and global total mobile advertising spend

"Content is king"	"Data is the new oil"	Big Tech dominates	Authenticated and anonymous web
2000–2010	**2010–2020**	**2020+**	**2025+**
2010 global digital ad spend < US$ 70 billion 15% total; mobile < US$ 1 billion	2018 global digital ad spend > US$ 250 billion 45% total; mobile US$ 100 billion	2018 global digital ad spend > US$ 600 billion 60% total; mobile US$ 360 billion	2030 global digital ad spend > US$ 1 trillion 80% total; mobile > US$ 7550 billion

Some key terms

Ad tech wiring/rails – the technology systems that allow the advertising ecosystem to operate.

Authenticated web – any Internet site where a user's identity is verified by logging in to a publisher, producing an authentication token.

Display advertising – online advertising using banner ads and other visual ad formats.

Vertical ad networks – businesses that aggregate online publisher inventories of a specific genre or type (travel, sports, finance, health and beauty) and sell aggregated contextual audiences to agencies and brands.

Walled gardens – large technology companies that provide a full-service publisher, advertising technology and data solution to advertisers (usually Google and Facebook, but also Snapchat and TikTok). In the digital world, a walled garden is a closed ecosystem in which all the operations are controlled by the ecosystem operator (de Poulpiquet, 2017). The main platforms with walled gardens are Facebook, Google, Amazon, Microsoft and Apple.

2000–2010: "Content is king"

Over this decade, global digital ad spend grew from US$ 9.7 billion in 2000, representing 2.8% of total global advertising spend, to US$ 62 billion in 2010, equivalent to 15.3% of the total global advertising spend. Over the same period, global mobile advertising spend increased from virtually nothing (GroupM, 2017) to US$ 1 billion (Informa, 2010).

Digital advertising had been established on the desktop Internet in the previous decade – AOL had launched in 1993, followed by Yahoo! in 1995 and Google in 1998. By 2000, the consumer Internet was alive and well with over 360 million global users (Solarwinds, 2010), 70% of whom were concentrated in the top-10 countries (the United States, Japan, Germany, China, the Republic of Korea, the United Kingdom, Italy, Canada, France and Australia). The number of global Internet users grew to 2 billion by 2010, with 60% in top-10 countries and with highest growth observed in China, India, Brazil, the Russian Federation and Nigeria. In this decade, content consumption and publisher breadth exploded with increased Internet adoption and broadband speeds and the launch of smartphones (the Apple iPhone launched in June 2007). People using Internet search engines became the most valuable format for advertisers, giving rise to the expression "Content is king (but Search is God)". Online advertising networks bundled online display advertising inventory to enable them to compete through scale with traditional offline advertising media. The price paid for online advertising was driven by consumer engagement in the highest-value media content.

2010–2020: "Data is the new oil"

The global digital ad spend rose to over US$ 250 billion by 2018, accounting for 45% of total global advertising spend. Mobile advertising spending rose to US$ 100 billion.

Data about users became highly valuable for targeting digital advertising (particularly display and video advertising) and measuring its effectiveness. Advertisements targeted to specific individuals perform better and give better return on advertising spend investment to brands than untargeted advertising. The Big Tech companies with walled gardens achieving big audience reach and sophisticated data collection benefited hugely, while independent publishers had to take action to survive. Venture capital investment flooded into programmatic advertising technology to help publishers to wire themselves together with global programmatic ad tech wiring/rails to drive performance. Given its power, independent open-ecosystem solutions often were less attractive than partnering with technology or data from, or acquired by, the same Big Tech companies (Google and Facebook). The role of online publishers became diminished (by the global platforms and advertising technology ecosystem) as the rise of social media and user-generated content drew bigger screentime audiences. In this golden period for digital media, the value of digital advertising was driven by walled-garden content consumption plus data and real-time programmatic ad technology, which unlocked value in a virtuous circle. The expression "Data is the new oil" became prominent.

2020 onwards: Big Tech dominates

By 2025, global digital ad spend is predicted to be over US$ 600 billion, representing 60% of total global ad spend, and mobile advertising spend will reach US$ 360 billion.

Since 2018 (when the EU GDPR regulation came into effect and in the aftermath of the Facebook Cambridge Analytica scandal (Confessore, 2018)), however, a backlash has been underway against the concentration of revenues and power in Big Tech walled gardens and widespread and unregulated use of consumer data to drive revenues, often without consumers' explicit opt-in consent. This has triggered the Big Tech companies owning browsers and operating systems (mainly Google and Apple) to adopt privacy-first positions and effectively accept that the behaviours of the current open-web wiring advertising ecosystem are inconsistent with consumer data privacy regulation.
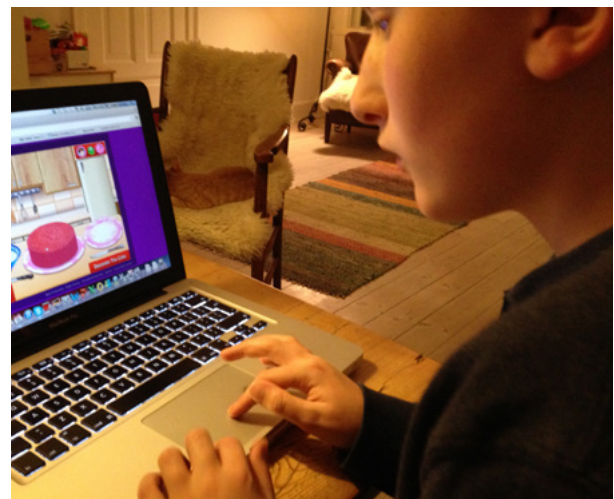
The major platforms are in the process of developing strategies to turn the current challenges to commercial advantage, albeit with some significant disruption. As consumer opt-in consent requirements were more complicated for open-ecosystem publishers and their multiple technology partners, the major walled gardens were unintended beneficiaries of GDPR and California Consumer Privacy Act (CCPA) privacy regulation. Apple and Google implemented restrictions in third-party cookies and MAIDs in response to consumer/competitive concerns about data privacy, with the second-order effect of disabling the measurement and attribution processes that enable the digital advertising industry.

Again, however, the Big Tech companies emerge as winners, as it is easier for them to build new solutions within their walled gardens by not serving the complexity of the open publisher ecosystem. Advertising money will continue to flow into digital formats with high levels of engagement and/or performance, such as social, video and search formats (often owned by the same Big Tech companies). The multitude of smaller publishers are left without underpinning targeting technology and are unable to meet the demand for targeted online advertising.

In response, some publishers have formed national publisher consortia (such as Ozone in the United Kingdom and Gravity in France) to combine their inventory into a larger universe where consumers (who are logged in and/or are subscribers) can be targeted and (for users who are not logged in) act jointly as vertical ad networks using contextual targeting.

Brands, agencies, regulators and consumers are reacting against the scale, power and behaviour of Big Tech – there is a search for new solutions and fairer taxation and even future threats of antitrust breakup measures. Facebook is facing significant revenue pressure from the changes to consumer data opt-ins required by Apple under the

iOS14 update (Yeshanew, 2021). The interplay between regulatory and technology changes in the advertising ecosystem will continue to have a profound effect on where the advertising money flows, the economic future of independent publishers and future success of the major walled gardens.

◆ Digital media advertising has changed dramatically over time and is predicted to account for 60% of global advertising expenditure by 2025. The focus shifted from engagement in content to the importance of activating users' data, leading to a progressive concentration of revenues among Big Tech companies. The changes implemented in response to the backlash against widespread and unregulated use of consumer data to drive revenues without consent also, ironically, have benefited Big Tech companies in the short term. The interplay between privacy, regulation and underlying advertising technology will determine how digital media advertising spend will be split between the major walled-garden platforms and independent publishers in the future.

06.

Digital advertising ecosystem shifts 2018–2020

Looking forward, some very recent fundamental shifts to the global digital advertising ecosystem warrant more detailed exploration. Since 2018, several pressures on the digital advertising ecosystem that have had a number of impacts have been identified (Fig. 5).

Fig. 5. Shifts in the digital advertising ecosystem between 2018 and 2020
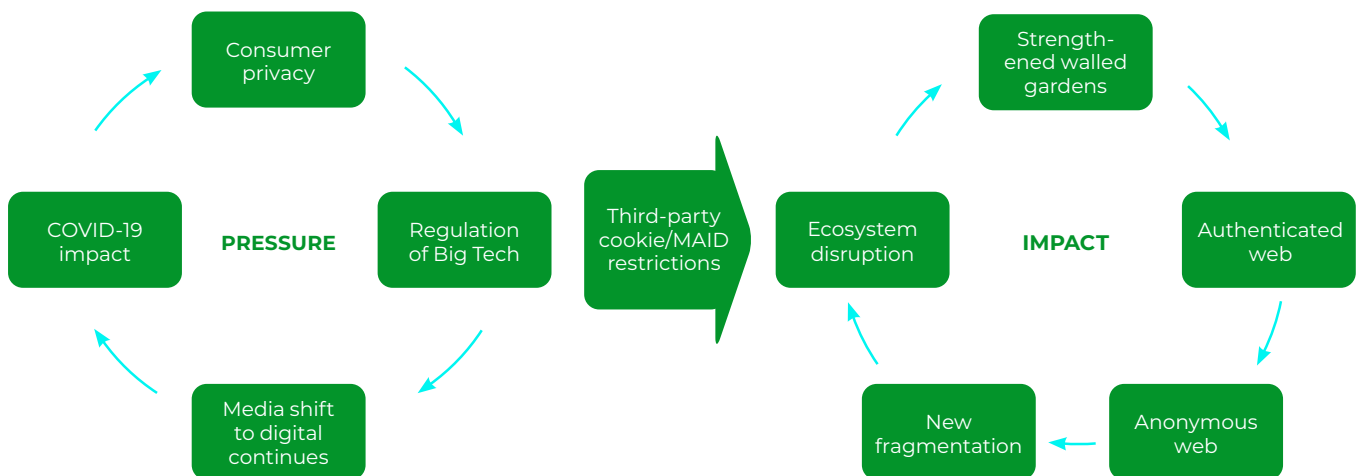

Fig. 5 represents **the period between 2018 and 2020**, and it is important to note that the story of how the advertising ecosystem will develop is still unfolding. Understanding of these key developments and trends will help reveal the implications for WHO and Member States as they consider the future of advertising of HFSS to children and adolescents in their markets.

Pressures on the digital marketing ecosystem between 2018 and 2020

As introduced above, by 2018 pressures on the established structure, technology and data practices of the digital advertising ecosystem were mounting.

Pressure 1: long-term shift to digital continues

Internet reach has grown to 4.7 billion people worldwide (59% of the global population) and the number of active social media users has reached 4.1 billion (Statista, 2021). Over 41% of the global population (3.3 billion) has access to a smartphone (85.9% Android and 11.8% Apple (O'Dea, 2021)) and average daily screentime is increasing for all age groups. Digital advertising continues to grow faster than the overall advertising market and there is continued innovation in digital programmatic technologies for marketing through video, in-game, audio/podcast and digital out-of-home (OOH) platforms. In the future, the metaverse will offer consumers full immersive technology experiences in virtual worlds, where advertising will also play a key role in experience monetization. Earlier industry projections for global digital advertising spend of US$ 325 billion by 2019 (Enberg, 2019) actually were surpassed by 16.6% to US$ 379 billion, but (due to the COVID-19 pandemic causing a retraction in global advertising spend) fell back to only 2.4% **above** previous projections for 2020 (Fig. 6). Global digital advertis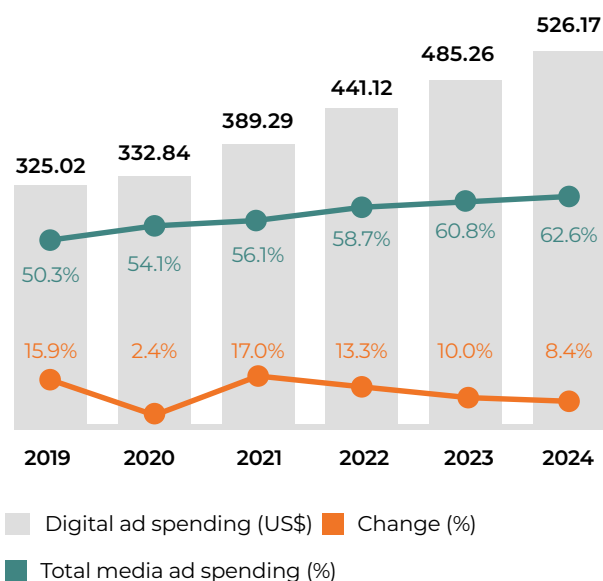ing continued to grow even through the pandemic. Current projections show that industry growth is expected to realign to previous forecasts for 2021 and beyond (Fig. 6).

Pressure 2: COVID-19 slows down advertising growth but accelerates shift to digital

The COVID-19 pandemic caused a considerable drop in advertising spend overall in most markets and across categories in 2020. The hardest-hit categories were marketing for travel and tourism, retail (not online), restaurants and automotive. In many countries, governments have emerged as major advertising buyers to promote public health messages or support journalism. Expenditure started to recover quickly in the fourth quarter of 2020.

The pandemic has accelerated the shift to digital marketing. Wherever consumer behaviour has shifted, advertising spend has adjusted in response, resulting in massive reductions in cinema, OOH advertising and print advertising, and spend from the travel and hospitality sectors. Meanwhile, in-home digital media usage went up significantly. Although broadcast TV viewership climbed, digital video consumption increased even more: use of social platforms and streaming services has risen almost everywhere and gaming has also grown dramatically. Digital news publishers have been particularly impacted as advertisers have sought to distance their products from coronavirus-related content, as have smaller publishers, who have struggled in a more turbulent market. In addition, there has been a decrease in the value of pay TV to the benefit of ad-supported streaming video services.

In the United States, for example, advertising spend reduced by US$ 39 billion (–10.3%) to US$ 340 billion in 2020 during the COVID-19 pandemic, but digital media spending grew by US$ 12.5 billion (+8.0%). The highest growth rates were in digital video (+27.1%), influencer social marketing (+15%), paid social media (+14.5%), display advertising (+6.8%) and search (+5.9%). OOH shrank by 19.3% and digital audio (radio/podcasts) decreased by 13.4% (World Federation of Advertisers, 2020) (Fig. 7). As people spent more time at home and screentime increased, the major platforms (Google, Facebook, Pinterest, Snap, Twitter and Amazon) reported record revenues for the fourth quarter of 2020.

As confinement measures were relaxed and OOH advertising began to grow back, these typically offline channels will accelerate their shift to digital. This will increase pressure on the advertising industry to improve how it measures return on investment across different media, devices and platforms.

In the United States, the value of third-party data (collected by an entity that does not have a direct relationship with the end users whose data are being collected) purchased by marketers grew 6.1% in 2019 to US$ 119 million, slowing from the 15.7% growth seen in 2018. Largely this slowdown was driven by changes predicated by CCPA/GDPR privacy regulation, but COVID-19 accentuated this, with cuts of up to 20%

Fig. 6. Digital ad spending worldwide, 2019–2014
(in US$ billions, percentage change and percentage of total media ad spending)

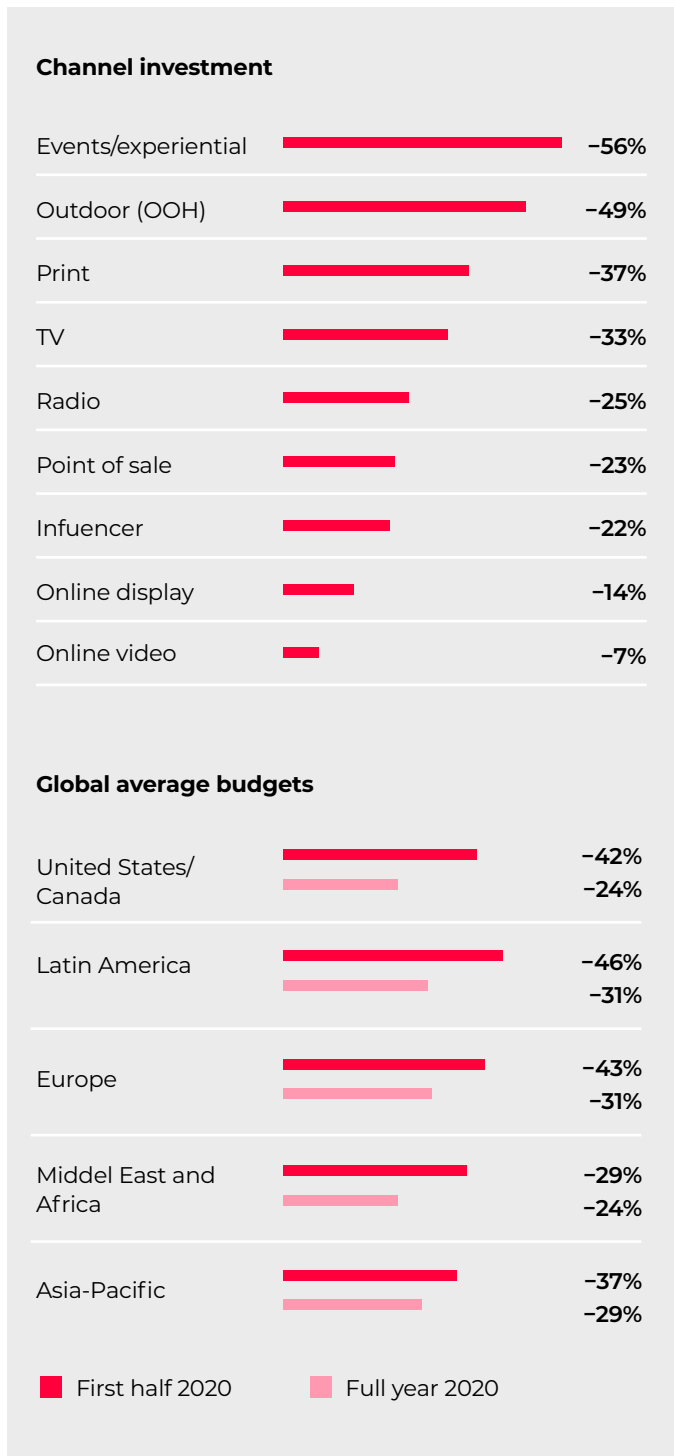Source: Enberg (2019). Reproduced by permission of Insider Intelligence (https://www.insiderintelligence.com/).
© Insider Intelligence 2019.

Fig. 7. Impact of the COVID-19 pandemic on global advertising during 2020 (channel investment and global average budgets)

Channel investment

Events/experiential	**−56%**
Outdoor (OOH)	**−49%**
Print	**−37%**
TV	**−33%**
Radio	**−25%**
Point of sale	**−23%**
Infuencer	**−22%**
Online display	**−14%**
Online video	**−7%**

Global average budgets

United States/Canada	**−42%**
	−24%
Latin America	**−46%**
	−31%
Europe	**−43%**
	−31%
Middel East and Africa	**−29%**
	−24%
Asia-Pacific	**−37%**
	−29%

■ First half 2020   ■ Full year 2020

Source: World Federation of Advertisers (2020). Reproduced by permission of the World Federation of Advertisers (https://wfanet.org/).

in third-party data value in the second half of 2020. Underlying these changes was a shift to higher use of first-party data (data that brands or publishers have collected directly with permission from the consumer), with spend on technology and data infrastructure (including consumer data platforms) up 9.8% in 2019 to US$ 5.5 billion (Winterberry Group, 2020).

Advertising industries in countries where digital marketing already accounts for a majority of ad spend suffered less from the effects of the pandemic. In China, for example, where consumers spend almost two thirds of their media time online, Tencent's digital ad revenues in the first quarter increased by 32% from the previous year (Tencent, 2020). As China reopens, its ad market is predicted to grow by 8.4% even after COVID-19 is accounted for, a figure even larger than the 8% ad growth forecast for the United States pre-pandemic.

COVID-19 has strengthened the position of digital platforms in two ways. They appear to be suffering less relative to others in the advertising ecosystem, enabling them to emerge faster and stronger from the crisis, and they own behavioural data collected during the pandemic. In an industry where all players are trying to understand consumer habits, this will give platforms a competitive edge going forward.

