Review of online targeting: Final report and recommendations
Contents

Foreword 3

Executive summary 5

Introduction 10

1 What is online targeting? 13
   Personalised online advertising 15
   Content recommendation systems 18
   The role of online targeting in the business models of major online platforms 22

2 Why does online targeting matter? 28
   Online targeting as a form of power 29
   Applying an ethical framework 32
   Benefits and harms of online targeting 35

3 Public attitudes towards online targeting 48
   Perceived benefits of online targeting 50
   Concerns about online targeting 51
   The impacts of online targeting 52
   Appetite for change 54
   Solutions 56

4 The regulatory environment 60
   The current regulatory framework 61
   How effective is current regulation? 67
   Potential developments 80

5 Recommendations 91
   Our approach: limiting harms and enabling beneficial uses of online targeting 92
   Accountability 95
   Transparency 102
   User empowerment 112

Appendices 117
   1 Targeting options on major online platforms 117
   2 Platform recommendation systems 118
   3 Online targeting and machine learning 120
   4 The current regulatory framework 122
   5 Glossary 130
Foreword

Roger Taylor
Chair, Centre for Data Ethics and Innovation

Online targeting is a remarkable technological development. The ability to monitor our behaviour, see how we respond to different information and use that insight to influence what we see has transformed the internet, and impacted our society and the economy.

When technology develops very swiftly, there comes a moment when the implications of what is happening start to become clear. We are at such a moment with online targeting. A moment of recognition of the power of these systems and the potential dangers they pose.

In considering how the UK should respond, our starting point was to understand public attitudes. What we found was an appreciation of the value of targeting but deep concern about the potential for people’s vulnerabilities to be exploited; an expectation that organisations using targeting systems should be held to account for harm they cause; and a desire to be able to exercise more control over the way they are targeted.

Most people do not want targeting stopped. But they do want to know that it is being done safely and ethically. And they want more control.

These are very reasonable desires. But that does not mean it is easy – or even possible – to accommodate them. In making our recommendations we are proposing actions that kickstart the process of working out how public expectations can best be met.

Some of it requires greater regulation – and that requires systemic and coordinated approaches that focus first on the areas of greatest concern – such as the impact of social media on mental health.

The world will be looking at the UK’s approach and it is vital that new internet regulation protects human rights such as freedom of expression and privacy.

But it also requires innovation: innovation in the way that we regulate and innovation in the way the targeting systems are built and operated. Our recommendations are designed to encourage both.

By emphasising the need for a regulator to have powers to investigate how targeting systems operate, we recognise that better understanding will lead to more effective and proportionate regulation.
Foreword

Giving people more control over the way they are targeted is a more complex challenge. Tools to manage consent or to set preferences are clunky and unsatisfying. More radical solutions are harder to implement. We believe our recommendations can act as spur to innovation and new models of data management.

We have made three sets of recommendations to enable the UK to realise the potential of online targeting, while minimising the risk. First, new regulation to manage online harms that the government is planning to introduce should ensure that companies that operate online targeting systems are held to higher standards of accountability. Second, the operation of online targeting should be more transparent, so that society can better understand the impacts of these systems and policy responses can be built on robust evidence. Third, policy should seek to give people more information and control over the way they are targeted, so that such systems are better aligned to individual preferences.

These recommendations will help to build public trust over the long term, and enable our society and economy to benefit from online targeting. The UK has an opportunity to develop a world leading approach, and the CDEI looks forward to working with industry, civil society, policymakers, and regulators to achieve it.
Data-driven online targeting is a new and powerful application of technology. Using machine learning, online targeting systems predict what content is most likely to interest people, and influence people to behave in a particular way.

Personalisation of users’ online experiences increases the useability of many aspects of the internet. It makes it easier for people to navigate an online world that otherwise contains an overwhelming volume of information. Without automated online targeting systems, many of the online services people have come to rely on would become harder to use.

Online targeting systems are used to promote content in social media feeds, recommend videos, target adverts, and personalise search engine results. Online targeting is already an important driver of economic value and is a core element of the business models of some of the world’s biggest companies. It enables individuals and organisations to find a bigger audience for their stories or point-of-view, and businesses to find new customers. Automated systems now make decisions about a significant proportion of the information seen by people online.

As the underlying technology continues to develop, online targeting will continue to grow in sophistication and it will be used in novel ways and for new purposes. There are already a number of services that help people make positive changes by tracking their health, diet or finances and use personalised information or nudges to influence their actions. There is significant potential for further innovation.

However, online targeting systems too often operate without sufficient transparency and accountability. The use of online targeting systems falls short of the OECD human-centred principles on AI (to which the UK has subscribed), which set standards for the ethical use of technology. Online targeting has been blamed for a number of harms. These include the erosion of autonomy and the exploitation of people’s vulnerabilities; potentially undermining democracy and society; and increased discrimination. The evidence for these claims is contested, but they have become prominent in public debate about the role of the internet and social media in society.

Online targeting has helped to put a handful of global online platform businesses in positions of enormous power to predict and influence behaviour. However, current mechanisms to hold them to account are inadequate. We have reviewed the powers of the existing regulators and conclude that enforcement of existing legislation and self-regulation cannot be relied on to meet public expectations of greater accountability.
Executive summary

7 The operation and impact of online targeting systems are opaque. Information about the impact of online targeting systems on people and society is difficult to obtain as much of the evidence base is held by major online platforms. This prevents the level of scrutiny required to robustly assess the impact of targeting systems on individuals and society, and helps to obscure accountability.

8 Our new research into public attitudes towards online targeting shows that people welcome the convenience these systems offer, but express concern when they learn about the systems’ prevalence, sophistication and impact. They are particularly concerned about the impact of online targeting on vulnerable people. People do not want targeting to be stopped. But they do want online targeting systems to operate to higher standards of accountability and transparency, and people want to have meaningful control over how they are targeted.

9 There is recognition from industry as well as the public that there are limits to self-regulation and the status quo is unsustainable. Now is the time for regulatory action that takes proportionate steps to increase accountability, transparency and user empowerment. We recommend a number of steps to address public trust over the longer term.

10 We do not propose any specific restrictions on online targeting. Instead we recommend that the regulatory regime is developed to promote responsibility and transparency and safeguard human rights by design. Regulators must be able to anticipate and respond to changes in technology, and seek to guide its positive development to be better aligned with people’s interests.

11 The government should strengthen regulatory oversight of organisations’ use of online targeting systems through its proposed online harms regulator, working closely with other regulators including the Information Commissioner’s Office (ICO). The regulator should be required to increase accountability over online targeting through a code of practice. The code should require organisations to adopt standards of risk management, transparency and protection of people who may be vulnerable, so that they can be held to account for the impact of online targeting systems on users.

12 Regulation of online targeting should be developed to safeguard freedom of expression and privacy online, and to promote human rights-based international norms. The online harms regulator should have a statutory duty to protect and respect freedom of expression and privacy.

13 The regulator will need information gathering powers to assess whether platforms are operating in compliance with the code of practice, so that they can be held to account. In some cases external independent support will be needed to establish this. The regulator should have the power to require platforms to give independent experts secure access to their data to enable further testing of compliance with the code.
Executive summary

The regulator must use its powers in a proportionate way, recognising that the use of targeting can be low risk and to ensure responsible innovation can flourish. The regulator’s use of its powers should be subject to due process, with an established threshold for investigation, consultation with stakeholders, and a process under which the regulator’s findings can be appealed. The regulator must act at all times to protect privacy and commercial confidentiality. The online harms regulator should work with the ICO and the Competition and Markets Authority (CMA) to develop formal coordination mechanisms to ensure regulation is coherent, consistent, and avoids duplication.

Online targeting systems may have a negative effect on mental health, for example as a possible factor in “internet addiction”. They could contribute to societal issues including radicalisation and the polarisation of political views. These are issues of significant public concern, where the risks of harm are poorly understood, but the potential impact too great to ignore. We recommend that the regulator facilitates independent academic research into issues of significant public interest, and that it has the power to require online platforms to give independent researchers secure access to their data. Without this, the regulator and other policymakers will not be able to develop evidence-based policy and identify best practice.

Platforms should be required to maintain online advertising archives, to provide transparency for types of personalised advertising that pose particular societal risks. These categories include politics, so that political claims can be seen and contested and to ensure that elections are not only fair but are seen to be fair; employment and other “opportunities”, where scrutiny is needed to ensure that online targeting does not lead to unlawful discrimination; and age-restricted products.

We recommend a number of steps to meet public expectations for more meaningful control over how users are targeted. This includes support for a new market in third party “data intermediaries”, which would enable users’ interests to be represented across multiple services, and new third party safety apps.

Our analysis of public attitudes shows that there is an expectation that the public sector should use online targeting to ensure that advice and services are delivered as effectively as possible. Clear standards for the ethical use of online targeting systems will encourage the public sector to have greater confidence in using these techniques.

Societies are in the early years of developing policy and regulatory responses to data-driven technologies like online targeting. It took over a century to develop a regulatory framework to respond to the impact of steam power. The UK must learn the lessons of the past. By focusing on building the evidence base for informed policymaking and creating the right incentives, the UK will be able to govern online targeting in a way that is both trustworthy and allows responsible, sustainable innovation to thrive.
Executive summary

Key recommendations

Accountability
- The government’s new online harms regulator should be required to provide regulatory oversight of targeting:
  - The regulator should take a “systemic” approach, with a code of practice to set standards, and require online platforms to assess and explain the impacts of their systems.
  - To ensure compliance, the regulator needs information gathering powers. This should include the power to give independent experts secure access to platform data to undertake audits.
  - The regulator’s duties should explicitly include protecting rights to freedom of expression and privacy.
  - Regulation of online targeting should encompass all types of content, including advertising.
  - The regulatory landscape should be coherent and efficient. The online harms regulator, ICO, and CMA should develop formal coordination mechanisms.
  - The government should develop a code for public sector use of online targeting to promote safe, trustworthy innovation in the delivery of personalised advice and support.

Transparency
- The regulator should have the power to require platforms to give independent researchers secure access to their data where this is needed for research of significant potential importance to public policy.
- Platforms should be required to host publicly accessible archives for online political advertising, “opportunity” advertising (jobs, credit and housing), and adverts for age-restricted products.
- The government should consider formal mechanisms for collaboration to tackle “coordinated inauthentic behaviour” on online platforms.

User empowerment
- Regulation should encourage platforms to provide people with more information and control:
  - We support the CMA’s proposed “Fairness by Design” duty on online platforms.
Executive summary

- The government’s plans for labels on online electoral adverts should make paid-for content easy to identify, and give users some basic information to show that the content they are seeing has been targeted at them.

- Regulators should increase coordination of their digital literacy campaigns.

- The emergence of “data intermediaries” could improve data governance and rebalance power towards users. Government and regulatory policy should support their development.

The CDEI would be pleased to support the UK government and regulators to help deliver our recommendations.
Introduction

About the CDEI

The adoption of data-driven technology affects every aspect of our society and its use is creating opportunities as well as new ethical challenges.

The Centre for Data Ethics and Innovation (CDEI) is an independent expert committee, led by a board of specialists, set up and tasked by the UK government to investigate and advise on how we maximise the benefits of these technologies.

Our goal is to create the conditions in which ethical innovation can thrive: an environment in which the public are confident their values are reflected in the way data-driven technology is developed and deployed; where we can trust that decisions informed by algorithms are fair; and where risks posed by innovation are identified and addressed.

More information about the CDEI can be found at www.gov.uk/cdei

About this review

We have a unique mandate to make recommendations to the government drawing on expertise and perspectives from stakeholders across society. We provide advice for regulators and industry. This supports responsible innovation and helps build a strong, trustworthy system of governance. The government is required to consider and respond publicly to these recommendations.

In the October 2018 Budget,¹ the Chancellor announced that we would be exploring the use of data in shaping people’s online experiences. This review forms a key part of our 2019/2020 work programme.² It relates closely to several government workstreams, including the planned Online Harms Bill. It also relates to a number of high-profile regulatory activities, including the Competition

---

Introduction

and Markets Authority’s (CMA) market study into online platforms and digital advertising,\footnote{‘Online platforms and digital advertising market study’, Competition and Markets Authority, 2019; www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study} and the Information Commissioner’s Office’s (ICO) code of practice on age appropriate design for online services.\footnote{‘Age appropriate design: a code of practice for online services’, ICO, 2019; https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/age-appropriate-design-a-code-of-practice-for-online-services/}

26 This is the final report of the CDEI’s Review of Online Targeting and includes our first set of formal recommendations to the government.

Our focus

27 There are many applications of online targeting systems. We focus on the most prevalent, powerful and high-risk forms of online targeting: personalised advertising and content recommendation systems.

28 We focus on the issues that we have found are of greatest concern to the public, and where we assess there are significant regulatory gaps. We have looked in depth at the role online targeting plays in three areas: autonomy and vulnerability, democracy and society, and discrimination. Online targeting is closely related to competition policy and data rights, but we have focused less on these issues as they are being addressed by the CMA and ICO respectively.

29 Online targeting systems are used across the internet. They become more powerful at scale, when informed by the data of large numbers of users. This is put to greatest effect by major online platforms. Despite their powerful positions in society, these platforms operate with low levels of accountability and transparency. Our analysis of the regulatory environment demonstrates significant gaps in their regulatory oversight. Our analysis of public attitudes shows greatest concern and interest about the use of online targeting on large platforms.

30 Our research demonstrates that online targeting systems used by social media platforms (like Facebook and Twitter), video sharing platforms (like YouTube, Snapchat, and TikTok), and search engines (like Google and Bing) raise the greatest concerns in these areas. Our analysis and recommendations focus on the use of online targeting by these types of platforms.

31 Our recommendations aim to address the underlying drivers of harm and promote ethical innovation in online targeting. We have developed them in the context of various government programmes, including the proposed Online Harms Bill and review of online advertising regulation, and government announcements on electoral integrity and the reform of competition regulation in digital markets.
Introduction

Our approach

As set out in our interim report, we have sought to answer three sets of questions:

- **Public attitudes:** Where is the use of technology out of line with public values, and what is the right balance of responsibility between individuals, companies and the government? The findings of our public engagement are summarised in Chapter 3. The full report is published here [www.gov.uk/government/publications/cdei-review-of-online-targeting](http://www.gov.uk/government/publications/cdei-review-of-online-targeting)

- **Regulation and governance:** Are current regulatory mechanisms able to deliver their intended outcomes? How well do they align with public expectations? Is the use of online targeting consistent with principles applied through legislation and regulation offline? The findings of our regulatory review are set out in Chapter 4. The summary of responses to our open call for evidence is published here [www.gov.uk/government/publications/cdei-review-of-online-targeting](http://www.gov.uk/government/publications/cdei-review-of-online-targeting)

- **Solutions:** What technical, legal or other mechanisms could help ensure that the use of online targeting is consistent with the law and public values? What combination of individual capabilities, market incentives and regulatory powers would best support this? Our recommendations are in Chapter 5.

Our evidence base is informed by a landscape summary (led by Professor David Beer of York University); an open call for evidence; a UK-wide programme of public engagement; and a regulatory review of eight regulators. We have consulted widely in the UK and internationally with academia, civil society, regulators and the government. We have also held interviews with and received evidence from a range of online platforms.

---

1. What is online targeting?

Summary

- Online targeting comprises a range of practices used to analyse information about people and then customise their online experience. It shapes what people see and do online.

- This report considers two core uses of online targeting:
  - Personalised advertising, which enables advertisers to target content to specific groups of people online based on data held about them.
  - Recommendation systems, which enable websites to personalise the content their users see, based on the data they hold about them.

- Both approaches involve using advanced data analytics to observe people, make predictions about their behaviour and show information to them on that basis. These processes can be wholly automated through machine learning.