Pressure 3: the major platforms strengthen their data and scale advantage

In February 2020, over 37% of the total time online among Internet users in the United Kingdom was spent on sites owned by Google and Facebook (Fig. 8). Prior to the COVID-19 pandemic, these users were spending an average of three hours and 24 minutes online each day. In April 2020, while most households were confined to their homes, the average Internet user in the United Kingdom spent three hours and 56 minutes online – an increase of 32 minutes each day, of which 39% was on Google and Facebook content (CMA, 2020)

Google collects a vast amount of user data from three main sources: its user-facing services (it provides over 50 such services, including Search and Gmail); mobile devices running Android and computers running Chrome, Google's operating system and browser; and the analytical technology it places on third-party sites and apps (known as tags).

Facebook gathers user data from the three main services it provides in the United Kingdom (Facebook, Instagram and WhatsApp) and from Facebook analytics technology placed on third-party sites (known as pixels) based on the ability to log into third-party services and apps using the Facebook log in.

The growing dominance of Google and Facebook properties in the United Kingdom can clearly be seen from the trends in numbers of unique users and total user time spent from 2015 to 2020 (CMA, 2020) (Fig. 9).

Fig. 8. Consumer time spent on top online properties in February 2020, United Kingdom
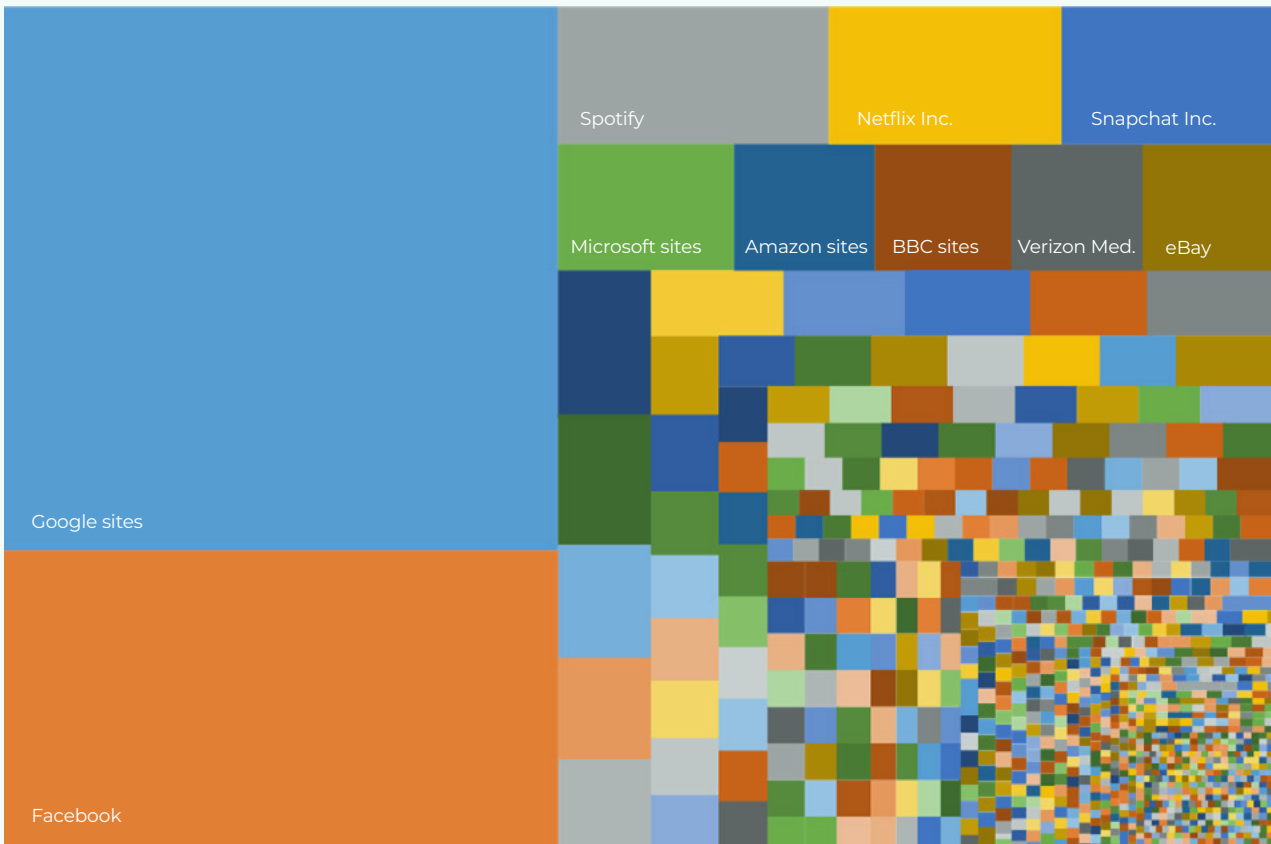
Source: CMA (2020). Reproduced by permission of the Competition and Markets Authority (www.gov.uk/government/organisations/competition-and-markets-authority) under Open Government Licence v3.0.

Fig. 9. Trends in social media use from July 2015 to February 2020: monthly active users (left panel) and total user time (right panel)
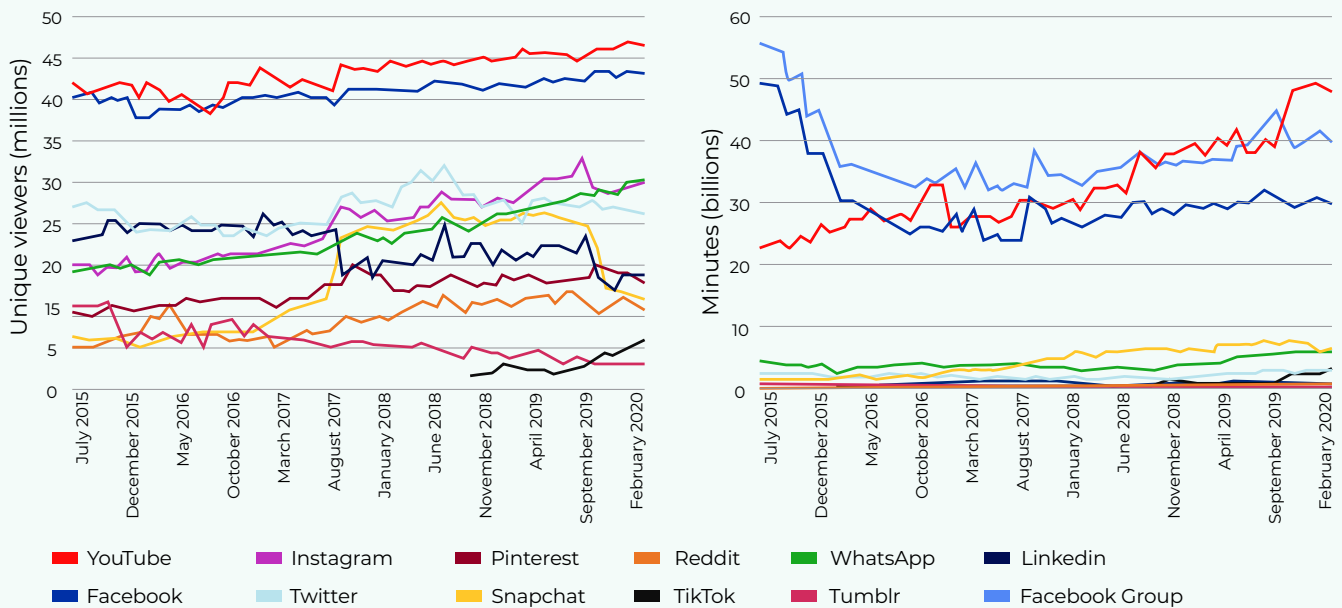
Source: CMA (2020). Reproduced by permission of the Competition and Markets Authority (www.gov.uk/government/organisations/competition-and-markets-authority) under Open Government Licence v3.0.

> ### Some key terms
>
> **First-party data** – data that an entity (brands and publishers) have collected with permission from their own consumers. The permissions determine the rights of the entity for the use of the data.
>
> **Data-management platforms (DMP)** – a software platform used for collecting, organizing and distributing data, allowing businesses to identify audience segments for targeting of advertising.
>
> **Demand-side platforms (DSP)** – technology platforms used by brands and agencies to buy targeted programmatic media.
>
> **Mobile ad IDs (MAIDS)** – the mobile ad ID (either the Apple iOS ID for advertising or the Android advertising ID) identifies phones and devices for advertising and is given by the device's operation system. The ID contains randomly selected numbers and letters and is used by advertisers to identify a device. The mobile ID can be used by free phone applications to understand the user and their choices and behaviour.
>
> **Supply-side platforms (SSP)** – technology platforms that enable publishers to sell their advertising inventory in the programmatic advertising ecosystem.
>
> **Third-party data** – data collected by an entity that does not have a direct relationship with the end-user (data subject) whose data are being collected.

Historically, it has been the reach of data collection from third parties' sites and applications that has really set Google and Facebook apart from the other smaller platforms and the open programmatic ecosystem (Fig. 10). The sustain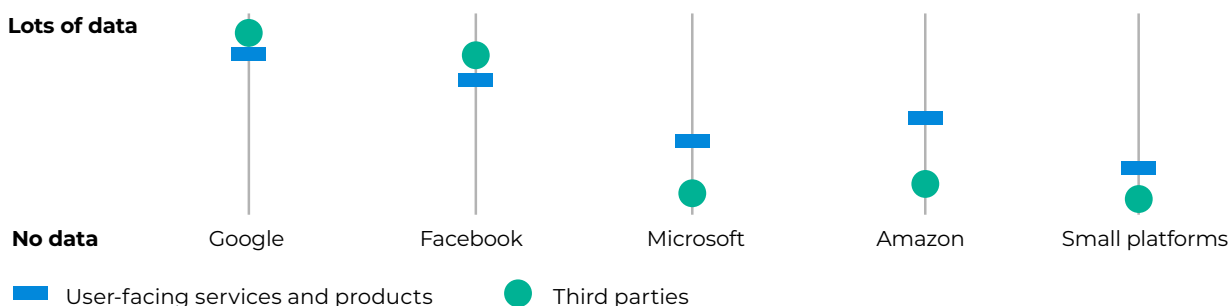ability of this network reach depends on the use of third-party cookies and MAIDs persisting in the future – without cookies, Facebook and Google will focus their data-mining capabilities on their own publisher networks.

Fig. 10. Relative scale of data collection by certain platforms, by first- and third-party data sources

Source: CMA (2020). Reproduced by permission of the Competition and Markets Authority (www.gov.uk/government/organisations/competition-and-markets-authority) under Open Government Licence v3.0.

Google offers in-depth targeting options driven by its unique and vast sources of data, while Facebook has the advantage of offering the ability to target specific audiences based on demographic characteristics, interests and location. This creates a substantial competitive advantage for Google and Facebook, both of which have access to more extensive datasets than their rivals. The inability of smaller platforms and publishers to access user data creates a significant barrier to entry.

Google and Facebook also have significant advantages in providing brands and agencies with the ability to measure the performance of digital advertising bought through them. Google tags are known to be present on roughly 80% of the highest traffic websites and Facebook has pixels present on around 40–50% of the highest trafficked websites and apps. Google and Facebook can therefore offer a more measurable and compelling advertising product to brands and agencies. This measurement capability, however, is crucially dependent on the third-party cookies and MAIDs provided by the main browsers (Google Chrome and Apple Safari) and mobile operating systems (Google Android and Apple iOS). These same identifiers also underpin independent publishers' ability to offer data-targeted personalized advertising to compete with Google and Facebook through the third-party open programmatic ecosystem.

One of the unintended consequences of privacy regulation in the EU and the United States was that the practices of the technology solutions outside of Big Tech's main walled gardens – the independent publishers, DSPs, SSPs and DMPs – were more challenging and difficult to maintain than the larger closed-garden publisher platforms. Over 2019–2020, major publishers in the United States and the EU developed consumer

consent management solutions for data and cookie usage so they could use the established programmatic data-targeting techniques. For the larger publishing walled gardens with their own in-house advertising technology platforms and data assets, this was a relatively straightforward development: consumers were keen to continue to use Facebook and Google services, so were likely to give consent. The consents were kept quite simple because there was only one company involved in the consent chain.

Some platforms operate a take-it-or-leave-it model in which they do not give their users the ability to control their data. This initially was particularly prevalent across most social media platforms, including Facebook and Instagram, whose users are unable to turn off personalized advertising while continuing to use the service, although more granular consent management approaches are now being built into the major platform services. This is in contrast to search engines: both Google Apple Safari and Firefox allow consumers to opt out of personalized advertising and some search engines such as DuckDuckGo do not use personalized advertising at all (CMA, 2020). The CMA in the United Kingdom recommends that platforms be mandated to provide a basic level of service to consumers who do not want to give consent to use of their data.

Smaller publishers did not have the luxury, however, of being able to operate on take-it-or-leave-it terms. They have had to depend on linked third-party technology and data companies to deliver the same performance-enhancing data-targeting and measurement needed to compete. This means that the consents they require are more complex. The ability to offer data-targeted advertising at scale is dependent on the third-party

programmatic advertising technology ecosystem, which relies on cookies and MAIDs to operate. In the midst of this complexity, brands and advertisers moved their spending to Big Tech's walled-garden platforms, which continued to deliver ever increasing campaign-scale and data-enhanced targeting performance.

Pressure 4: concentration in the third-party open display ecosystem

Another area of increasing concern in the digital media supply chain identified by the CMA analysis of market conduct in the digital advertising ecosystem is the growing dominance of Google at all stages of the third-party (that is, supporting independent publishers) programmatic supply chain for video and display advertising. The open ecosystem of technology players serving publishers generally has weakened and consolidated under the pressure of competing with the walled gardens of Big Tech companies. This means that in addition to its dominant advertising share in search (90% of search spend in the United Kingdom) and video advertising/YouTube (8% of display spend in the United Kingdom), Google's technical solutions have become the de facto market leaders for independent publishers to support their digital advertising businesses. Google has between 50% and 90% market spend share of the various technology platforms through which independent publishers buy advertising (Fig. 11). As a result, in aggregate, Google is also taking a very large share of the 35% of advertising revenue that independent publishers pay technology platforms to support their programmatic advertising businesses.

One of the key control points is the policy that Google has its own platform (the Display & Video 360 (DV360)

Some key terms

Advertiser ad server market – technology companies that provide advertising serving platforms (the technology that serves a specific ad creative to a specific advertising slot) to brands and agencies, as well as publishers.

DoubleClick for Publishers – Google's supply-side platform.

Demand-side platforms (DSP) – technology platforms used by brands and agencies to buy targeted programmatic media.

Open ecosystem – the independent publishers and technology platforms that sit outside of the Big Tech walled gardens owned by, for instance, Facebook, Google and Microsoft.

Header bidding – a new approach to exchange transactions designed to improve yield for publishers in which to maximize the win and gain more control over the bidding process, publishers offer an ad impression to several ad exchanges simultaneously. By giving the chance to bid on an ad to multiple demand source bidders, the profit of the publisher can be increased by accepting the best offer (Morrisroe, 2020).

Supply-side platforms (SSP) – technology platforms that enable publishers to sell their advertising inventory in the programmatic advertising ecosystem.

Walled gardens – large technology companies that provide a full-service publisher, advertising technology and data solution to advertisers (usually Google and Facebook, but also Snapchat and TikTok). In the digital world, a walled garden is a closed ecosystem in which all the operations are controlled by the ecosystem operator (de Poulpiquet, 2017). The main platforms with walled gardens are Facebook, Google, Amazon, Microsoft and Apple.

Waterfall bidding – a prevalent methodology for programmatic advertising transactions on exchanges which contrasts with Open Bidding, in which a publisher (seller) offers ad impressions to predetermined ad networks (buyers) for a fixed minimum price per impression (floor bid) in sequential order. That means if the publisher offers an ad impression for a minimum price of US$ 0.02, it will be sold to the first ad network to which it is offered that meets the floor bid (Zeropark, 2021).

demand-side platform) that is mandated to serve ads in YouTube. Given the growing importance of video display advertising and YouTube's dominance in video, this puts a lot of pressure on brands and agencies to use Google's DV360 platform for campaigns across several media.

Another key area of concern highlighted in the CMA report is Google's reluctance to participate in industry-wide publisher header-bidding initiatives. These recent initiatives allow publishers to accept the highest bid from advertisers rather than having to accept the first bid that meets the minimum price in the default waterfall bidding system. Established by the ad exchanges (of which Google AdX had a market-leading position), publisher header-bidding initiatives were launched in 2015 to counteract the bias in Google's waterfall-bidding platform. Google claims that because header bidding involves publishers offering the ad to different bidders, header bidding slows down the process, so it prefers to support its own proprietary platform (Open Bidding). In the United Kingdom CMA report on the industry, Google's documents showed that a major reason for the introduction of its Open Bidding platform was to protect Google's revenues from the impact of header bidding, while providing a service from which publishers could to some extent benefit. Open Bidding was designed in a way to avoid creating an alternative route directly competing with Google's AdX and to disadvantage third-party SSPs.

This is one example among several conflicts of interest that are inherent when a company has a majority share of all stages in the auction value chain for third-party

programmatic advertising. Fig. 11 illustrates Google's roles in the different stages of the chain. This is an area of specific concern to antitrust regulators, including those in the United Kingdom and the United States.
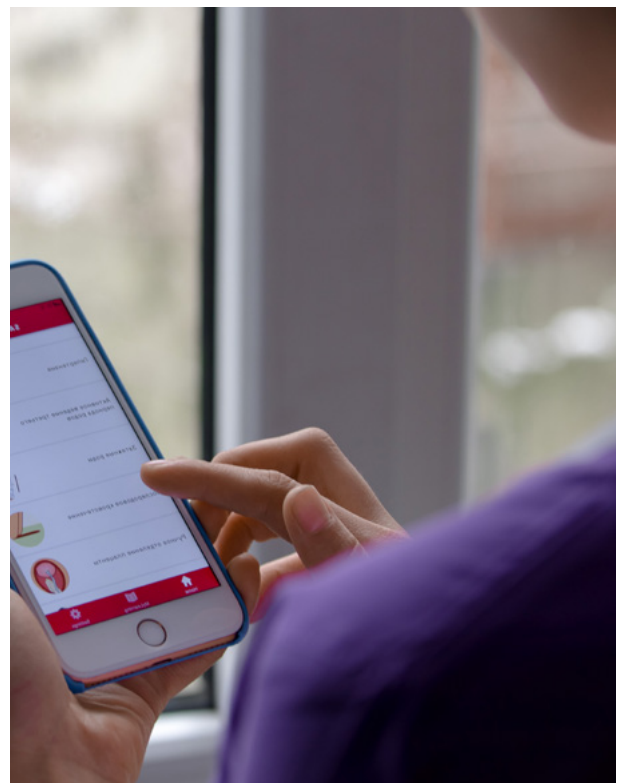
Fig. 11. Illustration of Google's role in the digital advertising market

| Google share [90–100%] | Google share [50–60%] | Google share [50–60%] | Google share [80–90%] |

| Publisher | Publisher ad server | SSP | | DSP | Advertiser ad server | Advertiser |

Sell side | Buy side

Large publishers	Google Ad Manager	Display & Video 360 Campaign Manager	Large advertisers
Small publishers	Google AdSense		
Mobile app publishers	Google AdMob	Google Ads	Small advertisers

Source: CMA (2020). Reproduced by permission of the Competition and Markets Authority (www.gov.uk/government/organisations/competition-and-markets-authority) under Open Government Licence v3.0.

Pressure 4a: consolidation in DSPs

Media agencies running advertising campaigns use technical tools called DSPs to buy, serve and track advertisements. The DSP allows ad campaigns to be tagged with information that ensures it is sent only to users with specific characteristics – that is, those who are most likely to be interested in buying.

One of the key potential control points is the policy that Google leverages in its own platform (the DV360 DSP) that is mandated to serve video ads in YouTube, a significant media choice in the digital media landscape. Given the growing importance of video display advertising and YouTube's dominance in video, this puts a lot of pressure on brands 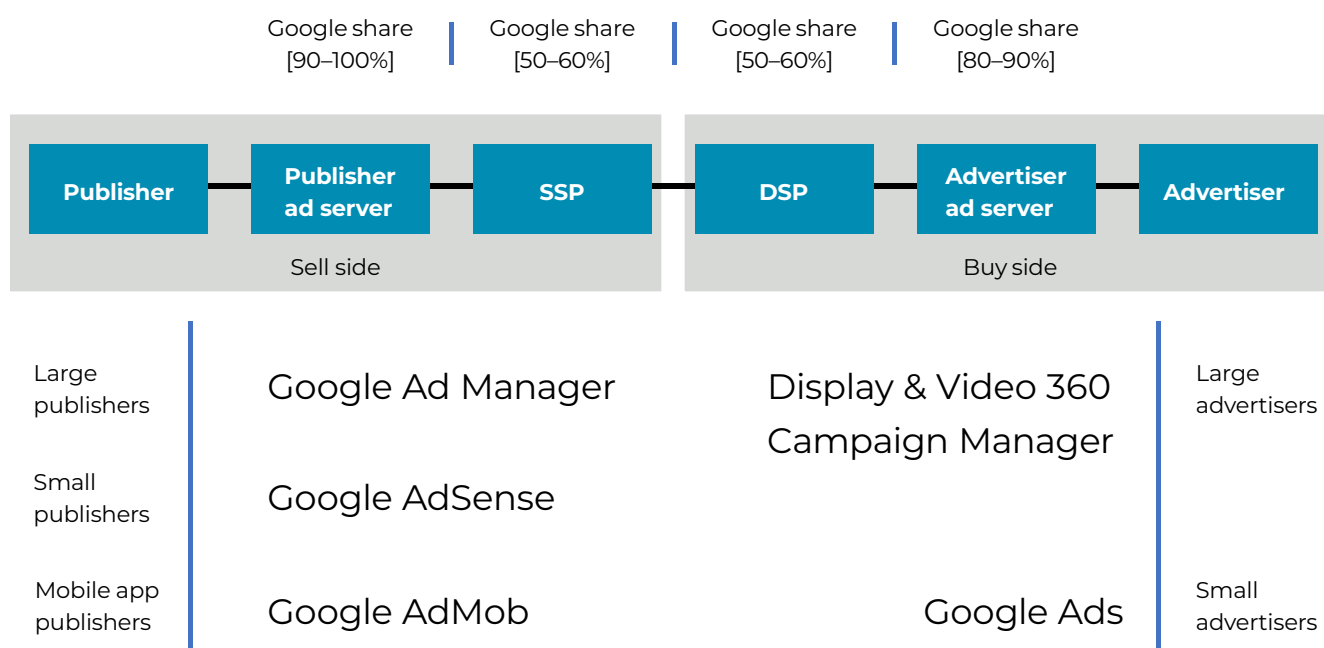and agencies to use Google's DV360 platform for campaigns. It then makes sense for agencies and brands to use DV360 more widely across all of their multi-media campaigns, making it harder for independent DSPs to thrive.

By only allowing advertisers to place ads on YouTube through its own DV360 platform, Google can take advantage of how important YouTube is for advertisers (as well as its high level of technology investment) to increase its market power in the DSP sector (Table 1). Google has argued that restricting third-party access to YouTube inventory is the best way to maintain the privacy of user information and to ensure that the ads appearing on YouTube are of a consistently high quality.

Table 1. Estimated market shares of DSPs in 2019 (percentage of value of ads purchased, with and without Google Ads)

DSP	Market share not including Google Ads (as % of value of ads purchased)	Market share including Google Ads (as % of value of ads purchased)
Google DV360	40–50	30–40
Google Ads	NA	10–20
The Trade Deck	10–20	0–10
Xandr	0–10	0–10
Criteo	0–10	0–10
Amazon DSP	0–10	0–10
Others (Quantcast, Verizon Media, Adobe, DataXu, Adform)	10–20	0–10

NA: not applicable.
Source: CMA (2020). Reproduced by permission of the Competition and Markets Authority (www.gov.uk/government/organisations/competition-and-markets-authority) under Open Government Licence v3.0.

Google has exclusive access to a large amount of user data that can be used for targeted advertising and for measuring advertising outcomes. These data are collected through the services it provides direct to consumers. Data collected on its search platform are particularly valuable for targeting, as they reveal users' purchasing intent. The availability of log-in data allows Google to identify all the computers and mobile devices associated with a user, relating all the data about the user to a single user ID.

Although larger advertisers and media agencies often use multiple DSPs across advertising campaigns, typically a single DSP is used for a given campaign, as this allows the advertiser to manage and control the entire campaign and facilitates better reporting. Some large advertisers use a single main DSP across all their campaigns, typically Google's DV360.

Pressure 4b: consolidation of SSPs

When an Internet user clicks through to a publisher's website, an ad request is sent to SSPs selected by the publisher. These SSPs manage the programmatic selling of the publisher's advertising inventory.

Since the introduction of header bidding in 2015, which allowed publishers simultaneously to send ad requests (known as ad impressions) to several SSPs, all major SSPs have had access to much the same publisher inventory of ad space and compete head-to-head on performance and price for each single impression. Header bidding arguably has made it easier for new SSPs to enter the market. At the same time, because all SSPs now have the same space to sell, they have to compete on the basis of price or the service provided, and this is pushing down their profit margins (Table 2) and driving consolidation.

Research from the Incorporated Society of British Advertisers shows that publishers receive only half of the money that brands spend with online publishers – the rest is lost in the programmatic advertising supply chain, and it is not completely clear where 15% of this money goes (Incorporated Society of British Advertisers, 2020). This underlines the problems with the digital advertising business model, where a so-called publisher's paradox (Sternberg, 2020) sees traffic increase, but not revenue. These challenges have been exacerbated by the COVID-19 pandemic and suggest that **greater transparency in the value chain is still required**.

Table 2. Estimated market share of SSPs in 2019 (% of total value of ads sold)

SSP/ad network	Market share (as % of value of ads purchased)
Google AdX	20–30
Google AdMob	10–20
FAN	10–20
Google AdSense	0–10
Xandr	0–10
Teads	0–10
Taboola	0–10
Others (Rubicon Project, Index Exchange, Outbrain, OpenX, Pubmatic, Triplelift, Smart, Freewheel, Verizon Media)	10–20

Source: CMA (2020). Reproduced by permission of the Competition and Markets Authority (www.gov.uk/government/organisations/competition-and-markets-authority) under Open Government Licence v3.0.
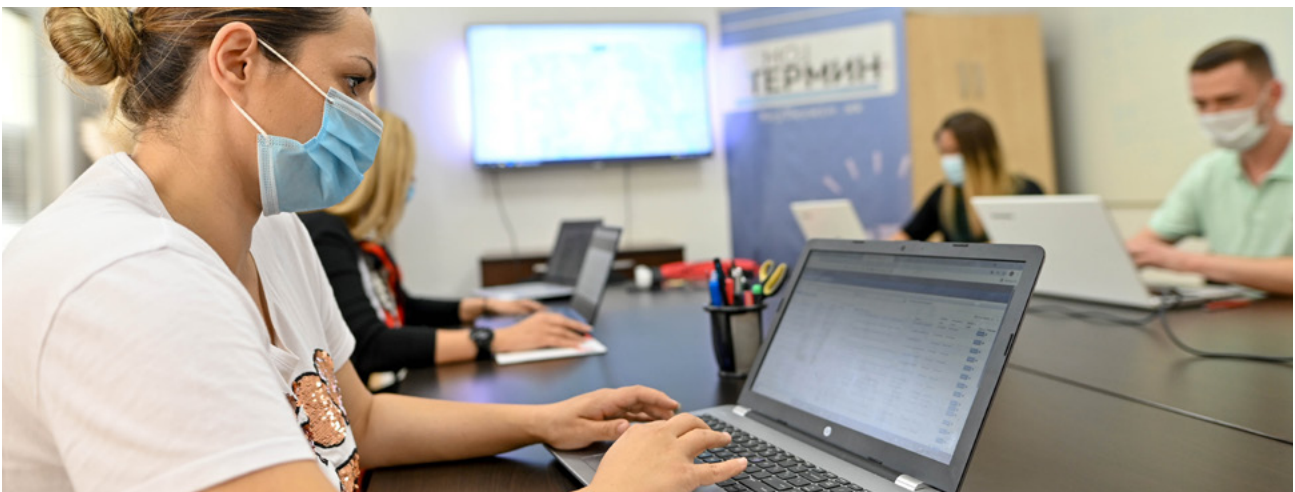
Pressure 5: political pressure

Another current area of pressure relates to antitrust, regulatory, political and commercial pressure on the main platforms: Google, Facebook, Amazon, Microsoft, Twitter and TikTok. The immediate pressure on Big Tech platforms became increasingly political in 2020.

- Market dominance became more obvious in the 2020 pandemic. The market value (capitalization) of Amazon, Apple, Google, Facebook and Microsoft now represents a staggering 25% of the Stan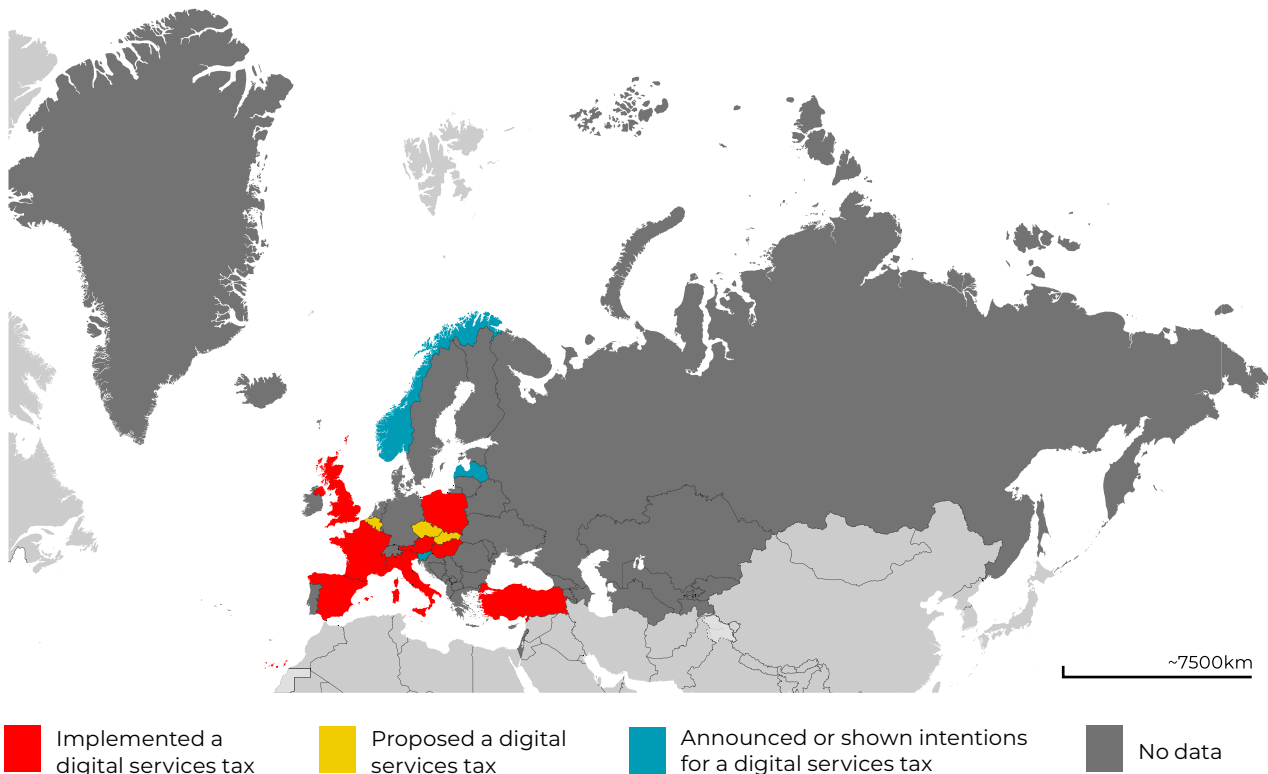dard & Poor's 500 index, and the value of these companies grew to US$ 7 trillion market capitalization in 2020 during the COVID-19 pandemic.

- Digital services taxes have been planned across most EU/OECD states (Fig. 12). In the United Kingdom, for example, a digital services tax has been introduced at a rate of 2% on revenues from search engines (Google), social media (Facebook) and online marketplaces (Amazon). This initially has been passed on as price increases to advertisers and sellers.

- Mobile apps became political, with outright bans and trade wars. India blocked TikTok and WeChat in June 2020, citing national data-security concerns. In August 2020, the United States ordered the disposal of TikTok operations in the country by November.

The United States tried to enforce a ban on TikTok and WeChat in September by removing them from Apple and Google app stores. These measures were relaxed in February 2021.

- Digital monopolies were challenged. In October 2020, the Congress of the United States filed an antitrust suit against Google, and the Administration of President Biden has since signalled concern about the dominance of Big Tech. Monopoly antitrust action is expected in the United States and other major markets (the United Kingdom, for example, is setting up a Digital Markets Unit in the CMA). Possible extreme solutions being mooted include the breakup of Facebook/Instagram/WhatsApp and the spinout of Google's digital advertising business. France, Germany, Sweden and the United Kingdom each undertook assessments of the digital media markets in 2020 and Australia, Germany, Japan, the United States and the EU already are discussing regulation of the major digital advertising platforms. Pressure is building.

- Most marketers in the United States believe, however, that while Big Tech will be subject to policy changes or fines, no outcomes on antitrust will come soon, and fewer than 10% believe that actual breakups of Big Tech companies will occur (Winterberry Group, 2021a).

Fig. 12. Current state of digital taxes and consumer data-privacy regulation (digital services taxes announced, proposed and implemented in Europe by October 2020)

Color	Legend
Red	Implemented a digital services tax
Yellow	Proposed a digital services tax
Teal	Announced or shown intentions for a digital services tax
Grey	No data

~7500km

Source: Asen (2021). Reproduced by permission of the Tax Foundation (https://taxfoundation.org/) under a Creative Commons Attribution NonCommercial 4.0 International License.

Pressure 6: data-privacy regulation became a "reality" in 2020

Data privacy has become a binding constraint on ad tech as global privacy regulation rolls out worldwide, matched by consumer awareness and concerns. Regulators in many key markets have been busy, and the message to the ad tech industry is that practices and platforms for data processing will finally **have to** change.

Examples include:

- the Children's Online Privacy Protection Act: this federal legislation launched in the United States as far back as 1998 sets guidelines for companies that collect and use data from children; it mostly is concerned with consent and parental permission for any data collected on a child under 13 years of age;

- the EU GDPR became law in April 2018; since Brexit, the United Kingdom has adopted a mirror regulation with some slight amendments (the Keeling Schedule) and currently is in consultation for a redraft of replacement United Kingdom-specific consumer privacy regulation;

- the CCPA came into effect in January 2020, and the California Privacy Rights Act is a state-wide data-privacy bill passed into law in 2020; it will become enforceable on 1 July 2023 and will significantly expand on the data-privacy requirements in the CCPA, tightening business regulations on the use of personal information and establishing a new enforcement agency; Virginia and Colorado have followed suit and it is expected that additional state-level regulation will follow, but many in the industry would prefer consistent federal legislation on consumer privacy in the United States;

- other global jurisdictions (Comforte, 2021) have passed equivalent consumer-privacy legislation, including the Personal Data Protection Act in Thailand, the Privacy Act Amendment in Australia, the General Data Protection Law in Brazil, the Act on Protection of Personal Information in Japan, the Personal Information Protection Act in the Republic of Korea and data-privacy regulation embedded in Chile's new constitution; and

- the Personal Data Protection Bill (passed in India in 2019), Protection of Personal Information Act (in South Africa in 2020), Personal Data Protection Law (in China in 2020) and the Digital Charter Implementation Act (in Canada in 2020) are in the draft legislative phase.

The EU ePrivacy Directive (Directive 2002/58/EC) is an additional draft EU regulation (updated in 2017 in the context of the GDPR) that requires consent for the non-essential storage of information or access to information stored on end-user devices, irrespective of whether such information can be considered personal data. The notion of consent in the context of the ePrivacy Directive

evolved to match the stricter requirements for valid consent adopted under the GDPR. For cookies to be stored and accessed in compliance with this reinforced definition, consent must be prior, freely given, specific, informed, withdrawable and unambiguous. This brings a number of implications:

- the proposed regulation would change significantly the way consent for online tracking (including third-party cookies and MAIDs) can be gathered;

- browsers would be required to ask users to opt into tracking via their privacy settings, rather than the cookie notification banners displayed on websites today;

- browsers will be required to ask users whether they wish third-party tracking (including cookies) to be activated upon installation; browsers already installed will be required to ask for consent during the next update or by the agreed deadline;

- the European Commission proposal suggests that browsers should offer a range of privacy-setting options, including "never accept cookies", "reject third-party cookies", "always accept cookies" and "only accept first-party cookies";

- specific configuration cookies (such as those for remembering the contents of a shopping basket) are distinguished explicitly from others and consent is not required;

- users would need to provide freely given, specific, informed and unambiguous consent for cookies and other types of third-party tracking used for digital advertising, which is a significant change from the notification and implied consent regime in place in many countries today that takes the form of a pop-up notification when a user visits a website for the first time; and

- the proposal for ePrivacy also introduces potential fines of up to €20 million or 4% of annual global turnover – which is identical to the fines facing companies under the GDPR.

By January 2021, 533 fines had been imposed in EU countries under GDPR since the regulation became law in March 2018 (CMS, 2021). The larger the fine

and the bigger the target, the more the digital advertising ecosystem takes notice and changes in technology and processes are implemented.

Data privacy remains a key concern for marketers in the United States, but the so-called marketers panic seen in 2019 as the reality of regulation became clear has somewhat abated to be replaced by COVID-19 concerns. In a July 2020 survey of marketers in the country, the Winterberry Group found only 18.9% of survey respondents reporting that such regulation would represent a primary challenge for their organizations in 2020 – significantly down from the 52.7% who said the same late in 2018. Diminished concern is probably linked to higher-order issues like COVID-19, but also indicates the level of investment in new solutions and processes to adapt data-collection practices to be in line with the new regulation (Winterberry Group, 2021b). Recently, however, the focus of marketers has turned to how customer permissions can be gained while enhancing overall customer experience.

The emergence of class-action or representative lawsuits in 2020 has also raised the game for global Big Tech and ad tech companies. For example:

- in September 2020, Duncan McCann, a father of three in the United Kingdom, launched a representative action in the High Court against the Google-owned video-streaming service YouTube over claims the platform routinely breaks United Kingdom and European data-protection laws by unlawfully targeting up to 5 million children – who cannot legally consent to their data being processed – with addictive programming and then harvesting their data for advertisers (Hodge, 2020); Google could owe affected children and parents more than GB£ 2 billion (US$ 2.5 billion); and

- the Privacy Collective launched a class-action lawsuit in courts in the Netherlands and the United Kingdom in August 2020 against tech firms Oracle and Salesforce for alleged GDPR violations over their use of cookies to harvest personal data (Scroxton, 2020); estimated damages could exceed €10 billion (US$ 11.7 billion).

The GDPR and subsequent mirror legislation in other jurisdictions has had a lasting effect on digital marketing in Europe. With its focus on user privacy, GDPR forced the hand of the marketing industry. The spectre of big fines forced publishers, platforms and media buyers to refocus attention on privacy-first solutions, changing the way digital media was bought and sold in the EU. In the current transition period during which similar privacy regulations are adopted in the United States and in other international markets, the EU's GDPR has caused a chasm in ad tech: throughout 2020 everywhere outside the EU still enjoyed the full capabilities of third-party buying without the overhang of legal culpability, while vendors in the EU have been forced to change to a user-first approach earlier and are building the tech capabilities necessary to operate in this new environment.

The industry still needs coordinated and consistent regulatory frameworks across all key global markets for the industry to define and adopt compliant new technical standards. At its basic level, there is still a different definition of personal data and personally identifiable information (PII) by regulators in the EU and United States (Table 3). The tide is flowing in terms of GDPR standards and definitions being more closely adopted globally and by global technology companies, but there is still widespread debate about whether data at household (rather than individual) level are considered as personal data within the GDPR or other regulatory frameworks.