- Online targeting is at the core of the platform business model. Online platforms are among the world’s biggest companies. Recommendation systems encourage users to spend more time on these platforms. This leads to the collection of more data, increases the effectiveness of the recommendations and of the platforms’ personalised advertising products, and makes them more attractive to advertisers.

- An increasing variety of sources of data and applications may enable online targeting to become more sophisticated. Advances in technology may also lead to online targeting becoming less reliant on personal data.
What is online targeting?

In the time it takes you to read this sentence, approximately 100 hours of video will have been uploaded to YouTube and over 72,000 tweets will have been posted to Twitter.6

Individuals only see a tiny proportion of the billions of items of content that are hosted online. And, increasingly, what one person is shown is different to what their neighbour is shown. **Automated decisions are constantly being made about what content to show different people. These decisions are made by algorithmic systems that we refer to as “online targeting systems”**. They play a critical role in shaping what people see and do online. And this is fundamental to our ability to engage with the online world: without targeting, the mass of information online would be overwhelming, impenetrable and of less value.

**Online targeting systems’ effectiveness lies in their ability to predict people’s preferences and behaviours.** They collect and analyse an unprecedented amount of personal data, tracking people as they spend time online and monitoring and learning from how they respond to content and how this compares to other people with similar characteristics. This enables them to predict how users will react when shown different items of content. Their predictions are used to decide what content to show people in order to optimise the system’s desired outcome. People's responses to this content are then collected and fed back into the system in an iterative cycle.

This report considers two core uses of online targeting: personalised advertising and content recommendation systems. Personalised advertising systems aim to increase the effectiveness of online advertising. Content recommendation systems aim to increase user engagement (for example by watching a video, liking a post or sharing a picture). Both work by showing users the content that they are most likely to find engaging. Often this means showing people the content they are most likely to click on.

What has changed?

Companies selling products and services have always used targeting. Advertisers target mailshots based on demographic information about different postcodes. Newspapers publish content that they think will most appeal to their readers. But online targeting is different from traditional forms of targeting in five ways:

- **Data**: platforms collect an unprecedented breadth and depth of data about people and their online behaviours, and analyse it in increasingly sophisticated ways.

---

6 Based on an average read time of 12 seconds: 500 hours of video uploaded to YouTube per minute; www.statista.com/statistics/259477/hours-of-video-uploaded-to-youtube-every-minute/ and 6000 tweets per second www.internetlivestats.com/twitter-statistics/
What is online targeting?

- **Accuracy and granularity**: content can be targeted accurately to small groups and even individuals.
- **Iteration**: online targeting systems learn from people’s behaviour to constantly increase their effectiveness in real time.
- **Ubiquity**: content can be targeted at scale and at relatively low cost.
- **Limited transparency**: the ability to accurately match people with content inevitably limits the broader scrutiny of that content (including by the media and Parliament) as fewer people see each item of content, and don’t know much about what other users are seeing.

The power and effectiveness of an online targeting system depends on the number of people it affects, the amount of data available, the sophistication of the analysis that is carried out on that data, and the amount and variety of content available for online targeting. This means that major online platforms like Facebook and Google, with billions of users and huge financial resources, are especially well placed to use, and benefit from, online targeting.

**Personalised online advertising**

Personalised online advertising enables advertisers to target online advertising to specific groups of people using data about them. Selling personalised online advertising is an important part of the business model of many internet companies, including social media, search, and video sharing platforms. In this review, we have largely focused on display advertising rather than search advertising. This is because search advertising has tended to be targeted contextually, based on keywords searched by users, rather than information about the users themselves (although the CMA have noted that the line between contextual and personalised advertising is being increasingly blurred).

Personalised online advertising systems use a broad range of data about people: their demographic characteristics, interests, location, devices, personality types and more. Data is collected, inferred and combined into digital profiles (see Appendix 1), by data-brokers (companies that collect and buy data in order to aggregate the information and sell it on), other actors within the online advertising ecosystem, and the platforms themselves.

Personalised online advertising enables advertisers to specify their target audience and how many people they want to reach, with more precision and often more cheaply than they can offline.

---

7 ‘Online advertising in the UK’ Plum Consulting, 2019; https://plumconsulting.co.uk/online-advertising-in-the-uk/
8 CMA market study, Appendix E.
9 ‘Targeting your ads’, Google; https://support.google.com/google-ads/answer/1704368?hl=en-GB
What is online targeting?

Personalised online advertising makes it easy for advertisers to test different messages with different audiences and monitor how people respond. This is often referred to as “A/B testing”. Analysing the results and feeding them back into the online targeting system enables advertisers to improve the effectiveness of their advertising.

The sophistication of these tools, and the ease of accessing them, represents a step change from older forms of offline and online advertising. Traditionally, targeting has been based on the likely consumers of a type of media (for example a typical newspaper reader), rather than personal information. In traditional advertising, advertisers may test concepts with focus groups before distributing their adverts regionally or nationally, or test the outcomes of running adverts in different media. They reach their target market by distributing their adverts in the media that advertisers’ data show they are more likely to consume. For example, upmarket fashion brands may pay for outdoor advertising in more affluent neighbourhoods, print advertising in high-end fashion magazines, or contextual online advertising based on the site’s content and aggregate audience.

There are two main types of targeted online advertising: “programmatic” advertising outside of platform environments and personalised advertising on platforms.

Programmatic advertising

Programmatic advertising allows advertisers to target the people they want to reach across the internet.11

A commonly used programmatic approach involves “real time bidding”. When someone visits a website, the website publisher auctions advertising spaces to multiple advertisers through an auction system. This includes information about the person visiting the website, likely gathered through tracking technologies embedded in websites such as cookies and fingerprinting. Advertisers may attempt to build a more detailed picture of the person by referring to data held by data brokers and others. Based on this information, they decide how much they think it is worth to advertise to this person, and bid for the advertising space on that basis. The highest bid wins the right to use the advertising space.

This whole process happens instantaneously. It involves many companies, sharing significant amounts of data (including personal data) between them. Academics have estimated that over 50 adtech firms observe at least 91% of an average user’s browsing history by virtue of data sharing through the real time bidding process.12 Billions of online ads are placed on websites and apps in this way every day. The ICO outlines in detail how real time bidding works, and its concerns about its compliance with data protection law, in its update report into

adtech and real time bidding, and continues to develop regulatory responses. The CMA discusses real time bidding in its interim report on online platforms and digital advertising.

**Personalised advertising on platforms**

Platforms like Google and Facebook provide tools that advertisers can use to target their user bases. This targeting is performed using data that platforms have collected and inferred about their users based on what they do on the platform and elsewhere online, and data provided by advertisers. This may include sensitive data, or enable sensitive characteristics to be inferred.

*Figure 1: Facebook – Male Star Wars fans aged 18–34 living in Wales*

Many platforms also enable advertisers to target “custom audiences”, using the advertisers’ own data (“hashed” so that no identifiable data is transferred). This enables advertisers to target their own customers by matching common features such as an email address or phone number to the platform’s data. Advertisers can also target potential customers by using platforms’ tracking code on their websites to show adverts to them when they visit the platform.

---

15 ‘Online platforms and digital advertising market study; Appendix H: Intermediation in digital advertising’, Competition and Markets Authority, 2019; www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study
16 ‘What is off-Facebook activity?’ Facebook, www.facebook.com/help/2207256696182627
17 E.g. Google Analytics Conversions, Facebook Pixel
What is online targeting?

Platforms also provide tools for advertisers to target “lookalikes” of their existing customers. Lookalikes are the platform users that are identified as those who most closely resemble an advertiser’s existing customers. This is typically based on an overall measure of each user’s similarity to other users, which is constantly iterated on as more data about users is collected. Facebook, for example, offers lookalike advertising to an accuracy of 1% of its user base. In other words, the advertiser can target the 1% of Facebook’s user base that most closely resembles an uploaded or tracked audience, though this depends on the quality of data held about those customers.