Table 3. Key differences between the EU GDPR and the CCPA

	GDPR	CCPA
Scope	"Personal data" is any information relating to or that can be used to identify a specific person. It does not include the "household" stipulation.	"Personal information" is anything that identifies, relates to, describes, is capable of being associated with or could reasonably be linked to a particular person or household.
Covered entities	You don't technically need to be a "business" at all – you just need to control or process relevant information.	The CCPA defines a "business" as a for-profit legal entity or sole proprietorship.
Disclosure/ transparency obligations	An entity is required to provide the identity and the contact details of the data controller, the recipients of that data, the legal basis and purposes for processing the retention period, the right of access and more.	Under CCPA, businesses need to inform consumers at or before the point of collection what information is being collected and why it is necessary.
Right of access	The GDPR allows people to learn how long that information is being retained. The GDPR also has an additional "right to portability" in certain cases.	Both the GDPR and CCPA give consumers the right to not only learn what information is being collected, but to also get a complete copy of that information.
Right to deletion	The GDPR applies to ALL data concerning a data subject, no matter where from.	The CCPA only applies to data collected FROM the consumer.
Right to opt out	The GDPR includes no such right. The GDPR is strict in other areas that if a consumer didn't want you to store and sell their data, there are other techniques they could use.	At any moment, the CCPA allows people to opt out of a business' ability to collect or sell their personal data. At that point a business is prohibited from doing anything meaningful with the data in any way.

Source: Gallacher (2018). Reproduced by permission of IS Partners (https://isp.capital/).

> ## Some key terms
>
> **Personally identifiable information (PII)** – elements that directly identify a person, such as a name, address, phone number, email address and a limited range of other identifiers.
>
> **Non-personally identifiable information (non-PII)** – any data that do not directly identify an individual. In the United States, this includes proxy identifiers such as cookies, mobile ad identifiers, Internet protocol (IP) addresses and other identifiers that may be unique but do not allow direct recognition of the individual. Under the EU GDPR, it can still be classified as Personal Data that require explicit opt-in consent to be used for the targeting of advertising.
>
> **Personal data** – the term used under GDPR that has a much wider scope than "personally identifiable information" because it includes data attributes that may single out and identify individuals when combined with personal data. This means that IP addresses, mobile ad identifiers, specific latitude/longitude elements, cookies and device IDs generally are classified as Personal Data under the legal remit of the GDPR.

There is strong support for a coordinated approach to global privacy regulation through Project Rearc (IAB Tech Labs, 2021) and the Worldwide Web Consortium (W3C) (W3C, 2021). Project Rearc is a new initiative from IAB Tech Labs that is designed to reconfigure the digital media supply chain according to privacy-by-design technologies. There is, however, still a long way to go. For instance, it is likely that more identifiers (including the MAID/ID for advertising (IDFA)/Android advertising ID (AAID)) and IP addresses will be considered PII under regulation in the United States in the future to more closely align with GDPR.

Despite this, by January 2020 marketers in the United States reported significantly reduced concern about new data-privacy regulation compared to 2019, and relatively

few reported reducing their spending or reliance on data. This implies that much investment in new consent mechanisms and data-management practices already is being implemented (Biegel, 2020) (Fig. 13). While the future ecosystem is still being defined, money continues to flow.

> ◆ For the last few years, the global digital advertising ecosystem has been facing many pressures, including the continuous shift to digital marketing, effects of the COVID-19 pandemic and further strengthening of the data and scale advantages of the Big Tech players, as well as political and regulatory pressures that include greater data-privacy regulation.

Fig. 13. Company actions reported to address new/potential data-privacy regulations in 2020 (%)
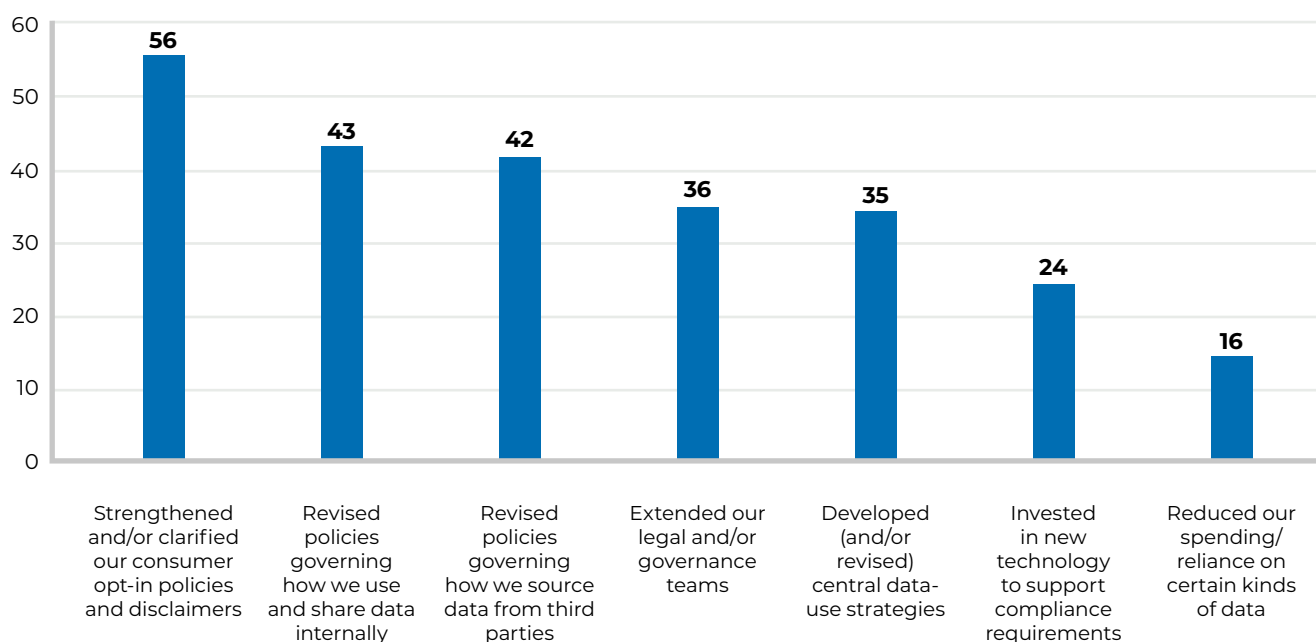
Source: Biegel (2020). Reproduced by permission of the Winterberry Group (https://www.winterberrygroup.com/).

Impacts of the pressures on the digital ecosystem between 2018 and 2020

A number of impacts on the digital ecosystem as a result of the pressures described above can be observed.

Impact 1: continued concentration of spend in global walled gardens

One of the effects of these multiple pressures on the digital marketing ecosystem is that ad spending has become even more concentrated in the global walled gardens of the Big Tech players.

Digital advertising increasingly has created flexible and affordable opportunities for smaller companies, and this has been part of their success. The scale of Google and Facebook provided the possibility for small- and medium-sized advertisers to reach potential customers on a national scale. These platforms provide self-service interfaces that automate and simplify the complex process of buying advertising. This makes advertising accessible to businesses with very small budgets, or even to individuals, resulting in Google and Facebook having a small number of large advertiser buyers and an extremely large number of customers with relatively low expenditure. Facebook has over 1 million advertiser customers in the United Kingdom and Google has over 200 000. The top 5–10% of advertisers on Google and Facebook, however, made up more than 85% of the total revenues of each, so despite the long tail, the vast majority of their revenue still comes from a small number of large companies.

Large agencies and brands progressively have moved significant amounts of spend to Google and Facebook even though they continued to raise concerns about media consolidation. In 2019, for example, 80% of the GB£ 14 billion spent on digital advertising in the United Kingdom was spent on Google (90% of search advertising, 8% of video/display advertising) and Facebook/Instagram (50% of display and video advertising) (CMA, 2020). Although use of alternative social platforms (Snapchat, Pinterest and TikTok) is growing, their share of the digital advertising market in the United Kingdom remains low. Without the reach and data power of the larger networks, it is harder for these platforms to gain a significant share of advertising revenue.

In June 2020, the United Kingdom's CMA raised the following concerns about market structure.

- Facebook has significant market power in display advertising. It accounts for over half of display-advertising revenues and is seen as a must-have platform for many advertisers because of its reach. It has a significant data advantage over smaller platforms and publishers, which both increases the value of its advertising inventory and creates additional barriers for its competitors to overcome. This has allowed Facebook to earn significantly higher revenues per user than its competitors, increasing annual revenue per user from an average of GB£ 0–5 in 2011 to GB£ 50–60 in 2019.

- Google has significant market power in search advertising. It accounts for over 90% of search advertising revenues and faces limited competitive constraints from other forms of advertising. Its rivals face significant barriers to attracting advertisers, in addition to barriers on the consumer side. Google's market power has allowed it to charge higher prices to advertisers than its competitors. On a like-for-like basis, Google's prices are on average 30–40% higher for desktop advertising and 30–40% higher for mobile advertising than those of Bing.

Facebook's revenues in the United Kingdom increased from around GB£ 100 million in 2011 to more than GB£ 2 billion in 2019, partly explained by an increased number of users and the rise in annual revenue per user described above. One driver of the revenue figures is the number of ads served to users, with the number served per hour increasing from 40–50 in 2016 to 50–60 in 2019. This increase in so-called ad load partly explains why Facebook's revenue per hour is greater than other platforms and has increased in the past four years (Fig. 14).

Fig. 14. Trends in average platform revenues and platforms' shares of display advertising (average annual revenue per user for selected platforms 2011–2019 in GB£ (left) and percentage shares of expenditure in United Kingdom display advertising in 2019 (right))
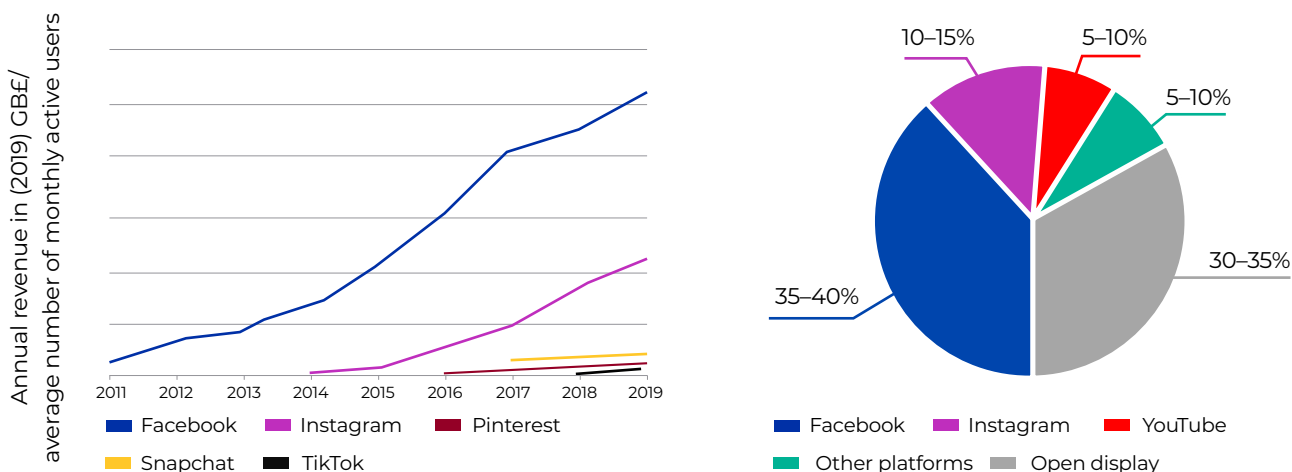
Impact 2: publishers fight back – new format development

Publishers and advertising technology companies have come up with new platforms and solutions. One of the endemic issues for publishers and media owners outside of the large walled gardens is that the cost of participating in the programmatic digital media market and working with multiple tech partners on the buying and selling side of the complex market means that the publisher's revenue is often only 50–60% of the total campaign value, whereas Facebook and Google capture a much larger net revenue share of bookings. As the mix of advertising has been driven to programmatic auctions, independent publishers have been getting a smaller share of the pie and, in some cases, have been earning less money even though total demand for their ad space has increased. In response to this – and as more offline ad space, such as advertising in the OOH and audio sectors, moves to the digital programmatic approach – the publishers and advertising technology companies have been innovating to draw money into publishers away from Google and Facebook.

The key areas of recent innovation include, with active development from the still vibrant third-party technology ecosystem:

- in-app video and display advertising (Ironsource, Applovin, Vungle, Unity);
- audio/podcast (Adswizz, Spotify);
- connected TV programmatic (Internet Advertising Bureau UK, 2020) – TV sets connected to the Internet through a streaming device or smart TV to watch broadcast-quality long-form video content live or on demand (Freewheel, SpotX, Magnite);
- in-game (Anzu, Adverty, Admix);
- native (Tripleshift, EngageYa, Gum-Gum, Picnic);
- digital OOH (Broadsign, Stratacache, Amscreen, Vista);
- voice assistant search (Amazon Echo, Google Home, Apple Alexa, Microsoft Cortana); and
- augmented reality (Blippar, Darabase, Snapchat, Ubiquity6).

Impact 3: commercial pressure – money talks

An important impact of growing consumer awareness and concerns about Big Tech conduct is that some advertisers periodically have stopped advertising on some platforms. In June 2020, for example, Unilever, Coca-Cola, Starbucks and more than 90 other advertisers removed spend from Facebook, Instagram and Twitter in response to hate-speech concerns in light of the Black Lives Matter movement. Commercial pressures forced more rapid changes on publishing and content policies around so-called hate speech. It has become increasingly clear that **growing consumer awareness matters.** Following on from the Cambridge Analytica scandal in 2018, the Netflix documentary "The Social Dilemma" aired in 2020, highlighting the dangerous practices of data harvesting, surveillance capitalism, ad targeting and habit forming in the major social platforms. Watched by 38 million people in 2020, the documentary generated a new wave of concern by Facebook users about the company's data practices.

Impact 4: "Tech for Good" rhetoric

Recognizing the need to appease (future) politicians and regulators, agencies, brands and consumers amid a shifting of consumer sentiment, major platforms are starting to adjust their defence of their dominant platform status. In early 2020, Facebook established a global Oversight Board (Facebook, 2021), the effectiveness of which has been questioned in light of the 2021 revelations made by whistleblower Frances Haugen (Wired, 2021). Twitter and Facebook marked political posts and censored fake news during the election in the United States in November 2020. In January 2021, Twitter (Twitter, 2021) (permanently) and Facebook (Kelly, 2021) (indefinitely) took unprecedented moves to ban former President Trump from platforms. Facebook launched its News Tab service to broadcast personalized news from certified publications in January 2021 and stated that it should not be regulated as a platform or a utility, but as a special case. In face of the growing political pressures and antitrust scrutiny, major tech companies, and Facebook in particular, ramped up their lobbying investment in Washington (DC) in 2020 (Fig. 15). Big Tech platforms clearly are recognizing that future regulation is likely, and this is accelerating efforts to adapt their data and advertising practices.

Fig. 15. Trends in lobbying expenditure of major tech companies (in US\$ millions)
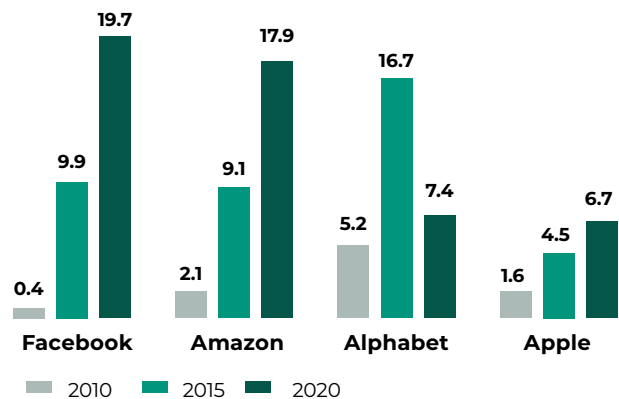
Note: Alphabet is the parent company of Google.
Source: Richter (2021). Reproduced by permission of Statista (https://www.statista.com/) under Creative Commons License CC BY-ND 4.0.

◆ The pressures facing the global digital advertising ecosystem have impacted on the ecosystem in multiple ways. Changes include an increasing share of total digital spend on Google and Facebook, development by publishers and technology companies of new and innovative formats, evidence of consumers and brands reacting against the practices of major platforms, and changes in the behaviour and positioning of the major technology companies. Dominant success based on the best data and technology is now generating a widespread reaction to how the digital advertising ecosystem should evolve in the near future.

07.

How Big Tech has reacted to these pressures

These pressures on the global digital advertising and technology ecosystem have driven a range of responses from the major platforms.

Business models of the five major Big Tech companies of the United States

The different business models and commercial objectives of the five major Big Tech companies of the United States (Apple, Google, Facebook, Amazon and Microsoft) to a large extent have determined their respective reactions to pressures on the digital advertising ecosystems. Collectively, the decisions they have made will shape the structure of the industry going forward. In the global advertising ecosystem, most attention is focused on the relative power of Google and Facebook, but when it comes to the underlying technology, it is the struggle between Apple and Google that has defined the underlying technology developments.

Apple is largely a global hardware business, with 86% of its revenue coming from hardware (iPhone is the largest contributor at 63%) and 14% from content and services (the App Store, Apple Pay, Apple Music and Apple TV). Apple has never chosen to develop a significant advertising revenue stream, yet as it controls the Safari browser and the iOS operating system, its technology underpins the digital advertising market on its devices worldwide. Consumer experience and a closed ecosystem have been key targets of the company, which has driven its success. Although it does not monetize data directly through advertising solutions, Apple is a powerful data engine and is understood to be building a comprehensive and powerful insight into individual customer behaviour, particularly around health. Its core commercial imperative in response to data-privacy concerns, however, was to make the Safari browser and the iOS operating system the leading consumer-focused and secure platform when it came to the use of data. Apple therefore was quick to follow the lead of Firefox Mozilla and restrict the use of third-party cookies on the Safari browser and implement new policies for the mobile identifier for advertisers on the iOS operating system. Apple was able to position itself as a safer platform than Google's Chrome browser and Android operating system.

By contrast, **Google** predominantly is an advertising business, with 70% of its global revenues coming from advertising on its own services (Search, YouTube, Maps and Gmail) and 14.6% from its third-party advertising technology business. Only 14.5% of revenues come from Google's other businesses, including Android, Chrome, Play, Home, Cloud and Fitbit. A major source of value from its Chrome browser and Android mobile operating system divisions is the data they help to collect from users that then support the core advertising businesses. When consumer privacy concerns reached crescendo levels (and consumer trust in Google's privacy practices was low) and Apple and Mozilla were differentiating heavily with their "more secure than Google" positioning, there was mounting pressure on Google to also restrict the use of third-party cookies on the Chrome browser. (It has yet to follow Apple's move in the mobile operating system space with any significant changes to the operation of the Android device ID.) This has caused a massive dilemma for Google, as the third-party cookie acts both as a primary source of data on consumers and underpins the third-party advertising network business that provides 15% of its global revenues. Google therefore has taken longer to work out how it can adapt its technology to meet consumers' expectations of data privacy while protecting and growing its advertising business.

Although **Microsoft** operates its own browser (Edge, formerly Internet Explorer) and formerly had its own mobile operating system (Windows Mobile), it largely has lost the Internet browser wars and, since 2019, uses Android as the operating system on all of its mobile and Surface Pro devices. Microsoft also has low dependence on advertising revenue streams, although it has sizeable businesses in Bing (number two in search advertising globally), LinkedIn and Xbox Gaming.

Amazon is a data-fuelled business with the richest and most powerful data source on what consumers actually buy. It is quietly building an on-site and audience network advertising business worth more than US$ 10 billion in the United States and the United Kingdom. This largely comprises on-site advertising with logged-in subscribers and has less dependence on third-party cookies to expand its audience. Watch this space.

Facebook is the company that is most affected by the moves of Apple and Google. It is almost purely an

advertising business (98.5% of global revenues), does not have its own browser or mobile operating system, and is completely dependent on the cookie and MAIDs for both collecting user data and monetizing through advertising on its own properties and its extended Facebook Audience Network (FAN), which represents third-party publishers as an SSP. FAN has roughly 5–15% share of mobile supply in the United Kingdom and generates approximately US$ 2 billion of annual revenue (3% of Facebook's total). Facebook was forced to close down the mobile web side of FAN in April 2021 due to increasing degradation of the cookie but as of January 2021 still operated its network for native mobile publishers (O'Reilly, 2020). The dependency on valuable iPhone customers in the lucrative United States market has Facebook in competition with Apple over the future of the mobile Internet (Hern, 2021) and Facebook revenues have suffered significantly as a result of the privacy-focused changes to the iOS14 operating system upgrade in 2021.

Google, Apple and Facebook understand that the data they collect are critical to their sustained competitive advantages. The driving forces for changes to the data-based technology landscape are a mix of consumer concern and regulatory action/threat, as well as the maturity of the digital media ecosystem, with technology power concentrated in a couple of Big Tech companies. These companies are having to tread a fine balance between maximizing their revenues and competitive positions and remaining in-step or ahead of consumer and regulation requirements.

Browser wars and the third-party cookie

Global market shares for mobile and desktop browser usage are estimated as follows:

- Chrome (62%) is by far the dominant browser player across desktop and mobile devices, followed by Firefox (13.5%) and Safari (9.7%); Firefox has an exceptionally high share in Germany (25%) compared to all other EU countries; and

- for mobile operating systems, browser global market shares are Android/Chrome 72.5% and iOS/Safari 26.9% (StatCounter, 2021).

Third-party cookies are the current principal means of achieving common identification of users on websites and are therefore a fundamental building block of the open-display advertising used by publishers. They enable the flow of data about users through the digital advertising ecosystem that is needed to target advertising and measure results. Cookie format and usage behaviours are determined by the browser technology provider (mainly Google (Chrome), Firefox and Apple (Safari)).

Targeting using first-party data and authenticated user data on publishers' own websites (such as Google's

portfolio or Facebook's mobile sites) does not require cross-site tracking and is unaffected by the demise of third-party cookies. Large incumbent platforms that provide leading services directly to consumers, such as Google and Facebook, are significantly less dependent on third-party cookies for delivery of high-performing targeted ads and continued advertising revenues than, for instance, small publishers with free-to-read content that does not require log in. Changes to the behaviour of third-party cookies, although an emotive topic for global data-privacy regulators, potentially present a fundamental challenge to the non-vertically integrated advertising business model used by newspapers and other online publishers.

In its market assessment report, the CMA in the United Kingdom observed that (CMA, 2020):

> measures which enhance an aspect of consumer privacy in the near term, may have dynamic effects which risk a negative impact on consumer welfare, for example a concentration of personal data amongst fewer providers, so impacting consumer choices and control in the longer term.

As a reaction to consumer privacy concerns, in advance of more intense regulatory scrutiny, and in attempts to differentiate against competing browsers on consumer data privacy and security to maintain usage penetration, the main Internet browser providers have restricted or degraded (or are planning to restrict or degrade) the use of third-party cookies for ad targeting and measurement purposes (Fig. 16).
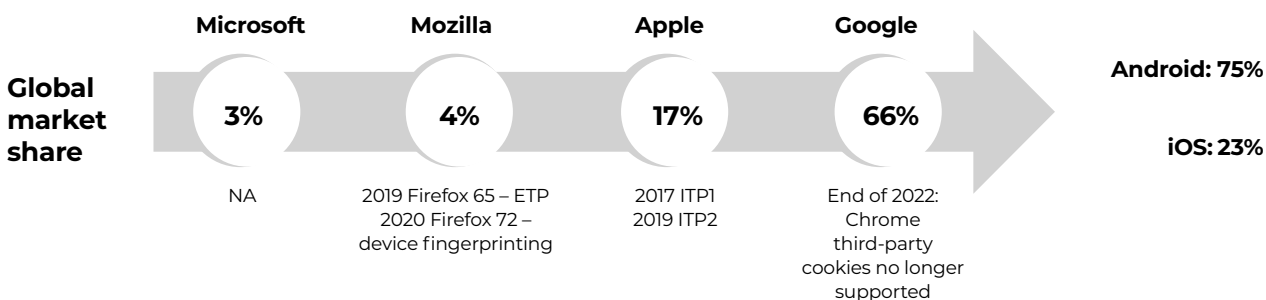
Mozilla Firefox has long made a strong play to position itself as providing strong privacy protections. Mozilla's anti-tracking policy enumerates its goals related to the uses it intends to block, only some of which currently it is able to do. The goal is also to eliminate the ability to perform covert or cross-site tracking; as a non-commercial entity, it has a strong motivation to lead as the developer of the most secure and privacy-safe web browser, being the first to restrict the use of the third-party cookie and device fingerprinting in 2018.

Apple Safari shares Mozilla's objective of eliminating user tracking across sites unless proper user opt-in consents are in place. Unconstrained by a significant advertising business model, Apple started to implement its Intelligent Tracking Prevention in 2017 and enhanced it in 2019.

Google Chrome discussed setting "Samesite" default in the Chrome browser in May 2019 to make all cookies first-party cookies by default, but this was never fully deployed on Chrome (Inventale, 2020). Under pressure from consumers and regulators to implement similar privacy controls, Google finally announced in January 2020 that it would no longer support third-party cookies, but with a two-year implementation period from the announcement to mid-2022. The reason for this long notice period, it was stated, was that Chrome's degradation of the cookie may have significant implications on the availability of data and the targeting ability of its competitors. Realistically, Google also needed to develop alternative strategies for harvesting and monetizing data first. Although there are some murmurs that the switch-off of third-party cookies on Chrome may be delayed until later in 2023, the industry is still planning to be ready by the end of 2022.

Although these developments seem positive under the guise of consumer privacy rights (after all, it was what the regulators and consumers asked for), ultimately the commercial impact of these moves is more detrimental to the third-party publishers who rely to a larger extent on these cookies and identifiers to support their fragile advertising businesses than to the major platforms themselves. There is an incentive for Google, Facebook and Apple to respond to data-protection regulation in a way that entrenches their own competitive advantage, including by denying third parties access to data that are necessary for targeting, attribution, verification and measurement, while preserving their right to use these data within their own walled gardens.

Fig. 16. Restrictions or changes to use of third-party cookies implemented by the main Internet browser providers[a]

	Microsoft	Mozilla	Apple	Google	
Global market share	**3%**	**4%**	**17%**	**66%**	**Android: 75%** **iOS: 23%**
	NA	2019 Firefox 65 – ETP 2020 Firefox 72 – device fingerprinting	2017 ITP1 2019 ITP2	End of 2022: Chrome third-party cookies no longer supported	

Others: Samsung 3.2%, Opera 2%.
NA: not applicable.
ETP: enhanced tracking protection.
ITP: intelligent tracking prevention.
[a] See detailed explanation in the text above.

Degradation of the third-party cookie

Ultimately, it should be assumed that the third-party cookie is going away – the common ID is no more. The industry will respond and develop new technologies and solutions, but the future of the digital advertising industry may be of a more chaotic and fragmented landscape. Media spend will need to be reallocated and measurement and targeting options will need to change or evolve. A significant rewiring of the digital media ecosystem is required.

The specific impacts of the degradation of the third-party cookie were posited in December 2020:

- cross-domain identity will not work – there will be no third-party cookies and there will be suppression of device fingerprinting (see section below);
- a large proportion of the open web will not be targeted or measured; without an ID, most of the baseline capabilities (such as people-based marketing, attribution, frequency capping and targeting) will be difficult/impossible;
- analysis of media effectiveness through last or multi-touch attribution will no longer be possible;
- standard frequency capping techniques will not work – this feature is based largely on third-party cookies so will no longer be available in its current form;
- third-party data currently being used for audience targeting will become unusable; data-management platforms will not be able to link IDs in the same way as they do today;
- application of first-party data to third-party audiences (audience extension) will not work;
- retargeting and most forms of dynamic creative targeting will become unworkable;
- measurement, not targeting, will be the major issue; without third-party cookies, it will be almost impossible to measure the overall effectiveness of online display advertising outside of the walled gardens; and
- cookie-based ad tech will shrink and consolidate as it becomes harder to measure or target at scale using third-party cookies.

The underlying technology that supported the large growth of digital advertising to a US$ 340 billion industry in less than 20 years and the birth of data-targeted programmatic media buying is about to change – and the digital media ecosystem needs to be rewired.

Device fingerprinting

In addition to the deprecation of support of third-party cookies, all major browsers have adopted a principle-based approach to prevent **device fingerprinting** and protect the privacy of users. Device fingerprinting (Peterson, 2019) has been used over the last few years as an alternative to the third-party cookie for identifying and tracking people on the Internet. Device fingerprinting

is a way to combine certain attributes of a device (the operating system version, the type and version of the web browser, the browser's language setting and the device IP address) to identify it as a unique device. Although not as accurate as a persistent third-party cookie, device fingerprinting can give a high probability of identifying and tracking the same device over time. It originally was developed for targeting between the mobile web and mobile app ecosystems on the same device and for powering programmes that make so-called identity graphs that try to link all users' IDs across devices (such as Adbrain, Drawbridge, Tapad, Crosswise and Novatiq).

The data usually used for device fingerprinting are passed regularly between the device and sites on the Internet to ensure that device and browser configurations are known and content delivery can be optimized. In 2020, Apple, Google and Mozilla announced that they will limit device fingerprinting. Apple Safari now obscures the data collected and combined for fingerprinting. Mozilla Firefox runs a blacklist of companies that are known to deploy device fingerprinting techniques and specifically prevents them from accessing the source data. Blacklisted companies include leading ad verification companies and DSPs. Google Chrome has announced, but not yet implemented, a volume cap on the amount of data a company can process, which limits their ability to run device fingerprinting algorithms.
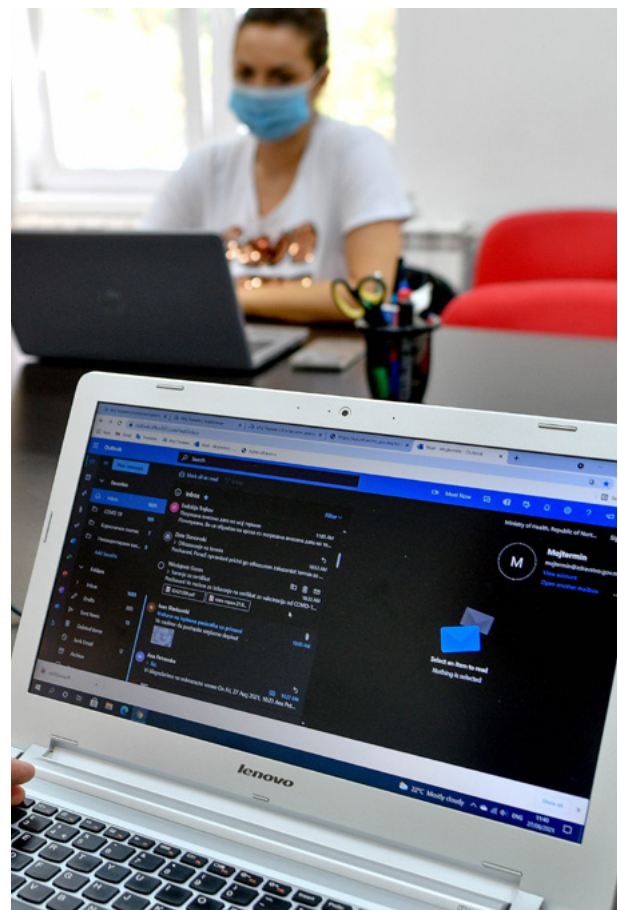
Aware that the removal of the third-party cookie would make the digital fingerprinting work-around much more prevalent, browser providers have made swift moves to close that loophole in advance.

Google Privacy Sandbox

As an advertising-focused company that derives enormous value from the data it collects and technology it sells to support the entire third-party advertising ecosystem on the Internet, Google faces a difficult conundrum with the changes to the use of the third-party cookie that have been forced by consumer, regulatory and competitive pressures. It naturally has been a follower (behind Mozilla and Apple) of these changes and has worked hard to construct solutions for data-targeting, measurement and attribution to maintain its position at the centre of the digital advertising ecosystem.

Its proposed solution is a series of initiatives labelled under the Google Privacy Sandbox banner. In Google's proposals, the demise of third-party cookies will be subject to the development of privacy-preserving and open-standard mechanisms to address the needs of users, publishers and advertisers. It is an evolving set of initiatives aimed at protecting user privacy while enabling advertisers to continue to take advantage of Google's information, insights and advertising technology platforms. It will allow websites and technology platforms to gather some information from the Chrome browser, but to cut the data flow off when it becomes too damaging. Privacy Sandbox proposals may still permit some third-party personalized advertising (interest-based advertising and remarketing), albeit at a less precise level of targeting and measurement.

The programme is still in its formative stages, but the idea is that cookies will be replaced with five application programme interfaces (APIs) (Joseph, 2020). Advertisers will use each API to receive aggregated data about specific advertising processes (targeting, conversion and attribution):

- the "conversion management" API determines measurement and attribution but does not count the number of ad impressions;
- the "aggregated reporting" API determines the number and frequency of unique views of an ad campaign across multiple domains;
- the "privacy budget" API restricts the level of data that can be extracted from the browser to prevent device fingerprinting;
- interest-based targeting through the Federated Learning of Cohorts (FLoC)[2] API uses machine learning to cluster users into similar behavioural audiences based on Chrome browsing history without disclosing PII; and
- the anti-fraud "trust" API is Google's alternative to the completely automated public Turing test to tell computers and humans apart (CAPTCHA) and will require a user to fill in a CAPTCHA-like programme once and then use so-called trust tokens to signal that the user is a human.

In addition, the Privacy Sandbox includes TURTLEDOVE

(an acronym for "two uncorrelated requests, then locally executed decision on victory"), a privacy-safe solution for consumer data that processes and stores user behaviours locally in their browsers through edge computing (versus the traditional approach of storing these data attributes on servers operated by SSPs, ad exchanges or publishers). This prevents these advertising technology servers from matching data sets to identify users. It is a technique for tracking user browser interests and allowing publishers to add their first-party audiences to cohorts when similar behaviours are identified. This means that all customer data stay on the user's device and is the gold standard for privacy compliance. The Privacy Sandbox also includes PIGIN ("private interest groups including noise"), which lets each Chrome browser track a set of interest groups to which a user is thought to belong.

Although Google's proposals are intended to be aligned with giving consumers more control over their data and with privacy regulations, they attempt to wire the digital media ecosystem around the functionality of the Chrome browser. The end goal appears to be to turn these APIs into open web standards that can also be adopted by Safari and Mozilla. Google is working with W3C on this goal. It is unclear whether Google's advertising technology platforms (Adwords and DV360) would have any preferential access to the data and
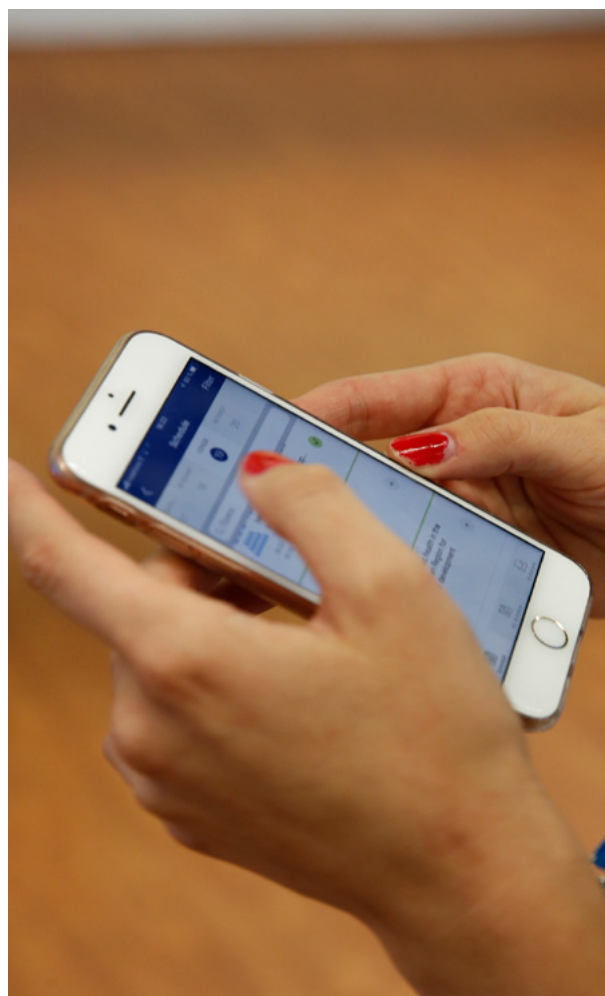
2   The FLoC proposes a new way for businesses to reach people with relevant content and ads by clustering large groups of people with similar interests.

insights from the Privacy Sandbox. There are recent concerns that Google's Privacy Sandbox/FLoC approach will not be sufficient to meet GDPR requirements in the United Kingdom and EU.

MAIDs

Advertising in mobile apps (the mobile app ecosystem) reached an estimated US$ 76 billion worldwide in 2020 and is forecast to grow to US$ 220 billion globally by 2025 (Shields, 2020). This is largely driven by Facebook (US$ 58 billion) and the Chinese ecosystem (Fig. 17) but includes an estimated US$ 10 billion earned from advertising in apps developed by independent developers outside China. Because of the dominance of Facebook in the format, less focus and scrutiny has been given historically to the app advertising supply ecosystem (led by Ironsource, Vungle, Applovin and Unity) and games developers.

Logically, the function of MAIDs is the same as the third-party browser cookie – to provide a persistent identifier that can link consumer behaviour between apps (and be refreshed/reset periodically). These were initially developed by Apple with the launch of the IDFA in 2012 (Bannerman, 2020) as a replacement for the permanent Universal Device ID to enable third-party advertising in the iOS mobile app ecosystem. This approach supported Apple's strategy of developing the app ecosystem by enabling an ad-funded business model for apps, where the switching costs and retention benefits of consumers sticking with the iPhone/Apple iOS over Android were highest, over the mobile web. MAIDs were then quickly adopted by Android to develop their mobile app advertising ecosystem. The presence of MAIDs also supported the mass-scale data-collection universe of both Apple (through the underlying iOS technology) and Facebook (through its Facebook Login Software Development Kit).

Initially, and throughout 2019, discussion about privacy regulation was largely focused on the desktop/mobile web cookie, probably because there was a high degree of familiarity and understanding about how cookies work and their widespread use across the Internet. In comparison, the industry lacked a deep understanding of the more closed Apple iOS ecosystem and the lower emphasis on the application side of the mobile advertising market with its more fragmented games and app publisher ecosystem and lower penetration of major brands (outside, of course, of Facebook). Given the challenges in dealing with the realities of how the Internet was using consumers' data, regulators may have been reluctant initially to challenge people's affection for smartphones, although this is clearly a key component of the long-term regulatory programme.