The platforms offer sophisticated analytics tools. Advertisers can easily compare the effectiveness of different adverts with a particular audience, or compare the effectiveness of the same advert with different audiences. This allows advertisers to determine which language and visual features are most effective for persuading an audience to do something and learning which potential audiences are most valuable.

Optimising for different measures of effectiveness will lead to different results. For example, a brand seeking to drive online sales may require the platform to optimise for product sales. This could lead to a small number of the most valuable potential customers viewing a high frequency of adverts. A brand seeking to raise consumer awareness of its product may optimise for reach. This could lead to more people seeing the advert at lower levels of frequency.

Divides are blurring, between offline and online, and between contextual and personalised advertising. Advertising company Global offers geotargeted advertising on digital London buses, meaning that the advert on the side of the bus changes based on GPS data. Sky’s AdSmart product applies personalisation to television advertising, allowing companies to serve different adverts to different households “based on millions of different data points”.

Content recommendation systems

Content recommendation systems enable websites to personalise what each of their users see. Social media feeds, search engine results and recommended products and videos all rank content based on what they know about their users. Platforms use this analysis to determine what content is displayed.

Content recommendation systems generate an individual ranking of the content hosted by the platform (e.g. posts, videos, products) for a specific user. This ranking uses factors such as the type of content, its source, how recently it was uploaded, how others engaged with it, and how the user has historically engaged with similar content. The system will then show content to users in order, so that the first thing a user sees is the item of content that

---

18 ‘Create a Lookalike Audience from a Custom Audience’, Facebook Business; www.facebook.com/business/a/custom-to-lookalike-audiences
20 ‘Ad Smart: 5 years and Forward’, Sky Limited, 2019; www.adsmartfromsky.co.uk/
the system has determined they are most likely to respond to. Like personalised advertising, content recommendation systems collect data and analyse it to create digital profiles and assess users’ similarity to one another.

Online platforms can also use content recommendation systems to enforce their content policies. Where content does not meet criteria for removal but may nevertheless breach their policies (for example misinformation), platforms reduce its ranking or stop recommending it altogether, so fewer people see it. For example, Facebook’s recommendation system tries to identify and reduce the prominence of posts with exaggerated or sensational health claims. In this case, its system identifies commonly used phrases to predict which posts are likely to breach their policies and refers them to human moderators or fact checkers, who can then decide to downrank it. However, because of the cultural context and nuance in language and images used in online posts, automated systems may not be as good as humans at identifying content correctly.

Many major online platforms also employ human moderators to support this process, though many content moderation decisions may be difficult for humans, too.

Figure 2: On YouTube, recommended “Up Next” videos are displayed next to the video that a user is watching

What is online targeting?

Figure 3: On Twitter, news and events are recommended to users based on what the platform thinks will interest the user.

There are two main types of content recommendation systems: content-based filtering and collaborative filtering.²⁴ Content-based filtering systems recommend content based on its similarity to content previously consumed by the user (“picture X has a similar title to previously viewed pictures Y and Z”). Collaborative filtering systems recommend content based on what similar users have consumed (“people A, B and C like this; a similar person D might also like this”). Some platforms use hybrid approaches combining features of both methods.²⁵

Figure 4: Collaborative and content-based filtering approaches²⁶

---

²⁶ Source: Sanket Doshi, ‘Brief on Recommender Systems’ Towards Data Science, 10 February 2019; https://towardsdatascience.com/brief-on-recommender-systems-b86a1068a4dd
Recommendation systems can also be analysed based on the type of recommended content:27

- **Closed**: recommended content is generated or curated by the platform itself.
- **Open**: recommended content is mostly user-generated. User-generated content is automatically added to the recommendation engine to be surfaced to users.

For example, BBC iPlayer is a closed system, which serves a mix of BBC content, including manually curated and personalised content recommendations, which for signed-in users are based on previous viewing history.28 YouTube is an open system, and takes many more variables into account when recommending content.29 Pinterest is also an open system. It encourages users to proactively indicate their interests, and uses this information to determine what content to promote to them.30

As someone spends more time on the platform, the recommendation system learns how they, and similar users, respond to different content. It then uses this learning to generate more accurate predictions of what content they are likely to respond to, and how, in the future.

As with personalised advertising, **recommendation systems can be optimised to serve different business goals**. For example, a platform focused on rapid growth may focus on short-term engagement metrics like clicks, whereas a platform focused on maximising long-term use (leading to a greater number of overall clicks) may adopt metrics that could correlate with a higher quality experience, such as the length of time a user spends reading an individual article.31

**Recommendation systems are a new way of spreading information.** Like editors of print and broadcast media, recommendation systems give prominence to certain types of content. In traditional media, these decisions are based on the editor’s view of what is likely to appeal to their readership or audience. Traditional editorial approaches involve human judgment, a single product, and a lack of information about readers or viewers at an individual level. Recommendation systems, by contrast, involve automated predictions about what will appeal to an individual, based on knowledge about that individual (see Box 1: Machine learning and online targeting).

---

28 ‘What are recommendations?’, BBC, www.bbc.co.uk/iplayer/help/questions/features/recommendations
What is online targeting?

Box 1: Machine learning and online targeting

Some modern online targeting systems use a machine learning technique called *deep learning*. This is a powerful pattern recognition system that can uncover relationships between different pieces of content. The systems uncover relationships by assigning numerical values to aspects of the content such as words in a sentence or the colours in an image.

These values are then used to produce a model of the relationships between values, and how users interact with pieces of content that have been assigned the same or similar values.

Content is disseminated according to mathematical values the system has assigned it. A machine alone cannot appraise that content in context as a human can. As such, if constraints cannot be specified in a form a machine can easily interpret, it may recommend content in a way a human curator would not (see Appendix 3).

The role of online targeting in the business models of major online platforms

Online platforms are digital services that facilitate interactions between users. While they have different business models, they share some core features. They make connections, between buyers and sellers (as in online marketplaces), people and information (as in search engines), or people themselves (as in social media). They generate revenue by enabling advertisers to target their users.

The platform business model has been harnessed most effectively by a small number of American and Chinese companies including Google, Facebook, Amazon, Tencent and Alibaba, which have gained vast, and in many cases, global user bases.

Seven of the world’s largest ten companies, and the world’s top 10 most visited websites, are online platforms. 89% of the UK internet audience aged 13+ shops on Amazon, 90% has a Facebook profile, and 73% of UK adults report consuming news on Facebook. Google and Facebook together generated an estimated 61% of UK online advertising revenue in 2018.

---

35 ‘Online advertising in the UK’, Plum Consulting, 2019; https://plumconsulting.co.uk/online-advertising-in-the-uk/
How online targeting drives the online platform business model

Content recommendation systems and personalised advertising work together to drive the success of the biggest online platforms. Content recommendation systems encourage users to spend more time on the platform and in the process users share more data about themselves. This increases the amount of revenue that can be earned from personalised advertising in three ways. First, users spend more time on the platform, increasing the number of opportunities to serve adverts to users. Second, it is easier to predict individual user behaviour, increasing the amount that platforms can charge advertisers for reaching the right people. Third, users may find personalised adverts more relevant, increasing their tolerance for an increased number of adverts. Every action users take enables the platform to extract more data, driving the value of the platform.

Figure 5: The role of online targeting in platform business models reliant advertising

In economic terms, platform business models are characterised by network effects, both direct (where a platform is more valuable to individual users the greater the number of other users also active on the platform) and indirect (where the value for users on one side of the platform such as content producers and advertisers increases with the number of users on the other side of
What is online targeting?

As more users are attracted to both sides of a platform, and more content is hosted, online targeting systems become increasingly important, as they enable users to navigate the platform and advertisers to reach their target audience. They also increase the platform’s ability to collect and monetise data about their users, improving their services and entrenching the network effects by attracting more users to both sides of the platform.

Online markets have also seen the emergence of “ecosystems”, offering different products and services under the same brand and extending the network. Google has built on its initial search engine with email (Gmail), a mobile operating system (Android), geographic services (Google Maps) and video streaming (YouTube). Through these different services, it can collect even more data about users that it can use to improve its online targeting systems and further increase user engagement and revenue. While some of these products have been developed in house (Android), others (YouTube) have been the result of strategic acquisitions.

Many platforms offer tools that embed tracking technologies in third party websites and apps. These provide analytics services but also enable platforms to collect more data about the users of the apps and websites that install them. Such trackers are now widespread. For example, research shows 88% of Android apps contain a Google tracker, 43% contain a Facebook tracker, and 34% contain a Twitter tracker.

Platforms are increasingly acquiring or developing physical products that enable data collection in traditionally offline environments. These include products for the home such as smart speakers, thermostats and video doorbells. Platforms are also investing in wearable technology involving activity trackers and operating systems for cars. The rollout of 5G is predicted to create new opportunities for platforms to extend their networks of connected devices and target users with greater sophistication through more accurate location sharing with apps. This may enable companies to target consumers more accurately with location or time-specific offers.

38 E.g. Amazon Alexa, Google Home
39 E.g. Google Nest, acquired by Google in 2014
40 E.g. Ring, acquired by Amazon in 2018
41 E.g. Apple Watch or Fitbit (which Google announced its intention to acquire in November 2019)
42 E.g. Apple’s CarPlay and Google’s Android Automotive
What is online targeting?

Box 2: The influence of Chinese platforms

In China, a parallel ecosystem of platforms has developed. This reflects the inability of Chinese people to access many of the American-owned platforms, as well as different consumer expectations from online services. Companies like Tencent, Alibaba, ByteDance and Baidu have grown to become some of the world’s biggest businesses, largely catering to Chinese consumers. In the 2000s, many Chinese internet companies developed as near-imitations of their international counterparts. However, in recent years, some of the features of Chinese platforms are being adopted by American platforms and ByteDance-owned TikTok has become successful in the West in its own right.

Tencent-owned WeChat is a social media messaging platform which has been described as China’s Facebook. However WeChat includes many other features within a single app, including payments, search, travel booking, taxi hailing, and the ability to buy services including utilities, healthcare, lottery tickets and visas. Personalised advertising represents a comparatively smaller share of WeChat’s revenue, with the platform receiving a processing fee for its payments service and users’ data used to help sell other services, such as video gaming. Facebook has adopted features associated with WeChat, including video gaming within Messenger. In 2019, Mark Zuckerberg announced the future of Facebook would involve a greater focus on encrypted, private groups and plans for its own payments system.

ByteDance is the first Chinese platform to develop a significant user base in Europe and the United States. The company’s two main products in China are Douyin, a recommender service for user-generated short videos, and Toutiao, a personalised news aggregator. ByteDance’s international products include TikTok, which follows a very similar use design to Douyin, and news aggregator NewsRepublic. TikTok was launched in 2017 and is reported to have acquired 500 million monthly active users (more than Twitter, LinkedIn or Snapchat).

---

46 Ashley Galina Dudarenok, ‘As Facebook looks to WeChat, China’s digital world is wowing the West, and globalisation is no longer a one-way street’, in ‘South China Morning Post’, 01 April 2019; www.scmp.com/comment/insight-opinion/article/3004101/chinas-digital-world-wows-west-and-globalisation-no-longer
What is online targeting?

While the importance of online targeting systems is clear, it is difficult to quantify their impact with publicly available information. Studies released by major online platforms tell us, for instance, that 35% of purchases on Amazon, 53 70% of views on YouTube54 and 80% of all user engagement on Pinterest55 come from recommendations. In 2016, Netflix valued its recommendation system at US$1 billion per year and showed that “when produced and used correctly, recommendations lead to meaningful increases in overall engagement with the product (e.g. streaming hours) and lower subscription cancellations rates.”56 Google has stated that the YouTube recommendation system “represents one of the largest scale and most sophisticated industrial recommendation systems in existence”, with “enormous user-facing impact”.57

Conclusion

Online targeting systems are changing rapidly in response to new technologies, new regulations, and new ways in which people interact with online content. Many respondents to our call for evidence highlighted that the direction of travel is towards more sophisticated, and intrusive, predictions, and an increased role for targeting technologies in different areas.58 They highlighted the availability of new data sources, the adoption of new approaches such as facial recognition and improved sentiment analysis, and the potential to combine online and offline data. Others suggested that emerging technologies and the widespread uptake of encryption will lead to improvements in privacy. This could allow for targeting

The Washington Post’s official TikTok page; www.tiktok.com/@washingtonpost
What is online targeting?

to become more accurate without personal data being shared, though would not necessarily mean reductions in the power of targeting or the tracking of user behaviour.\textsuperscript{59}

In the next chapter, we assess online targeting in the context of the OECD human-centred principles on Artificial Intelligence. We explain how limited transparency and accountability over online targeting is a hazard. We discuss the benefits and harms online targeting can lead to, in particular in relation to autonomy and vulnerability, democracy and society, and discrimination.

2. Why does online targeting matter?

Summary

- Online targeting is powerful: it enables people’s behaviour to be monitored, predicted and influenced at scale. It also contributes to and benefits from platforms’ market power.

- Online targeting systems used by major online platforms help people to make sense of the online world. Further innovation in ethical recommendation systems can benefit people and society.

- However, the major online platforms have harnessed the power of online targeting with low levels of accountability and transparency. This falls short of the UK-endorsed OECD principles for the ethical use of artificial intelligence and calls into question the legitimacy of the platforms’ power.

- In these circumstances, the operation of powerful online targeting systems is a hazard. There is some evidence of harms caused by online targeting systems in relation to autonomy and vulnerability, democracy and society, and discrimination. However, the ability to understand the impact of online targeting systems is limited because much of the evidence base lies with the major platforms themselves.

- The way in which online content is targeted is a critical factor in determining how harmful it is likely to be. This is highly relevant for the UK government’s proposed Online Harms Bill.
Why does online targeting matter?

Online targeting as a form of power

The power of online targeting

1. A new way of consuming information

Online platforms are used by people all over the world to connect with others, and create and access a wide range of content. The content each user is shown on the platform is personalised to them by online targeting systems. The content they see may be provided alongside private messaging services, blurring the lines between private and public spaces.

In the analogue world, ideas travel through public debate and personal networks (families, friends and colleagues), and through institutions (the media, the state and religious institutions). Unlike online platforms, these institutions select the information they share on the basis of its expected level of public interest and its fit with their agenda.

2. Changing power structures

The role online platforms play in society, and their use of online targeting systems, translates to significant social and political power. This power can be exerted by the platforms themselves. It can also be harnessed by others who use platforms, from bloggers and activists, to charities and political parties, to terrorist groups and hostile state actors.

The four key elements to platform social and political power are:

- **Observation**: the platforms can observe people’s behaviour in environments where they have an expectation of privacy, such as the home. Knowledge about individuals makes it easier to influence their actions. When people know they are being observed they may behave differently.60

- **Influencing perception**: the platforms have become a major source of news and information.61 The decisions made by online targeting systems influence the flow of information in society and this affects what people perceive as normal, important and true.62 This impact is compounded by the fact that people do not know that this process is taking place: it does not involve a conscious choice like turning on the TV or picking up a newspaper.

---


61 Ofcom found that half of people now use social media for news – 49%, compared to 44% in 2018. “Use of many social media platforms for news has increased, with more people saying they use Twitter, WhatsApp and Instagram, while Facebook has remained stable. However, social media was less trusted as a source of news than broadcast and print media with only 37% of people saying it was impartial”, 'News consumption in the UK', Ofcom, 2019; www.ofcom.org.uk/research-and-data/tv-radio-and-on-demand/news-media/news-consumption; The Cairncross Review reported that 74% of UK adults read news each week via an online source (including social media): ‘The Cairncross Review: a sustainable future for journalism’, HM Government, 2019; www.gov.uk/government/publications/the-cairncross-review-a-sustainable-future-for-journalism

Why does online targeting matter?