Fig. 17. Global in-app advertising market size projections
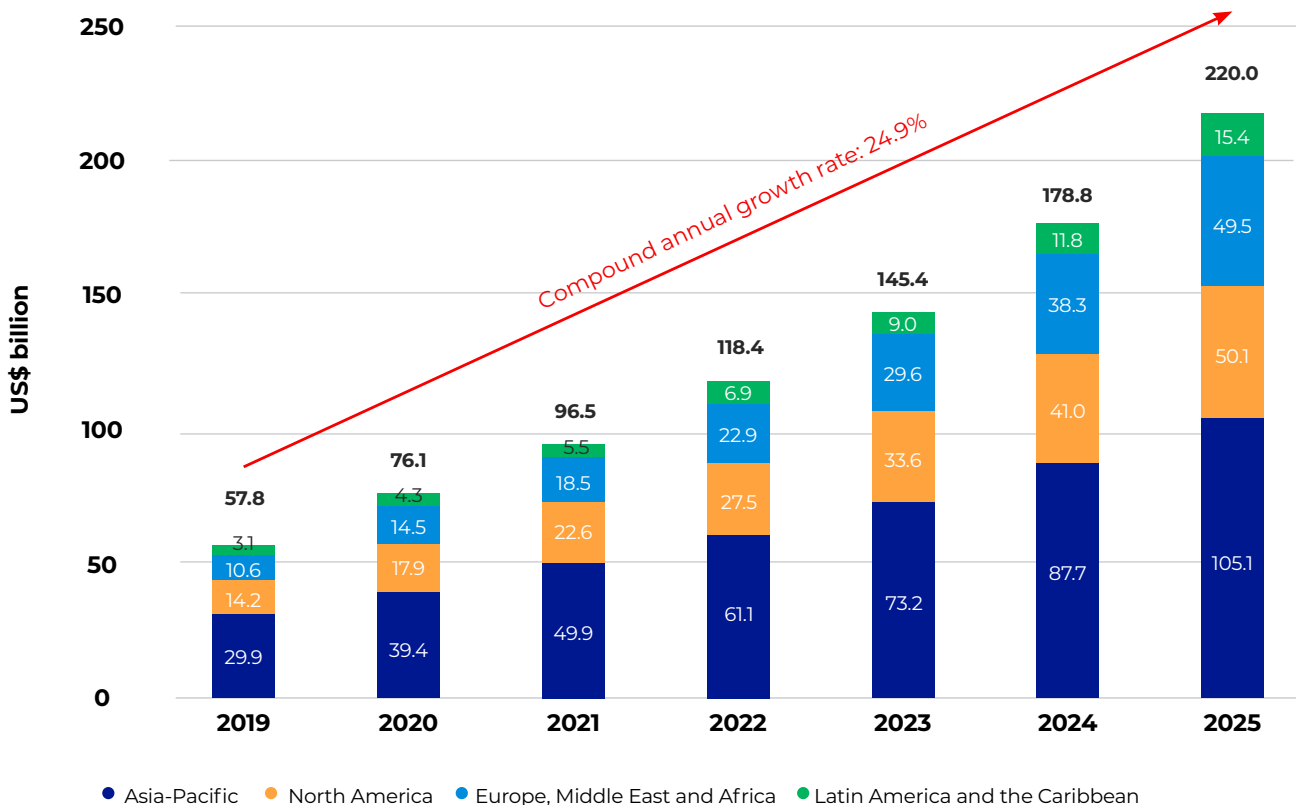
Source: author, informed by KBV Research (2019) and Rosenfelder (2020).

Inevitably and logically, Apple started to extend its privacy-first approach on Safari to the iOS mobile operating system with the release of iOS12 in November 2018 and iOS13 in September 2019. The first steps taken with iOS12 were largely to give users the ability to switch off default data-collection features, such as a re-emphasized "limit ad tracking", "disable all of Apple analytics", "disable location-based alerts, Apple ads and suggestions" and "disable stored frequent location history" (Manalo, 2018). All of these changes were opt-out decisions buried deep in the Settings section and, by early 2019, only 16% of iPhone users worldwide were limiting the use of their data. Although Apple was providing users with choice by keeping the default on and not making it an opt-in requirement, the company came under increased pressure for its data-harvesting practices.

By 2019, key features of iOS13 were:

- the launch of Apple Sign In so consumers can log in to apps using their Apple IDs, in addition to the Facebook, Google and Twitter log-in software development kits that are prevalent across the app ecosystem; with Apple Sign In, only the username and a temporary email address are passed over to the app developer, with no other customer data being provided;
- fine-tuned controls on the type of location data that can be collected by apps, with more granular visibility of the data being harvested by apps, and the app developer having to describe why those data are required; and
- blocking of the automatic right of apps to track location through Bluetooth and Wi-fi.

Wholesale use of the IDFA for ad tracking and targeting, however, was still permitted.

Apple launched iOS14 in September 2020 and announced that during 2021, the default availability of the IDFA effectively would be disabled and all apps that collect and share data with third parties for advertising-targeting purposes would be required to include a new data-consent window that prompts users to **opt in** to give consent for the use of their data. Without consent from the user, data matched to the IDFA cannot be used by the app developer, and it will be impossible to offer targeted and personalized advertising to the user.

Blocking third-party cookies and switching off the MAIDs (in the case of the "limit ad tracking" setting on iOS mobile devices) does not, however, affect the personalization of ads on the Facebook (or other first-party apps) app itself, regardless of browser or device. Facebook uses first-party cookies on its servers and the consumer is logged in to record their activity on Facebook's properties and can still select personalized ads. Blocking third-party cookies does, however, disrupt Facebook's ability to track and use consumers' off-Facebook activity for some websites (such as FAN websites and apps) to personalize ads. More importantly, iOS14 requires Facebook to get explicit upfront opt-in
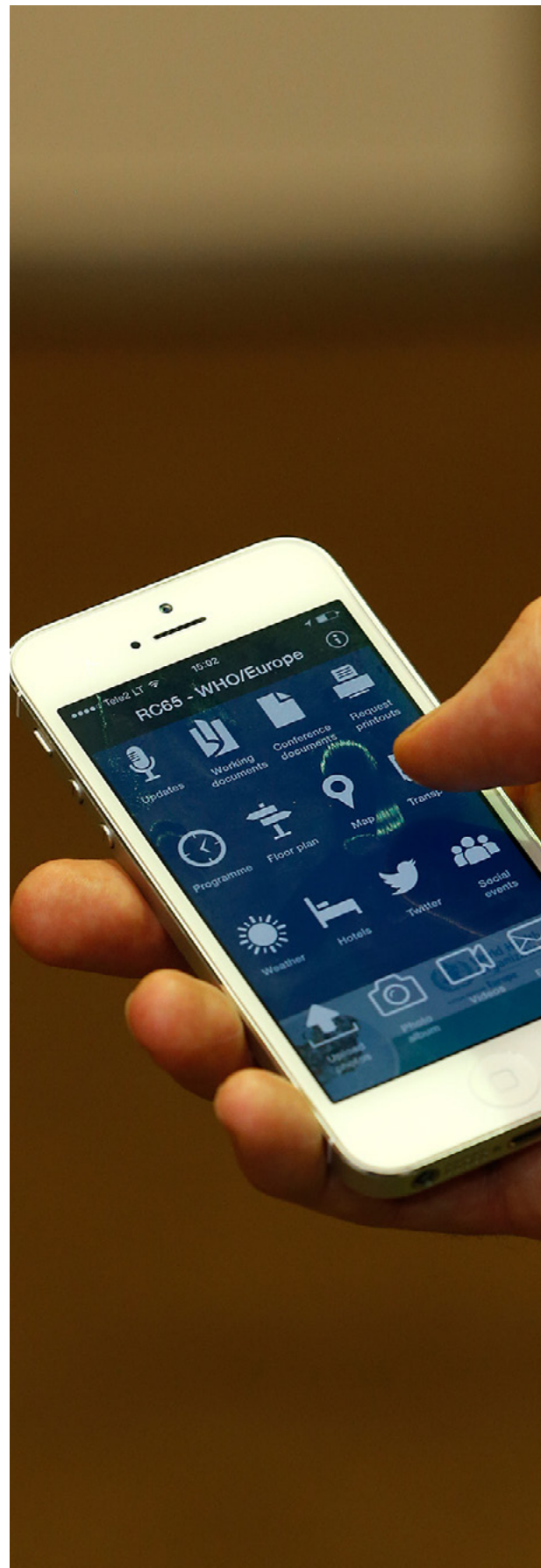
consent from its users to use data for ad targeting even on the Facebook app, which had a significant impact on Facebook's revenues in 2021 in its core and iOS-dependent markets in the United States and the United Kingdom. In October 2021, Facebook announced that it was stopping access to many more contentious data attributes for ad targeting on its network, including any references to causes, organizations or public figures that relate to health, race or ethnicity, political affiliation, religion or sexual orientation. Reportedly thousands of data attributes will no longer be available (Mudd, 2021). As late as November 2021, however, Facebook still faced criticism for the use of data to target advertising to teenagers and children (Lomas, 2021).

Facebook has criticized Apple's position on the IDFA, saying that advertising revenues for app developers would fall by 40–50% and openly warning all developers in the FAN to prepare for the disappearance of advertising revenues (Facebook Audience Network, 2020). This will equate with a loss of revenue of around US$ 5 billion annually to the independent app and games developer industry.

Like Google, Facebook will continue to develop workarounds. For many other websites, in practice, the Facebook pixel can be implemented using first-party cookies – a feature Facebook introduced following recent moves by browsers to block third-party cookies. Facebook explained this was to maintain choice for third parties to be able to share data with Facebook, similar data to which may otherwise not be available from browsers blocking third-party cookies.

For now, Google largely has been silent on its response and plans for the AAID, the Android equivalent of the IDFA. Android gives users the option to reset the AAID but not to turn it off completely. Google Play allows users to opt out of personalized ads (formerly known as interest-based ads). The fact that the AAID can only be reset but not turned off sparked a GDPR complaint in May 2020 by the European privacy advocacy group, noyb-eu, accusing Google of tracking Android users via the AAID without legally valid consent (Lomas, 2020). Although Android users are asked to consent to its terms of data usage and tracking in the Android device set-up journey, they are forced to accept that the AAID can be reset but not disabled and, under GDPR, consent must be given freely for it to be legally valid. The argument is that Google is only giving users the choice of "tracking" or "no tracking", with no genuine choice not to be tracked at all.

Third-party data ecosystem

Third-party data are data collected by an entity that does not have a direct relationship with the end-user (data subject) whose data are being collected. The combined impact of data-privacy regulation and the future degradation of the third-party cookie have been a so-called double whammy (a twofold setback) for the actors involved in the previously large and growing third-party data ecosystem.

In Europe, the **GDPR regulation has resulted in a clampdown on the third-party data ecosystem.** Oracle Data Cloud stopped selling its data-management platform services in Europe in September 2020 (AdExchanger, 2020) after facing a multi-billion-dollar class-action lawsuit regarding its former data-reselling platform BlueKai. Salesforce is included in the class-action lawsuit for practices related to its Krux DMP business (Page, 2020). These platforms were leaders in the third-party data-management platform space. DMP platforms such as Liveramp and Lotame nevertheless are still operating in Europe, pivoting their technology and business model to customer data platforms for first-party data onboarding.

This has also led to a **closing down of distributed data platforms for Google and Facebook.** Prior to consumer-privacy regulation, Facebook and Google extended the reach of their data monetization opportunity by offering audience data for use by third parties. In response to requirements for more complicated consents to pass data to third parties, these specific services have been discontinued.

◆ The business models and commercial objectives of the five major Big Tech companies in the United States (Apple, Google, Facebook, Amazon and Microsoft) have determined their reaction to pressures on the digital advertising ecosystems. Ultimately, the decisions they have made are shaping and continue to shape the structure of the industry going forward. While Google and Facebook have large revenues coming from advertising, Apple and Microsoft are not significantly affected by restricting the use of third-party cookies and have different incentives. Although the future stable structure of the ecosystem is still being formulated, significant change is inevitable.

08.

Wider digital advertising industry reaction

While the Big Tech companies will largely fend for themselves and play an active role in defining the future landscape, within the next 1–2 years all other independent publishers, brands and agencies will have to adapt quickly to the forthcoming changes in how the digital media ecosystem operates, as their day-to-day businesses depend on effective advertising. This chapter sets out 10 areas of likely response to the ecosystem disruption of removing the third-party cookie that will have an impact on the future digital media advertising landscape (Fig. 18).

Industry responses to ecosystem disruption

Response 1: shift to first-party data

First-party data are data that a company (typically brands and publishers) have collected with explicit opt-in permission from the consumer. The permissions determine the rights of the entity for use of the data.

Email login to publisher sites gives a persistent first-party ID through email; this can be mapped against first-party cookies and first-party data held on customers.

There has been a shift to **use of first-party data** as restrictions and complications relating to the collection, storage and activation of third-party audience data have grown. Sixty per cent of marketers in the United States said they expected to shift expenditure to first-party data, away from third-party data, from 2020 onwards (Winterberry Group, 2020). **Increased demand to scale first-party data** is driving enterprise markets and publishers. First-party identity graphs increasingly have been adopted, but first-party data and identity graphs are only going to be valuable if it is feasible to scale them up, and they are accurate.
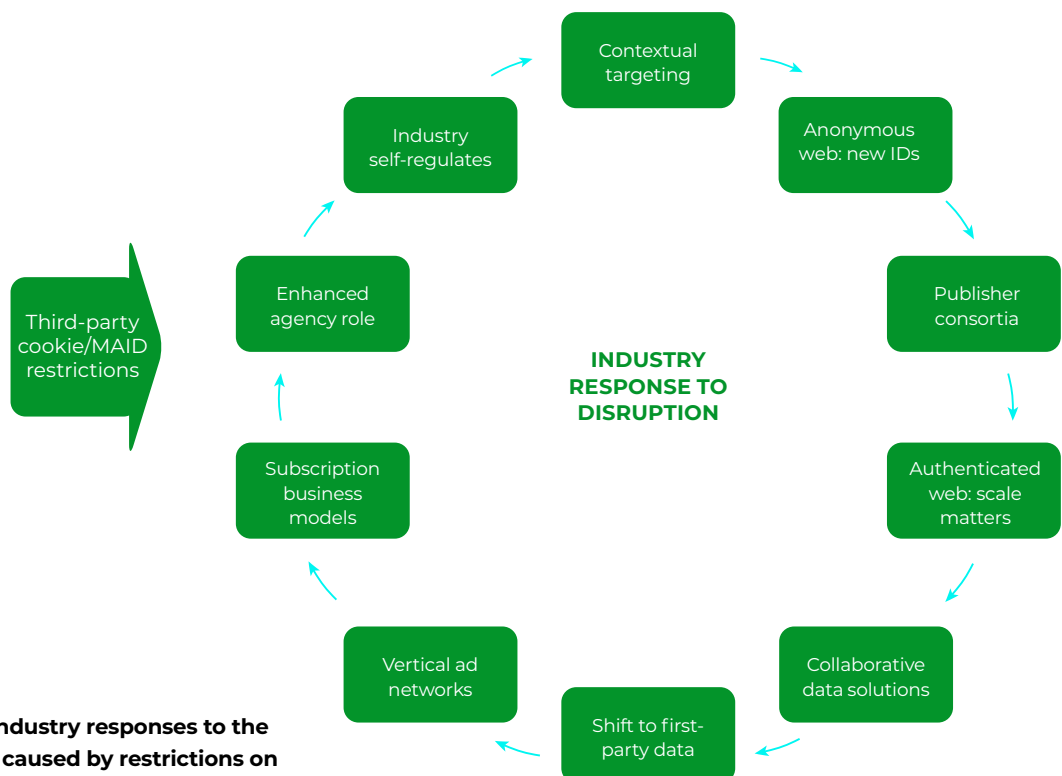

Fig. 18. Ten potential industry responses to the ecosystem disruption caused by restrictions on third-party cookies and MAIDs

Response 2: collaborative second-party data solutions, including data-sharing and so-called clean-room environments

Data-sharing models have evolved over last 30 years, from data cooperatives established from 1992 onwards to the creation of data marketplaces from 2010 and data exchanges since 2018. Clean-room technical data environments, including Infosum, Liveramp Safe Haven, Kalsgate, Transunion TrueAudience and Google AdsDataHub, are now creating the future of second-party data partnerships.

There has been a re-emergence of second-party data – in other words, data that are shared in a dedicated environment with a clearly defined set of permissions and rights sent between each of the parties, frequently with a third-party technology provider managing the environment.

Clean rooms and associated identity-/data-matching techniques are using the ability to link data by pseudonymization while maintaining the security and privacy of the data from both partners. First-party data owners have the ability to activate their data outside of their own platform network environment without sharing the underlying data or breaching any consumer privacy requirements for complicated consent chains. Differential privacy techniques and guidelines prevent the re-identification of individual PII.

In 2020, 62% of marketers in the United States and 52% in the United Kingdom stated that they were using collaborative clean-room data-sharing environments (Biegel et al., 2020).

Response 3: authenticated web coalitions

The degradation of third-party cookies will change fundamentally the wiring that underpins the Internet and generally will stop practices that have allowed the misuse of customer data without consent for the last 10 years or more. Large-scale publishers who have enough users, enough content, enough data and enough demand from users who are willing to log in to use services, however, will be less affected because they do not need to rely as much on third-party cookies to operate.

In the future, the Internet may be characterized as two separate parts – the so-called authenticated web and the anonymous web. In the authenticated web, people are logged in and fully deterministically identified to their publisher or service provider. In the anonymous web (secondary users on larger sites and most users on smaller sites and services), users are not logged in and will not be able to be identified or targeted by personalized advertising (Fig. 19).

Under this scenario, the main platforms' walled gardens (including Facebook, Google, Amazon, Microsoft and Snap) deliver scale and performance through their logged-in consumer base. The other 20% of advertising on the Internet, which today is outside of these walled gardens, will have to find ways to monetize their content. This could include new collaboration models to build scale, new unified ID identifiers, new ways to link users across logged-in domains and new privacy-compliant data-sharing models attaching second- and third-party data to unified IDs.

Fig. 19. Scenario for the future of the Internet – the authenticated web and anonymous web co-exist
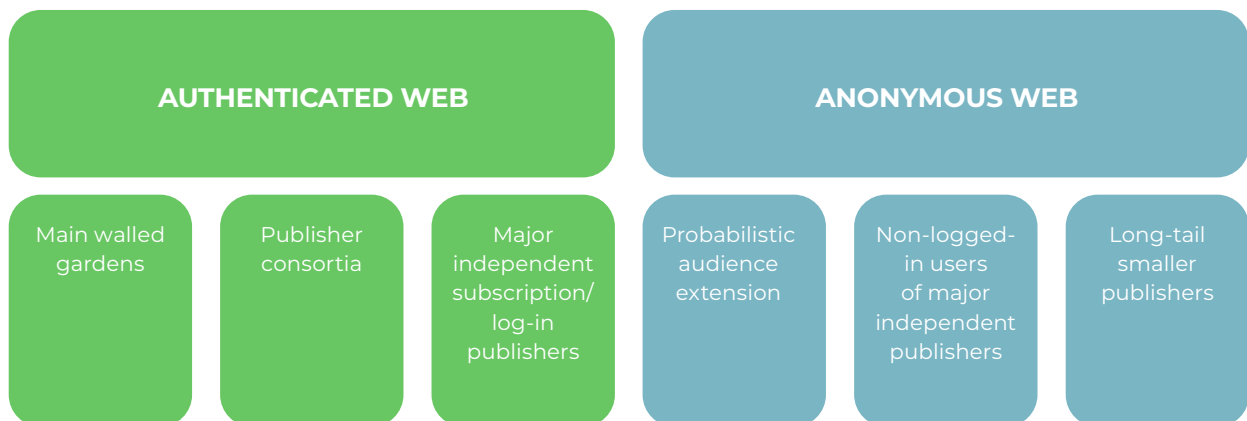
Users are identified by log-in ID matched to email/mobile ID, consent for using first-party data and identity linkages for second- and third-party data.

Users are not logged in and can no longer be identified by third-party cookies. Publishers who have some signed-in users can increase their reach by using probabilistic modelling techniques to identify "lookalike" audience segments.

Response 4: publisher consortia to build scale on authenticated unified ID users

Cooperation is critical to beating the scale of the walled gardens, as publishers group together to generate scale or work with media owners and advertisers participating in ID-sharing technologies.

Matched first-party data provide the most robust way of identifying consumers and creating addressable audiences, because there is a unique, persistent identifier (such as an email address or phone number) that exists between two (or more) websites. This enables, for example, an online retailer to retarget someone who has abandoned an online shopping basket without completing a purchase on another website if the consumer logs into both sites using the same email address. Additionally, it enables publishers and advertisers to know how ads perform in terms of yield and return on investment, creating a feedback loop for optimization.

Consortia that have emerged include the following.