- **Prediction and influence:** organisations using online targeting systems can learn from how people react to content and use this knowledge to make increasingly accurate predictions which can be used to influence people’s actions and even beliefs, as individuals, but also across populations.

- **Control of expression:** online platforms, through their content policies and dissemination systems, are able to play a major role in determining how people express themselves and how far those views travel.

**Online targeting and the power of the major online platforms**

1. **A concentrated market**

   Online targeting has been used most successfully by a number of online platforms operating in search, social media and video sharing. The Digital Competition Expert Panel report (the Furman report) describes a tendency for a small number of companies to dominate digital markets, while Ofcom analysis shows that the characteristics of some online services can lead to a range of market failures, including market power.

2. **Market effects**

   The UK Competition and Markets Authority (CMA) interim report on its market study into online platforms and digital advertising found that Google and Facebook are “the largest online platforms by far, with over a third of UK internet users’ time online spent on their sites”. It concludes that their profitability has been “well above any reasonable estimate of what we would expect in a competitive market”, and that they “appear to have the incentive and ability to leverage their market power... into other related services”. Their control over user data, and ability to use it in their online targeting systems, is an important factor in this.

   While the CMA did not report any direct evidence of abuse of their market power, it comments that if competition in search and social media is not working well, this could lead to reduced innovation and choice in the future, and to consumers giving up more data than they feel comfortable with. It states that weak competition in digital advertising can increase the prices of goods and services across the economy and undermine the ability of newspapers and others to produce valuable content.

---


64 ‘Online market failures and harms – an economic perspective on the challenges and opportunities in regulating online services’, Ofcom, 2019; www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/online-policy-research/online-market-failures-and-harms

65 ‘Online platforms and digital advertising market study’, Competition and Markets Authority, 2019; www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study
3. Further harms from high online platform concentration

Market failures, including market power, could in some cases lead to a range of consumer and societal harms. Online targeting could play a role in this. Ofcom sets out that some online services are incentivised to maximise the data and attention they capture from consumers, using processes which are made more effective by online targeting. This can help to increase the value of the platform to advertisers, but could also contribute to the spread of harmful content. Further, Ofcom highlights that, if this data is used to influence consumer decision making through online targeting, this may limit users’ exposure to a variety of views.66

4. Legitimacy

The major platforms’ market position means they have been best able to exercise the power of online targeting. This, in turn, gives them significant social and political power. In this context, it is not necessarily clear who, online platforms, governments or users, has the most legitimate authority to set rules about how content is promoted.

It could be considered legitimate for platforms to set these rules, because their users individually offer consent by using the service.67 On this basis, newspapers are largely self-regulating. Democratic governments could also claim legitimacy to set these rules as their power is derived from the consent of the governed.68 On this basis, broadcasting is subject to statutory regulation. Another argument is that platform users have the greatest legitimacy to set the rules. This could be for democratic reasons (platform users should have the right to shape the rules they are required to follow) or because users are part of a community that generally offers benefits (so they should be required to follow group norms, but be able to influence these in some way including through informal mechanisms).69 On this basis, political parties elect their leaders.

66 Online market failures and harms – an economic perspective on the challenges and opportunities in regulating online services, Ofcom, 2019; www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/online-policy-research/online-market-failures-and-harms
Why does online targeting matter?

We do not believe that platforms have full legitimacy, because of the lack of consumer choice between platforms and because platforms’ decisions have impacts on people who are not their users. Platforms may not always wish to be in positions of political power – some have expressed concern about having to take choices that would historically have been left to democratically elected governments.70 We therefore think that democratic governments and citizens should play a bigger role in deciding how online targeting is governed.

Applying an ethical framework

We aim to help create the conditions where ethical innovation using data-driven technology can thrive. There are a number of ethical frameworks that we can draw on to guide our thinking.71 In particular, we have welcomed the commitment of 42 countries, including the UK, to the OECD human-centred principles on AI.72 These are framed specifically with reference to Artificial Intelligence and are therefore directly relevant to the content recommendation systems driven by machine learning. They also provide a relevant framework for evaluating any complex algorithmic system and are therefore relevant to online targeting in general.

As discussed above, online targeting helps people to make sense of the online world. Without online targeting, it would be harder for people to navigate virtually unlimited content to find the news, information and people that have meaning and value to them. Whether people are using an app, connecting with fellow enthusiasts to talk about a hobby, looking for a job, or catching up with the news, online targeting shapes what they see.

Online targeting is integral to many online business models. It lets companies, including small companies, reach people who may be interested in their products and services more cheaply and easily. And it has great potential to be used in the public sector, to help people find training, avoid risky behaviour and make healthy life choices.

However, we believe that the use of online targeting systems by major online platforms is currently inconsistent with the OECD principles.

---


**Why does online targeting matter?**

*A high-level assessment of online targeting systems used by major online platforms against the OECD human-centred principles on AI*

<table>
<thead>
<tr>
<th>Principles</th>
<th>Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>AI should benefit people and the planet by driving inclusive growth, sustainable development and well-being.</td>
<td>While online targeting systems offer economic benefits to people and businesses, they have also contributed to the significant market power of a small number of major online platforms. The impact of online targeting on wellbeing is highly contested. For example, the Royal College of Psychiatrists argues that there is growing evidence of an association between social media use and poor mental health, but that the lack of research on the connection between mental health and technology makes it difficult to identify causality. Moreover, the information needed to establish the balance of benefits and harms is only accessible to the major online platforms. More research should be done on the impact of online targeting on sustainable development, though some studies warn that online advertising uses high levels of energy.</td>
</tr>
<tr>
<td>AI systems should be designed in a way that respects the rule of law, human rights, democratic values and diversity, and they should include appropriate safeguards.</td>
<td>Online targeting systems may undermine the rule of law by disseminating illegal content and facilitating unlawful discrimination. They may impact negatively on human rights, such as privacy, data protection and freedom of expression. And the targeting of political content online may undermine democratic values by enabling political campaigning to take place in a way that is not visible to opponents and as a result cannot be properly contested in public discourse.</td>
</tr>
<tr>
<td>There should be more transparency around AI systems to ensure that people understand AI-based outcomes and can challenge them.</td>
<td>There is very limited transparency over online targeting systems, to users and to society more widely. Users are not provided with sufficient understanding or control of online targeting.</td>
</tr>
</tbody>
</table>

---


Why does online targeting matter?

### Principles

<table>
<thead>
<tr>
<th>Principles</th>
<th>Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>AI systems must function in a <strong>robust, secure and safe way</strong> throughout their life cycles and potential risks should be continually assessed and managed.</td>
<td>Risks associated with online targeting systems are assessed and managed inconsistently. Many online platforms have introduced processes designed to mitigate some risks, such as the spread of misinformation through content recommendation systems. However, these tend to be reactive instead of proactive and are not subject to any scrutiny or independent oversight. In this light, it is difficult to assess if they are sufficient.</td>
</tr>
<tr>
<td>organisations and individuals developing, deploying or operating AI systems should be held accountable for their proper functioning in line with the above principles.</td>
<td>Organisations that choose to use online targeting systems (and the people that make decisions to do so) need to be accountable for their effects. There is currently no effective mechanism in the UK whereby platforms operating AI driven content recommendation systems are held to account for their behaviour.</td>
</tr>
</tbody>
</table>

91 The OECD principles contain three concepts that we believe are particularly relevant to this review: transparency, safety and accountability.

92 Generally, **people do not understand how online targeting can affect them and what they can do about it**. Individual users often do not know what data platforms hold about them, how they collect it and how it is used in their online targeting systems. They may not be aware that they are seeing targeted content. Even if they are, it may not be clear where the content has come from, why it has been targeted to them and what content they are missing out on. Users are therefore less likely to be able to evaluate the content critically, and to know when and how they may have been harmed by an online targeting system. When they are aware, **there may not be a satisfactory way for people to seek redress from platforms.**

93 On top of this, many **online platforms also offer limited transparency to society more widely** (regulators, the media, civil society organisations, academia, government, Parliament and so on). In recent years, some online platforms have started to make some information available publicly about their operations in the form of transparency reports, but these are limited, not independently verified and not comparable across platforms.

94 The UK Government’s Online Harms White Paper (see Box 5 below) **sets out a range of evidence of unsafe targeting practices.** It notes that some companies have taken steps to improve safety on their platforms, but that

---

overall progress has been too slow and inconsistent. The Carnegie UK Trust has argued that many online platforms have failed to systematically monitor and mitigate the risks their systems pose to users.76

95 The operators of these systems are not currently held to account in any meaningful way. There are few regulatory incentives for them to empower their users and align more closely with their interests, and the interests of society more widely. Given their global nature, the fast pace of change in technology and its uses, the complexity of platform business models, the scale of content they host and the variety of services they offer, regulation has not yet adapted to enable online platforms to be held to account where it may be necessary.

96 We set out further evidence supporting these assessments in the remainder of this chapter, where we consider the harms and benefits of online targeting. In Chapters 3 and 4, we draw on our research into public attitudes towards online targeting and our review of the strengths and weaknesses of the UK regulatory environment to set out further evidence.

**Benefits and harms of online targeting**

**Online targeting plays an essential role in people’s lives. However, currently it is a significant hazard.** As set out in the introduction to this report, we have focused our work in this review on the areas we have found to be of greatest concern to the public, and where we assess there are significant regulatory gaps. We have looked in depth at the role online targeting plays in three areas: autonomy and vulnerability, democracy and society, and discrimination.

**Limited evidence base**

**There is limited understanding of the impact of online targeting on individuals and society.** Beyond anecdote, little empirical evidence is available to assess the risks posed by online targeting and the extent of the harms it causes or exacerbates. This view has been expressed widely: many respondents to our call for evidence cautioned that there is limited reliable evidence in the public domain about how online targeting works and the impacts it has on people and society.

99 However, absence of evidence of harm is not evidence of absence of harm. Where there is anecdotal evidence of people experiencing harm caused or exacerbated by online targeting systems, it is possible that other people have also experienced similar harms. Much of the information needed to understand the extent of harm is only accessible to the major online platforms. Respondents to our call for evidence saw this as a serious problem for policymakers and regulators.
Why does online targeting matter?

The following section outlines some of the available evidence about the benefits of online targeting, and the harms it may cause or exacerbate. In some cases, platforms have told us that their practices have changed since the incidents cited.77

The benefits and harms captured below do not apply uniformly across all online targeting systems. Different applications of online targeting carry different risks, depending on the content they target and what they are optimised to achieve. For example, in broad terms, content recommendation systems used by social media and video-sharing platforms aim to highlight relevant and engaging content to keep users on the service for longer, whereas those used by search engines aim to find relevant and engaging content to direct users off the service as quickly as possible. In this case, risks that people get stuck in “rabbit holes” are higher on social media and video-sharing platforms than on search engines.

Autonomy and vulnerability

1. Benefits

Navigation and discovery

Online targeting helps people to navigate the vast amount of information available online by showing them content it has predicted they will engage with. It can also broaden people’s horizons through content “discovery”, by suggesting content that they wouldn’t have sought out but which might be beneficial to them. For example, a study has found that 79% of all consumers, and 90% of those under 30, agree that streaming services that use online targeting systems play a huge role in their discovery of new video content.78

Influencing behaviours and beliefs

There are also great opportunities for applications of online targeting to influence people’s behaviour positively. Used responsibly, online targeting can help people make informed choices and support important public information campaigns. For example the Department for Transport achieved an 11% increase in young men who thought it was unacceptable to let a friend drive after drinking, following an online public awareness campaign targeting them.79

77 For example, since January 2019, Google has launched over 30 different changes on YouTube to reduce recommendations of “borderline” content, content that could misinform users in harmful ways and content that comes close to violating their Community Guidelines. It has said it has made changes to elevate “authoritative” sources in its systems and provide reliable information faster for breaking news. Facebook has said it has changed its News Feed recommendations to prioritise posts that encourage “meaningful interactions” between people. Instagram has started working with third-party fact-checkers to help label false information. It has prohibited graphic images of self-harm and reports that it is working to ensure that it is not recommended.


There is a growing number of tools and apps that provide personalised information and advice to people, for example to help them maintain a healthy diet and progress in their education. British company Sparx Maths provides an online learning tool that assesses students’ maths ability based on their homework performance. It then generates class and homework tasks tailored to their ability.80

**Protective online targeting**

Online targeting can also be used to predict where people may be susceptible or vulnerable to particular harms and aim to prevent them seeing potentially harmful content. For example, online targeting systems could be used to avoid showing children advertising for age-restricted products and unhealthy food choices. The Advertising Standards Authority (ASA)’s Code of Non-Broadcast Advertising and Direct & Promotional Marketing (CAP code) says that, when advertised on social media, the ASA expects advertisers “to make full use of any tools available to them to ensure that ads are targeted at age appropriate users”.81

The Samaritans is working with industry and government to deepen the understanding of how people engage with online content relating to self-harm and suicide.82 Some of the major online platforms have attempted to address the potential impact of content relating to self-harm and suicide. Instagram, for example, can (and does) remove, reduce the visibility of, or add sensitivity screens to this type of content, but recognises that sharing this type of content can also help vulnerable people connect with support and resources that can save lives.83

**Targeted support to vulnerable people**

With appropriate safeguards and controls, online targeting could be used to support vulnerable people. Public Health England uses data to target its campaigns to people who show interest in specific topics (such as mental health issues), or people in areas where the prevalence of specific conditions is high. This enables them to provide more tailored messaging and to be more efficient with their resources. The NHS Mid-Essex Clinical Commissioning Group (CCG) ran an advertising campaign on Facebook to raise awareness of local mental health services, targeting 18–45 year-old men, who are most at risk of suicide. After a four-week trial, traffic to the CCG’s website increased by almost 74% (of which 341 visits came directly from Facebook, compared to just 24 visits the previous month). Overall, referrals to the service increased by 36% over the trial period, with a marked increase in referrals from men.84

---

80 ‘Why does Sparx Maths Work: Evidence Based Design’, Sparx Maths; https://sparx.co.uk/impact/
81 ‘Children: Targeting’ Advertising Standards Authority, 2018; www.asa.org.uk/advice-online/children-targeting.html#Age-Restricted%20products
Why does online targeting matter?

2. Harms

Exploiting first-order preferences

Online targeting systems are informed by a deep understanding of people and how they behave online. This has led to widespread concern that online targeting systems can exploit people’s “first order preferences” (their impulsive, rather than reflective, responses). The Mozilla Foundation’s list of “YouTube Regrets” documents real-life stories of YouTube “rabbit holes”. Experiments have also shown that when adverts were targeted at people based on psychological traits (such as extraversion and openness) inferred about them from their Facebook data, they were 40% more likely to click on the ads, and 50% more likely to make purchases.

Manipulating behaviours and beliefs

Online targeting can reinforce people’s existing preferences and shape new ones. In doing so, it can also have a wider impact on users’ behaviours and beliefs. For instance, by randomly selecting users and controlling the content they were shown (giving some users slightly more upbeat posts and others more downbeat ones), Facebook influenced the sentiment of these users’ posts, which were correspondingly slightly more upbeat or downbeat depending on the content they had been shown. Equally, the ranking of Google search results can shift the voting preferences of undecided voters by 20% or more, without people being aware.

Exploiting people’s vulnerabilities

The risk that online targeting poses to autonomy is more significant for people who may be vulnerable. Many of the “YouTube Regrets” stories referred to above document the experience of children and older people. The ASA has found gambling adverts served to children online, in direct contravention of the CAP code (online gambling adverts are powerful: the Gambling Commission found that 45% of online gamblers were prompted to spend money on gambling activity due to the adverts they saw). Anti-vaccine groups are known to have used Facebook to target new mothers with misinformation on vaccine safety (Facebook used to allow advertisers to target users it classified as being interested in “vaccine controversies”).