Ozone (United Kingdom): this initially helped publishers by coordinating integrations with the unified IDs being promoted by Prebid.org. It has since graduated to a scaled managed service ad network model. These evolved cooperatives are intended to drive significant additional brand spend, helping publishers stave off drops in cookie-based revenue. Ozone can reach an audience of over 44.5 million in the United Kingdom.[3]

Gravity Alliance (France): this initiative, which brings together around 15 publishers to pool audience data, was reported to reach 44% of the French population every day by June 2017, a figure that was predicted to reach 50% by autumn 2017, according to alliance member Les Echos. Google reportedly has a market reach of 60% and Facebook has 70% in France, although eMarketer puts Facebook's reach at around the 40% mark. Members of the group include: national media publishers Lagardère, Les Echos Group and L'Équipe; classifieds publisher SoLocal (formerly PagesJaunes); broadcasters SFR and M6; magazine publishers Prisma Media and Condé Nast; several regional newspapers; and retailer FNAC Darty's ecommerce sites.

NLProfiel (the Netherlands): three leading publishers in the Netherlands – Sanoma Media, Telegraaf Media Groep and de Persgroep – signed an agreement to use a common DMP for their joint data-alliance initiative NLProfiel.

Media Impact + Ads Alliance: Germany's biggest publishing houses, including Axel Springer, Funke Mediengruppe, RTL Groupe and Gruner+Jahr, have come together to form an advertising alliance.

---
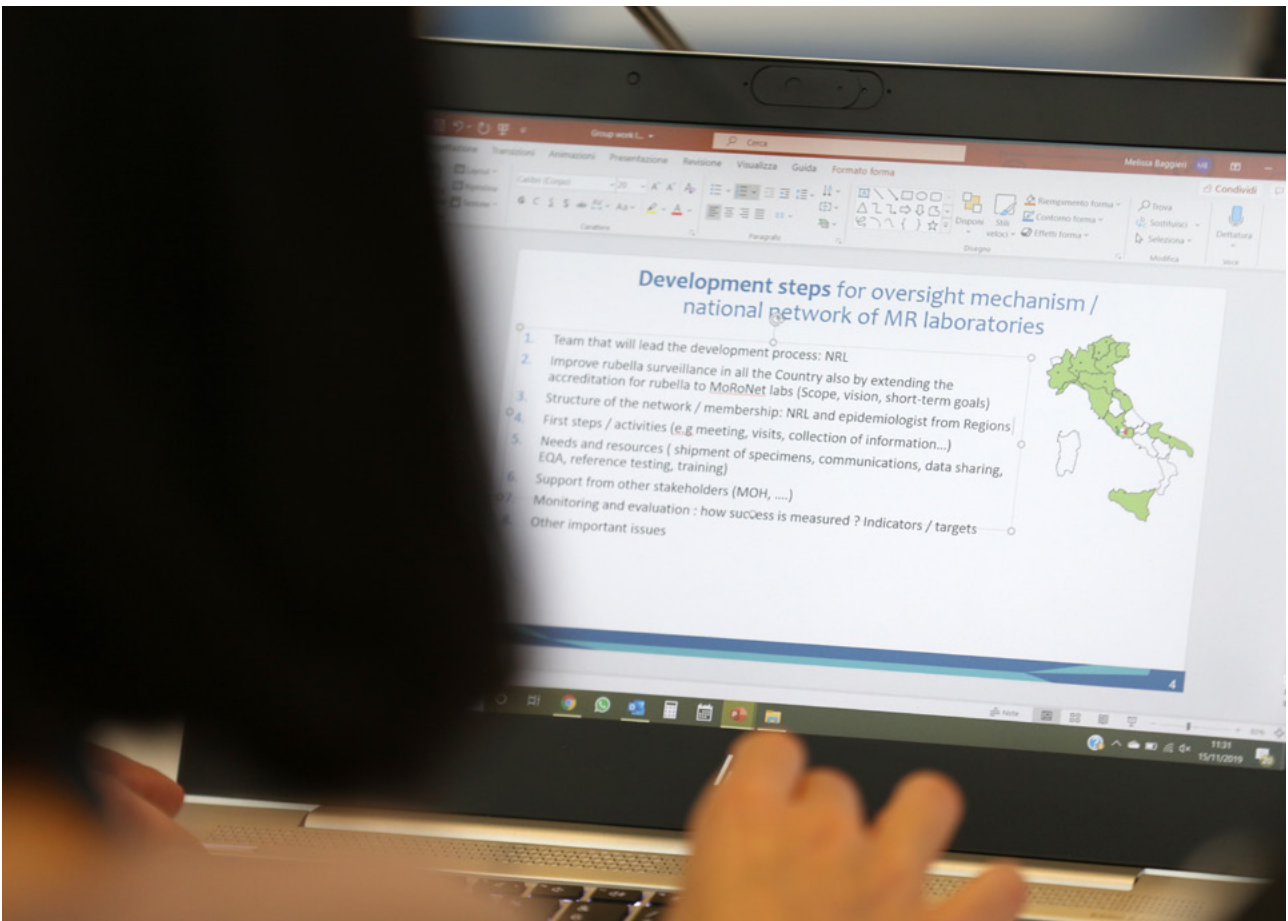
3   Other previous United Kingdom publisher consortia failed. In 2015, the United Kingdom-based publisher collective Pangaea, formed by The Guardian, FT, CNN International, The Economist and Reuters, was soon followed by the announcement of the AOP-led equivalent Symmachia, representing Dennis Publishing, Telegraph Media Group and Time Inc.

Publisher login unions have started to form in Belgium, Estonia, Finland, France, Latvia, Lithuania, Germany, Portugal, Romania and Switzerland.

Response 5: anonymous web impact and new ID solutions

However large the authenticated web becomes, the breadth and diversity of content on the Internet is likely to continue and many smaller publishers will have to operate outside of the large walled gardens and publisher consortia. The anonymous web will remain hugely important for the advertising ecosystem, as it still represents the big opportunity in the decade ahead. The third-party (outside of the walled gardens) authenticated web will remain large but will be restricted to users actively logging into publisher websites. The scale simply will not be sufficient to compete with Google, Facebook, Amazon, TikTok, Twitter and Snap.

Estimates suggest that sites that cannot offer programmatic personalized advertising as a main revenue stream are likely to lose at least 70% of their advertising revenue potential by being able only to offer untargeted ads. Even with access to programmatic buying systems and ad technology from SSPs, many sites wil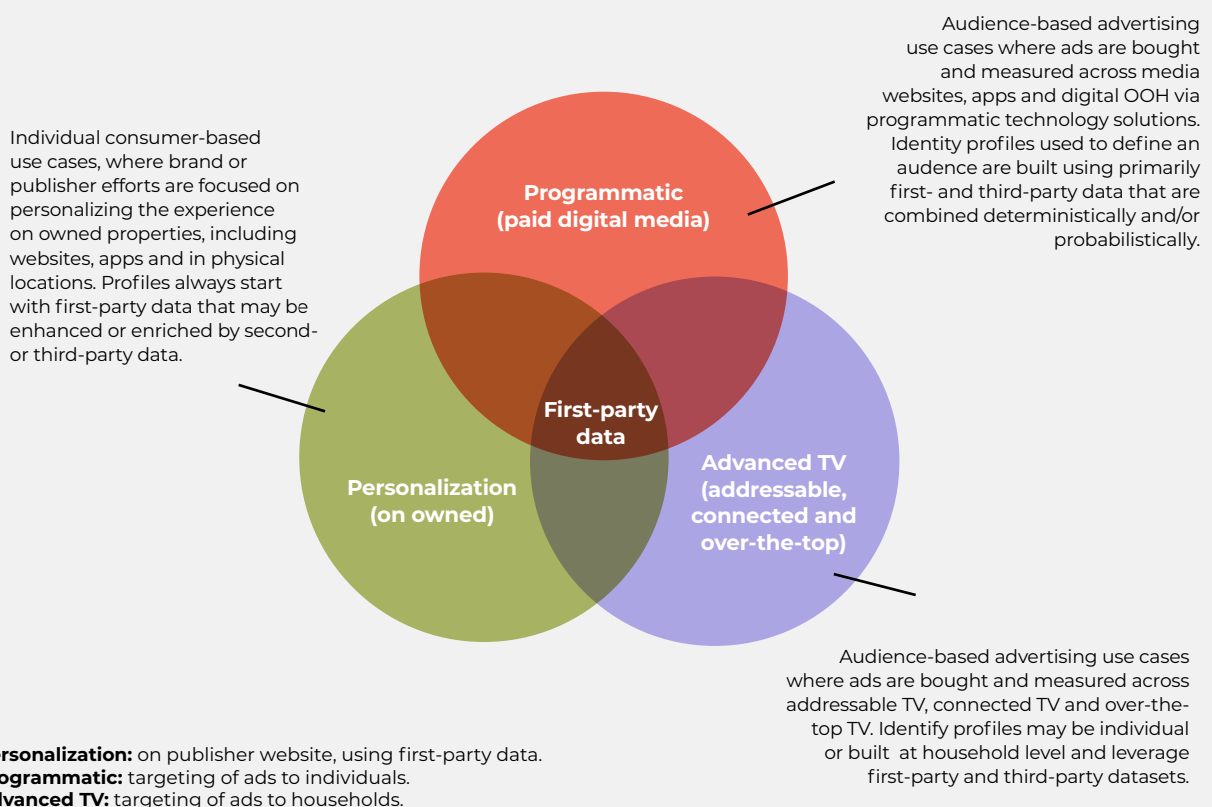l find the cost of selling advertising without data-targeting too high to be viable in the future. For these publishers, finding an alternative way of delivering data-enhanced targeting without a third-party cookie will be a matter of survival.

The enforcement of privacy regulation (GDPR/CCPA) and the degradation of third-party cookies are forcing innovations among data and technology companies to replace cookie-centric models with privacy-compliant approaches.

The need for new identity-resolution solutions is also being driven by the increase in the number of devices at individual and household levels and an immediate recognition of the importance of identity to the advertising industry for targeting, measurement and attribution. Because of the earlier adoption of GDPR in the EU, Europe is serving as the testing ground for new identity technologies in the programmatic digital advertising space.

In addition to the authenticated and anonymous web, a third use of identity is driving the future of the advertising industry: the emerging importance of over-the-top television and connected television will lead to a blended approach to identity that mixes individual and household solutions (Fig. 20).

Fig. 20. Three different advertising ecosystems – personalization, programmatic and addressable TV

Individual consumer-based use cases, where brand or publisher efforts are focused on personalizing the experience on owned properties, including websites, apps and in physical locations. Profiles always start with first-party data that may be enhanced or enriched by second- or third-party data.

Audience-based advertising use cases where ads are bought and measured across media websites, apps and digital OOH via programmatic technology solutions. Identity profiles used to define an audence are built using primarily first- and third-party data that are combined deterministically and/or probabilistically.

Programmatic (paid digital media)

First-party data

Personalization (on owned)

Advanced TV (addressable, connected and over-the-top)

Audience-based advertising use cases where ads are bought and measured across addressable TV, connected TV and over-the-top TV. Identify profiles may be individual or built at household level and leverage first-party and third-party datasets.

Personalization: on publisher website, using first-party data.
Programmatic: targeting of ads to individuals.
Advanced TV: targeting of ads to households.

Source: Biegel et al. (2020). Reproduced by permission of the Winterberry Group (https://www.winterberrygroup.com/).

Biegel et al. (2020) have identified five classes of new identity solutions being created in the market:

1. proprietary ID based on first-party data, where a brand or media owner establishes a unique ID for use on their own properties or for matching with partners in a collaborative clean-room environment (examples include Zeotap);

2. common ID based on a third-party data match to a PII-based third-party data-reference set to achieve sales across media providers with deterministic scale and probabilistic audience extension (examples include Tradedesk Unified ID/Prebid.ord and Liveramp Identity Link);

3. a common third-party identity token used to facilitate enhanced recognition across the programmatic trading ecosystem (such as ID5 and Skyrise);

4. a second-party data environment based on clean-room environments with anonymous ID linking (such as Infosum and Liveramp); and

5. a household ID based on IP address and geographical match (deterministic and probabilistic).

Given the advanced pressures of GDPR, much of the early innovation on alternative ID solutions is coming from European technology companies. The number of new approaches to identifying post-third-party cookies is increasing, but the industry is not yet at the stage where standardized solutions have been established.

Companies like Permutive are using artificial intelligence/machine learning techniques to enable publishers to extend their logged-in first-party audiences with probabilistic lookalikes on the anonymous web.

There is no clear preference for one standard approach to identity over the others, and it is likely that the ecosystem will be defined by a blended approach to identity going forward, without the ubiquity and consistency of the third-party cookie and the IDFA/AAID. No one solution will rule. Measurement and attribution therefore will remain more challenging and multi-media modelling approaches will become more valuable and widespread.

Response 6: move to contextual targeting

Contextual targeting (the selling of audiences defined by the content or publication they are consuming) is how advertising targeting first started. With the advent of programmatic data-driven targeting of advertising based on the cookie and MAID in the last 10 years, it has become a secondary approach. Degradation of the third-party cookie means contextual targeting is again becoming a more attractive and viable solution for brands and publishers.

Two modern twists on audience-based contextual targeting are:

- keyword contextual targeting, where keywords on a page of content are matched to determine suitability and likely effectiveness for ad placement; and

- semantic contextual targeting, which uses artificial intelligence/machine learning techniques (or augmented targeting) to understand the overall meaning of a page and likely target audience.

The degradation of the third-party cookie and MAIDs has left many smaller publishers without a viable identity solution for the future, so contextual targeting is set to become a more important alternative to personalized targeting of advertising.

Response 7: re-emergence of vertical ad networks

An extension of the themes of data collaborations and contextual targeting is the re-emergence of the **vertical ad networks (VANs)** model. VANs target specific audiences aggregated across different publishers. New, independent businesses built around vertical audiences are likely to emerge (O'Kane, 2020). In a world without the third-party cookie, agencies can still find and buy ad space via the walled gardens and ID-based programmatic advertising, but there is going to be a wave of new VAN solutions coming to the market as buyers go hunting for hard-to-find premium audiences. The idea of the VAN is a simple one – combining advertising inventory from different publishers using a mix of first-party cookies, contextual targeting and third-party technology. This effect will cause a fragmentation of media spend across multiple sales points, versus the centralized DSPs in programmatic trading. Smart media buyers will seek out audience verticals, building businesses on strong publisher relationships, vertical-audience specialism and managed-service expertise.

Examples of child-safe vertical ad networks/advertising platforms include:

- Superawesome (acquired by Epic Games in 2020)
- Kidoz (acquired by Shoal Games in 2019)
- Spinmaster Toca Boca
- Disney+
- LEGO
- Mattel
- YouTube Kids.

Response 8: move to subscription, in-app purchase business models and direct-to-customer

As advertising-based business models become harder to execute (especially for smaller publishers) and consumer and regulator concerns about data privacy and data usage strengthen, some publishers may look to adopt more subscription-based and in-app purchase-based business models. If content is compelling enough, publishers often can achieve similar levels of revenues to advertising-funded services without the complications that data privacy and the advertising ecosystem present.

Netflix, for instance, achieves a revenue of US$ 30 per user on average through its subscription model versus US$ 50 for Facebook through its advertising model.

Other large-scale publishers who have successfully executed a pure subscription or a hybrid subscription/advertising business model include Disney+, Netflix, Amazon Prime, Apple TV (universe of Apple), the Telegraph and the Wall Street Journal.

Smaller games publishers should be able to move to paid downloads and in-app game purchases if their advertising revenues collapse. The cost of the content, however, will migrate to end users, who ultimately may be cash-constrained young people, thereby restraining market opportunities and accessibility. Brands may look for more opportunities in sponsored content or apps and to develop direct-to-customer business models in which they can have a direct relationship with the customer and build up their first-party data assets.

Response 9: enhanced role for agencies

The role of agencies and other specialists is likely to increase as audiences and technology become more fragmented at global and regional levels and as more innovative approaches are needed to find audiences through contextual and data-targeting means. Fewer brands will look to manage their digital media ad buying in-house as the simplicity of programmatic buying gets fragmented. The alternative of buying all media through the walled gardens is not seen as a desirable outcome for brands, agencies or publishers, and independent content on the Internet needs to be funded by a vibrant advertising ecosystem.

Response 10: lobbying for self-regulation

The fundamental changes facing the advertising ecosystem largely have been triggered by consumer and regulatory concerns about the power of the walled gardens and how data have been (mis)used across the advertising supply chain. There are wide industry concerns that it will take some time for regulators to understand the advertising technology systems in sufficient detail to formulate effective regulation that has the desired outcomes. The alternative to regulation is the adoption of more transparent and consumer-focused practices by the key industry players. The main walled gardens are moving their policies and processes in the right direction. An example of wider industry organization on pre-regulation is the Partnership for Responsible Addressable Media that was launched in August 2020. Its stated principles can be summarized as: privacy is important; a healthy open Internet is better for society; all marketers and publishers should have equal access to the mechanism for operating an addressable Internet; and everyone must abide by applicable laws.

◆ The wider digital advertising industry has had to react to the changes in the digital marketing ecosystem. This can be seen, for example, in the shift to the use of first-party data, sharing data by partnering-up of brands or publishers, and the division of the Internet into an authenticated web and an anonymous web. The enforcement of privacy regulation (GDPR/CCPA) and the degradation of third-party cookies are forcing innovations among data and technology companies to replace cookie-centric models with privacy-compliant approaches. New identification solutions are proprietary ID based on first-party data, common ID based on a third-party data match to a PII, a common identity token, second-party data environment with anonymous ID linking or a household ID based on IP address and geographical match. Moving to contextual targeting can be a reaction to the new restrictions, and industry responses to the new data-protection measures include the re-emergence of the VANs model, in-app purchase solutions and an agency-enhanced role in a fragmented ecosystem. The industry is still undergoing significant disruption and transformation and its future structure is still being determined.

09.

Looking forward – how it all plays out

As a proxy for the health of the global advertising economy, advertising spend in the United States is expected to have bounced back in 2021 to near 2019 levels of spend (US$ 375 billion + 10.0% year-on-year), but with significant shifts to digital media (+17.8%) versus offline (+2.3%), driven by digital video (+40.0%), influencer (+32.4%), digital OOH (+19.4%), display (+19.1%), digital audio (+17.4%), paid social (+15.5%) and search (+14.1%). Although still growing, spend is shifting away from the traditional search-and-pay social heartlands of Google and Facebook, although these companies continue to innovate in new formats to continue to capture overall advertising revenue share. The same trends are expected in other major digital media markets worldwide.

Brands will leverage first-party identity solutions for personalization while utilizing third-party identifiers to increase recognition reach and to be able to continue to use targeting within the broader programmatic ecosystem. Expanded development and use of first-party identity graphs initially by larger brands and marketers can be expected, with rapid adoption across the mid-market between 2021 and 2023. Small and medium enterprises and small business advertisers will lose out more without access to these new techniques and tools. Within these first-party identity graphs, privacy-compliant third-party data will continue to be used to enhance and/or enrich first-party profiles.

For publishers, the consensus view clearly indicates that the centre of the new programmatic ecosystem will also be based on first-party cookies and other first-party data and the most profitable future is in the authenticated web. Publishers, however, will leverage the broadest set of identity solutions to achieve both scale and reach while maintaining the desired level of accuracy. Contextual targeting and probabilistic audience extension will enable publishers to increase reach beyond their logged-in user bases, and major publishers will work together in consortia to try to achieve network-level scale in authenticated users. Hybrid subscription and advertising funded models will be more widely adopted.

In relation to major global technology providers (often based in the United States), Europe has been a complicated place to operate and roll-out across markets for ad tech from the United States for many years. Given the dynamics in the industry, it is increasingly difficult and expensive for American ad tech companies to flourish. Europe is a fragmented web of markets and employment laws. This situation has not been helped by the emergence of stringent privacy laws and the ever-present threat of fines from European data regulators. Europe will not be a happy hunting ground for ad tech from the United States, which ultimately could be good news for European-based companies. Many of these companies may be acquired as strategic global players look to maintain and grow their ad businesses in Europe.

Despite their clear capabilities, data and scale advantages over other publishers, Google, Amazon, Facebook and Apple will not continue to grow share until they get 100% of the market because:

- agencies cannot be seen by clients to be giving all of their media spend to the walled gardens – this would be tantamount to commercial suicide, because the agencies' clients may no longer see any need to use or pay agencies when they could go directly to the platforms of the walled gardens;

- people consume much of their digital media outside Google, Amazon and Facebook, and ultimately, money follows eyeballs;

- the walled gardens are challenged by ID and cookie deprecation, as ultimately it restricts them to their own user-generated content services and prevents them from expanding their advertising networks and data assets onto third-party sites; and

- improvements in contextual targeting and identity-resolution techniques often work just as well as behavioural targeting based on programmatic data.

◆ Advertising spend is bouncing back after the initial impact of the COVID-19 pandemic, but with significant shift changes towards digital media. Going forward, brands, publishers and technology providers continue to face challenges and will be required to make significant changes to deliver the most effective brand campaigns at scale to consumers.

10.

Implications for the WHO European Region and health regulators

The previous chapters have outlined the complex and constantly evolving system for buying, selling and delivering digital advertising. Since 2018, when the WHO Regional Office for Europe published its report on *Monitoring and restricting digital marketing of unhealthy products to children and adolescents* and presented the CLICK monitoring tool (WHO Regional Office for Europe, 2019), the digital ecosystem has undergone significant change. For policy-makers and health regulators concerned about children's exposure to digital advertising for unhealthy products, it is important to understand the digital ecosystem and the dramatic shifts that are occurring.

The COVID-19 pandemic has increased government focus on health and the obesity crisis, especially in light of evidence that failure to address the obesity crisis has exacerbated the impact of the pandemic. Two areas of government policy – health (specifically tackling overweight and obesity) and regulation of Big Tech – are aligning. This alignment of policy priorities presents an opportunity, as seen in the United Kingdom, for example, with a decision in November 2020 to implement in 2021 a total ban on online advertising of HFSS foods (Department for Digital, Culture, Media and Sport and Department of Health and Social Care, 2021b).

The key aspects of the recent changes can be summarized as follows:

- digital advertising has now further consolidated onto the major technology platforms (with Google, Facebook, Amazon, Microsoft and Apple accounting for between 60% and 80% of digital media spending in key global markets);

- there is a continued lack of accurate and verified age data that would allow children to be identified as children; and

- personalized targeting across the open anonymous web will not continue; ultimately, there may be less advertising funding content for children and adolescents, and it will be easier to control advertising content in more focused children's apps and social and video channels, although advertising in long-tail publishers will no longer be able to be targeted to adults, so children may see more advertising.

There are several important implications of these recent and ongoing changes for policy-makers and regulators.

- To be effective, WHO and national policy-makers should address policies towards the main technology

platforms directly to influence changes to the rules for advertising to children for HFSS foods.

- Given the spectrum of regulatory and political pressures that these businesses are facing, the timing is good for more concentrated and direct discussions on future policies with the platforms. Without active participation from Facebook and Google in the programmes, coordinated at regional and global levels, national programmes are likely to fail to have significant impact on digital advertising to minors.

- On the positive side, changing policies within the walled gardens (such as Google and Facebook) is theoretically and technically easier than changing behaviour across the whole open ecosystem. The new environment simplifies the process of data collection for national-level market mapping – the open ecosystem has become less relevant and national publishers are easier to identify at source. This also facilitates discussions among global research partners.

- There will, however, continue to be a conflict between the platforms' commercial objectives and momentum around restricting advertisers on the platforms. Blanket bans on HFSS advertising are likely to be resisted by brands, agencies, global platforms and national publishers, and operational implementation will be complex.

- A coordinated WHO approach in national and EU-wide regulatory debate will be most impactful. A focus on publisher consortia and the main walled gardens (Google, Facebook, TikTok and Snap) is recommended, with increased attention on identifying and authenticating audiences (by age) by child-focused content VANs (such as SuperAwesome/Epic). Focusing on the platforms with the largest media usage by children will have more immediate impact than changing the rules of the whole programmatic advertising ecosystem.

Understanding the constantly evolving digital marketing ecosystem remains essential for health policy-makers and regulators intent on reducing children's exposure to marketing of HFSS foods. The recent and ongoing significant changes require a shift in approach from policy-makers, and it will be more important than ever to initiate meaningful dialogue with the major technology platforms to explore the possibilities for harnessing the power of technology to protect children from marketing of unhealthy products.

References[4]

AdExchanger (2020). Oracle to stop selling third-party data in Europe; InMarket scoops up location company NinthDecimal. In: AdExchanger [website]. Rockville (MA): Access Intelligence LLC (https://www.adexchanger.com/ad-exchange-news/thursday-09102020/).

Asen E (2021). What European OECD countries are doing about digital services taxes. In: Tax Foundation [website]. Washington (DC): Tax Foundation (https://taxfoundation.org/digital-tax-europe-2020/).

Bannerman A (2020). A history of IDFA – Apple's privacy u-turn. In: Permutive [website]. London: Permutive (https://permutive.com/2020/09/03/a-history-of-idfa-apples-privacy-u-turn/).

Biegel B (2020). The outlook for data-driven advertising and marketing 2020. New York (NY): Winterberry Group (https://dmcny.org/wp-content/uploads/2020/01/Winterberry-Group-The-Outlook-for-Data-Driven-Marketing-2020-1.16.2020.pdf).

Biegel B, Ping C, Harrison M (2020). Identity outlook 2020: the evolution of identity on a privacy-first, post-cookie world. New York (NY): Winterberry Group (https://www.merkleinc.com/identity-outlook-2020-evolution-identity-privacy-first-post-cookie-world-addendum/thankyou).

Boyland E, Nolan S, Kelly B, Tudur-Smith C, Jones A, Halford JC et al. (2016). Advertising as a cue to consume: a systematic review and meta-analysis of the effects of acute exposure to unhealthy food and nonalcoholic beverage advertising on intake in children and adults. Am J Clin Nutr. 103(2):519–33. doi:10.3945/ajcn.115.120022.

Cairns G, Angus K, Hastings G, World Health Organization (2009). The extent, nature and effects of food promotion to children: a review of the evidence to December 2008. Geneva: World Health Organization (https://apps.who.int/iris/handle/10665/44237).

CMA (2020). Online platforms and digital advertising market study. London: Competition and Markets Authority (https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study).

CMS (2021). GDPR enforcement tracker. In: CMS [website]. London: CMS Legal (https://www.enforcementtracker.com/).

Comforte (2021). 17 countries with GDPR-like data privacy laws [blog]. In: Comforte [website]. Wiesbaden: Comforte AG (https://insights.comforte.com/12-countries-with-gdpr-like-data-privacy-laws).

Confessore N (2018). Cambridge Analytica and Facebook: the scandal and the fallout so far. The New York Times. 4 April 2018 (https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html).

de Poulpiquet P (2017). What is a walled garden? And why it is the strategy of Google, Facebook and Amazon Ads platform? In: mediarithmics_what is? [website]. San Francisco (CA): Medium (https://medium.com/mediarithmics-what-is/what-is-a-walled-garden-and-why-it-is-the-strategy-of-google-facebook-and-amazon-ads-platform-296ddeb784b1).

Department for Digital, Culture, Media and Sport, Department of Health and Social Care (2021a). Introducing a total online advertising restriction for products high in fat, sugar and salt (HFSS). London: Department for Digital, Culture, Media and Sport, Department of Health and Social Care (https://www.gov.uk/government/consultations/total-restriction-of-online-advertising-for-products-high-in-fat-sugar-and-salt-hfss/introducing-a-total-online-advertising-restriction-for-products-high-in-fat-sugar-and-salt-hfss).

Department for Digital, Culture, Media and Sport, Department of Health and Social Care (2021b). Introducing further advertising restrictions on TV and online for products high in fat, salt and sugar: government response. London: Department for Digital, Culture, Media and Sport, Department of Health and Social Care (https://www.gov.uk/government/consultations/further-advertising-restrictions-for-products-high-in-fat-salt-and-sugar/outcome/introducing-further-advertising-restrictions-on-tv-and-online-for-products-high-in-fat-salt-and-sugar-government-response#outcome-and-next-steps).

Enberg J (2019). Global digital ad spending 2019. In: eMarketer [website]. New York (NY): eMarketer (https://www.emarketer.com/content/global-digital-ad-spending-2019).

4   All references accessed 8 March 2022.

Facebook (2021). Meet the board. In: Oversight Board [website]. Menlo Park (CA): Facebook (https://oversightboard.com/meet-the-board/).

Facebook Audience Network (2020). Preparing audience network for iOS 14 [blog]. In: Facebook Audience Network [website]. Menlo Park (CA): Facebook Audience Network (https://www.facebook.com/audiencenetwork/news-and-insights/preparing-audience-network-for-ios14/#).

Gallagher B (2018). A comparison of GDPR and CCPA. In: IS Partners [website]. Dresher (PA): IS Partners (https://www.ispartnersllc.com/blog/gdpr-ccpa-comparison/).

GroupM (2017). This year next year. Worldwide media and marketing forecasts. London: GroupM (https://www.amic.media/media/files/file_352_1404.pdf).

Hastings G, Stead M, McDermott, Forsyth A, MacKintosh AM, Rayner M et al. (2003). Review of the research on the effects of food promotion to children. Final report. Prepared for the Food Standards Agency. London: Food Standards Agency (https://webarchive.nationalarchives.gov.uk/ukgwa/20110908054742/http://www.food.gov.uk/multimedia/pdfs/foodpromotiontochildren1.pdf).

Her Majesty's Revenue and Customs (2020). Digital services tax. In: Gov.UK [website]. London: United Kingdom Government (https://www.gov.uk/government/publications/introduction-of-the-digital-services-tax/digital-services-tax).

Hern A (2021). Apple and Facebook at odds over privacy move that will hit online ads. In: The Guardian [website]. London: Guardian News and Media Ltd; 2021 (https://www.theguardian.com/world/2021/jan/28/apple-and-facebook-at-odds-over-privacy-move-that-will-hit-online-ads).

Hodge N (2020). Companies face greater risk as GDPR class actions emerge. In: Compliance Week [website]. Boston (MA): Compliance Week (https://www.complianceweek.com/data-privacy/companies-face-greater-risk-as-gdpr-class-actions-emerge/29512.article).

IAB Tech Labs (2021). Project Rearc: how to participate. New York (NY): IAB Tech Labs (https://iabtechlab.com/project-rearc/).

ICO (2020). Age appropriate design: a code of practice for online services. Wilmslow: Information Commissioner's Office; 2020 (https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/).

Incorporated Society of British Advertisers (2020). Time for change and transparency in programmatic advertising. In: Incorporated Society of British Advertisers [website]. London: Incorporated Society of British Advertisers (https://www.isba.org.uk/news/time-for-change-and-transparency-in-programmatic-advertising/).

Informa (2010). Global mobile advertising revenues set to rise. In: Informa [website]. London: Informa (https://www.informa.com/media/press-releases-news/latest-news/global-mobile-advertising-revenues-set-to-rise-/).

Internet Advertising Bureau UK (2020). A guide to the connected TV supply chain. In IAB.uk [website]. London: Internet Advertising Bureau UK (https://www.iabuk.com/standard-content/guide-connected-tv-supply-chain).

Inventale (2020). SameSite Cookies, Chrome 80, Privacy Sandbox – what's what? In: Inventale [website]. Samara: Inventale (https://inventale.com/en/blog/privacy-sandbox/).

Joseph S (2020). WTF is Google's Privacy Sandbox? In: Digiday [website]. New York (NY): Digiday Media; 2020 (https://digiday.com/marketing/wtf-googles-privacy-sandbox/).

KBV Research (2019). Market research report. New York (NY): KBV Research (https://www.kbvresearch.com/in-app-advertising-market/).

Kelly M (2021). Facebook bans Trump indefinitely. In: The Verge [website]. Washington (DC): Vox Media (https://www.theverge.com/2021/1/7/22218725/facebook-trump-ban-extended-capitol-riot-insurrection-block).

Lomas N (2020). Google's Android ad ID targeted in strategic GDPR tracking complaint. In: TechCrunch+ [website]. Bay Area (CA): Verizon Media (https://techcrunch.com/2020/05/13/googles-android-ad-id-targeted-in-strategic-gdpr-tracking-complaint/).

Lomas N (2021). Facebook accused of continuing to surveil teens for ad targeting. In: TechCrunch+ [website]. Bay Area

(CA): Verizon Media (https://techcrunch.com/2021/11/16/facebook-accused-of-still-targeting-teens-with-ads/).

Manalo A (2018). 30+ privacy and security settings in iOS 12 you should check right now In: Gadget Hacks [website]. Austin (TX): WonderHowTo (https://ios.gadgethacks.com/news/30-privacy-security-settings-ios-12-you-should-check-right-now-0185045/).

McDermott L, O'Sullivan T, Stead M, Hastings G (2006). International food advertising, pester power and its effects. Int J Advert. 25(4):513–39. doi: 10.1080/02650487.2006.11072986.

Morrisroe B (2020). What is header bidding and why should you care? In: Publift [website]. Sydney: Publift (https://www.publift.com/adteach/what-is-header-bidding-and-why-should-you-care).

Mudd G (2021). Removing certain ad targeting options and expanding our ad controls. In: Meta for Business [website]. Menlo Park (CA): Meta (https://www.facebook.com/business/news/removing-certain-ad-targeting-options-and-expanding-our-ad-controls).

O'Dea S (2021). Smartphones – statistics & facts. In: Statista [website]. New York (NY): Statista (https://www.statista.com/topics/840/smartphones/).

O'Kane C (2020). Why the vertical ad network will win the decade. In: ExchangeWire [website]. London: ExchangeWire.com (https://www.exchangewire.com/blog/2020/04/14/why-the-vertical-ad-network-will-win-the-decade/).

O'Reilly R (2020). Facebook will shut down Facebook Audience Network's mobile web arm. In: Digiday [website]. New York (NY): Digiday Media (https://digiday.com/media/facebook-plans-shut-facebook-audience-networks-mobile-web-arm/).

Page C (2020). Oracle and salesforce hit with $10 billion GDPR class-action lawsuit. In: Forbes [website]. New York (NY): PARS International Corp. (https://www.forbes.com/sites/carlypage/2020/08/14/oracle-and-salesforce-hit-with-10-billion-gdpr-class-action-lawsuit/?sh=b40d66e323c2).

Peterson T (2019). WTF is device fingerprinting? In: Digiday [website]. New York (NY): Digiday Media (https://digiday.com/marketing/what-is-device-fingerprinting/).

Richter F (2021). Tech giants ramp up lobbying in face of antitrust scrutiny. In: Statista [website]. New York (NY): Statista (https://www.statista.com/chart/18792/annual-lobbying-expenditures-of-major-tech-companies-in-the-us/).

Rosenfelder S (2020). Global app install ad spend to double by 2022 to hit $118 billion. In: AppsFlyer [website]. San Francisco (CA): AppsFlyer (https://www.appsflyer.com/blog/trends-insights/app-install-ad-spend/).

Scroxton M (2020). GDPR lawsuit against Oracle and Salesforce moves forward. In: Computer Weekly.com [website]. London: TechTarget (https://www.computerweekly.com/news/252491537/GDPR-lawsuit-against-Oracle-and-Salesforce-moves-forward).

Shields R (2020). Privacy changes are making mobile advertising more complicated. In: Adweek [website]. New York (NY): Adweek (https://www.adweek.com/programmatic/privacy-changes-are-making-mobile-advertising-more-complicated/).

Solarwinds (2010). The incredible growth of the Internet since 2000. In: Solarwinds Pingdom [website]. Stockholm: Solarwinds (https://www.pingdom.com/blog/incredible-growth-of-the-internet-since-2000/).

StatCounter (2021). Mobile operating system market share worldwide Sept 2020–Sept 2021. In: StatCounter Gobal Stats [website]. Dublin: StatCounter (https://gs.statcounter.com/os-market-share/mobile/worldwide).

Statista (2021). Global digital population as of January 2021. In: Statista [website]. New York (NY): Statista (https://www.statista.com/statistics/617136/digital-population-worldwide/).

Sternberg J (2020). The publisher's paradox: clicks are up, but not ad revenue. In: Adweek [website]. New York (NY): Adweek (https://www.adweek.com/performance-marketing/publishers-paradox-clicks-up-ad-revenue-coronavirus/).

Tencent (2020). Tencent announces 2020 first quarter results. Shenzhen: Tencent (https://cdc-tencent-com-1258344706.image.myqcloud.com/uploads/2020/05/13/4fd0bbf73926176c433cc60314d492ff.pdf).

Twitter (2021). Permanent suspension of @realDonaldTrump [blog]. In: Twitter Inc. [website]. San Francisco (CA): Twitter Inc. (https://blog.twitter.com/en_us/topics/company/2020/suspension.html).

United Kingdom Government (2020). New public consultation on total ban of online advertising for unhealthy foods. In: Gov.UK [website]. London: United Kingdom Government (https://www.gov.uk/government/news/new-public-consultation-on-total-ban-of-online-advertising-for-unhealthy-foods).

W3C (2021). W3C [website]. Cambridge (MA): World Wide Web Consortium (https://www.w3.org/).

Winterberry Group (2020). The state of data 2020. New York (NY): Winterberry Group (https://www.iab.com/wp-content/uploads/2020/07/IAB-Winterberry_Group_The_State_of_Data_2020_July_2020.pdf).

Winterberry Group (2021a). The future of data-driven marketing. New York (NY): Winterberry Group.

Winterberry Group (2021b). Collaborative data solutions: data and identity in the era of permission. New York (NY): Winterberry Group (https://www.iab.com/wp-content/uploads/2021/05/Winterberry-Group-Collaborative-Data-Solutions-Final.pdf).

Wired (2021). How to fix Facebook, according to Facebook employees. In: Wired [website]. New York (NY): Wired (https://www.wired.com/story/how-to-fix-facebook-according-to-facebook-employees/).

WHO Regional Office for Europe (2019). Monitoring and restricting digital marketing of unhealthy products to children and adolescents. Report based on the expert meeting on monitoring of digital marketing of unhealthy products to children and adolescents, Moscow, Russian Federation June 2018. Copenhagen: WHO Regional Office for Europe (https://apps.who.int/iris/handle/10665/346585).

World Federation of Advertisers (2020). Survey: Covid-19 global response (April 2020). Brussels: World Federation of Advertisers (https://wfanet.org/knowledge/item/2020/05/13/Survey-Covid-19-global-response-April-2020).

Yeshanew H (2021). How the iOS 14 privacy change impacts small businesses. In Entrepreneur Europe [website]. Irvine (CA): Entrepreneur Media, Inc. (https://www.entrepreneur.com/article/383662).

Zeropark (2021). Waterfall vs. header bidding for web & in-app advertising. In: Zeropark [website]. Cracow: Zeropark (https://zeropark.com/blog/waterfall-vs-header-bidding-web-in-app-advertising/#Waterfall_bidding_explained).

The WHO Regional Office for Europe

The World Health Organization (WHO) is a specialized agency of the United Nations created in 1948 with the primary responsibility for international health matters and public health. The WHO Regional Office for Europe is one of six regional offices throughout the world, each with its own programme geared to the particular health conditions of the countries it serves.

Member States

Albania	Lithuania
Andorra	Luxembourg
Armenia	Malta
Austria	Monaco
Azerbaijan	Montenegro
Belarus	Netherlands
Belgium	North Macedonia
Bosnia and Herzegovina	Norway
Bulgaria	Poland
Croatia	Portugal
Cyprus	Republic of Moldova
Czechia	Romania
Denmark	Russian Federation
Estonia	San Marino
Finland	Serbia
France	Slovakia
Georgia	Slovenia
Germany	Spain
Greece	Sweden
Hungary	Switzerland
Iceland	Tajikistan
Ireland	Turkey
Israel	Turkmenistan
Italy	Ukraine
Kazakhstan	United Kingdom
Kyrgyzstan	Uzbekistan
Latvia	

**WHO European Office
for the Prevention and Control
of Noncommunicable Diseases**

9, Leontievsky pereulok
125009 Moscow, Russian Federation
Tel.: +7 (495) 787 21 17
Email: NCDoffice@who.int
Website: www.euro.who.int/en/NCDoffice