References:
2 Why does online targeting matter?

The advert and Facebook page in question were later investigated by the ASA and found to be in breach of the CAP code due to misleading claims and causing distress.92

“Internet addiction”

Some online products incorporate “persuasive design” features to encourage continuous use.93 Research has found that online targeting could exacerbate addictive behaviours.94 The number of people suffering from clinical addiction in this way has not been reliably quantified, but there are well-documented extreme cases of vulnerable individuals for whom addiction has got in the way of social lives, sleep, physical activity and other parts of a healthy, balanced lifestyle.95 While there is limited evidence to demonstrate a causal negative effect on mental health from persuasive design and increased screen time, the UK’s Chief Medical Officers have recommended platforms follow precautionary approaches.96

Amplifying “harmful” content

Content recommendation systems may serve increasingly extreme content to someone because they have viewed similar material.97 The proliferation of online content promoting self-harm, including eating disorders, is reasonably well documented.98 Ian Russell, the father of Molly Russell, who died by suicide in 2017 aged 14, believes that the material she viewed online contributed to her death and has said that social media “helped kill his daughter”.99 The coroner investigating Molly’s death has written to social media companies demanding they hand over information from her accounts, to help find out whether the “accumulated effect” of self-harm and suicide content she had seen “overwhelmed” her.100

Why does online targeting matter?

Democracy and society

1. Benefits

Increasing voter participation

Online targeting can help people stay informed about the things that matter to them, from news about their local area, to changes to national education systems, to humanitarian crises in other parts of the world. It can lower barriers to political debate, activity and organisation, enabling people to communicate with others with similar perspectives and helping them to connect online. It may also have the capacity to improve voter turnout.101

Giving people “reach”

Some online platforms have increased the ability of people across the world to express themselves and form communities of interest. Online targeting systems have a significant impact on how widely users’ posts are distributed among other platform users, and therefore can be seen to amplify people’s posts. These online platforms are increasingly used in communicating information and organising for social action.102 This effect is widely considered to have played a role in democratic movements such as the Arab Spring.103

Improving democratic accountability

Online targeting has the capacity to improve democratic accountability, enabling people to be informed of policy decisions that affect them. By targeting messaging to people most likely to be affected by decisions, it may be possible to facilitate more meaningful communication between the government and citizens, or political parties and voters.

2. Harms

Undermining the news industry and public service broadcasting

Online platforms are widely considered to have had a negative impact on the sustainability of the traditional news media industry.104 Online targeting is a factor in this: through their targeting systems, platforms have a significant influence over traffic to news publishers’ websites, and therefore the level of advertising revenue they can generate.105 Online targeting may also have an impact on public service broadcasting (PSB), as online platforms, unlike broadcasters, are not required to ensure that public service content is easy

102 ‘Plugged In’, Demos, 2018; https://demos.co.uk/project/plugged-in/
103 P Howard, A Duffy, D Freelon, M.M. Hussain, W Mari, & M Mazid, ‘Opening Closed Regimes: What Was the Role of Social Media During the Arab Spring?’, 2011; http://dx.doi.org/10.2139/ssrn.2595096
Why does online targeting matter?

to find. Ofcom has recommended legislation to extend prominence rules to television delivered online, and has proposed that PSB content should be given protected prominence within TV platforms’ recommendations and search results.  

In addition, online targeting may make it harder for the news media to play their traditional role of holding politicians to account. It is likely that the widespread personalisation of online experiences reduces the news media’s ability to identify and scrutinise targeted political messaging.

Online targeting can also stop important news from spreading. For example, in 2014 protests took place in Ferguson, Missouri, in response to a fatal shooting of an African American man by a police officer. This news was extensively debated on Twitter on its then chronological (i.e. non-targeted) feed. However, researchers found the topic was “suppressed” on Facebook’s algorithmically curated News Feed, because it did not meet the criteria for “relevance”.

Polarisation and fragmentation

Online targeting may also lead to social fragmentation and polarisation through “filter bubbles” (which narrow the range of content recommended to users) and “echo chambers” (which recommend content that reinforces users’ interests). Online targeting may also influence the type of online content that people create, as content producers are incentivised to study what types of content is amplified through the online targeting system, and create similar content themselves, increasing people’s exposure to their content and maximising their advertising revenues.

Together with a reduction in scrutiny, this risks an increase in fragmentation and polarisation, as political parties and campaigners are incentivised by the design of online targeting systems to adopt more provocative language or positions that align with their existing supporters’ views on particular issues, rather than seek to persuade people to change their minds. This is problematic, given democracies rely on people being willing to be persuaded.

---


Online targeting systems that seek to optimise user engagement have been shown to prioritise controversial, shocking, or extreme content that produces emotional responses. They have repeatedly been found to play a major role in spreading disinformation and conspiracy theories. The MIT Media Lab found that false news stories are 70% more likely to be retweeted than true stories, and that true stories take about six times as long to reach 1,500 people as false stories. In 2019, Caleb Cain spoke out about his experience of radicalisation which he believes to have been brought about when he “dived deeper” into content recommended to him by YouTube.

Online targeting systems may amplify “harmful” content, and accelerate its spread. For example, from March to June 2018 Daesh/ISIS content on YouTube was regularly seen tens of thousands of times before it was removed from the platform, and Facebook removed original footage of the Christchurch

Why does online targeting matter?

massacre 45 minutes after the video was streamed, by which time it had been viewed some 4,000 times.113 Content that aims to challenge conspiracy theories or extremism can become “drowned out” by recommendations for the very content it seeks to dispute.114 For example, in 2008 a pro-vaccination charity was forced to leave YouTube because anti-vaccine conspiracy theory videos were repeatedly being promoted alongside its content.115

However, while there is reason for concern, there is conflicting evidence about the existence and impacts of “filter bubbles” and “echo chambers”.116 It is not clear to what extent the proliferation of increasingly polarised content is a result of the operation of the platforms’ online targeting systems or of human psychological biases. It is also unclear whether increasingly polarised content results in increased polarisation of users’ political views, or contributes to increased polarisation of public debate more generally.

“Coordinated inauthentic behaviour”

Online targeting systems can also be exploited by third parties, including malicious actors using networks of inauthentic accounts. There is significant evidence that these activities are being carried out by hostile states among others.117 By artificially inflating views, likes, shares, and other metrics, networks of inauthentic accounts can manipulate content recommendation systems to increase the likelihood that certain items of content are recommended more widely.118

There are political and economic incentives for this. First, these approaches allow companies or governments to amplify endorsement of their actions, creating the impression of more genuine support. Second, they can drown out the noise of their opponents without appearing to actively censor dissent. Third, they can weaken opponents by amplifying division. Researchers at the Computational Propaganda Project found evidence of organised political social media manipulation campaigns in 70 countries in 2019, including by state actors.119 Private information operations can be purchased

113 ‘YouTube’s Ongoing Failure to Remove ISIS Content’, Counter Extremism Project, 2018; www.counterextremism.com/press/cep-report-youtube’s-ongoing-failure-remove-isis-content;
Why does online targeting matter?

cheaply. As part of a recent study, for just €300, researchers bought over 3,000 comments, 25,000 likes, 20,000 views, and 5,000 followers, enabling them to identify almost 20,000 inauthentic accounts being used for social media manipulation.120

**Discrimination**

1. **Benefits**

Online targeting is discriminatory by its nature. This can be positive, as under-represented groups can be targeted with information relevant to them that they may otherwise not have seen. Recruitment professionals have highlighted the over-reliance on a standard, default selection of broad-reach media for marketing job vacancies without complementing this through highly-targeted channels, as a major barrier to diverse recruitment.121

2. **Harms**

**Discriminatory targeting of online adverts**

Discriminatory targeting may be harmful, for example, when it reflects existing societal biases embedded in targeting criteria, algorithms, and the datasets that underpin them. In the case of advertising, unlawful discrimination can occur intentionally (where an advertiser chooses to target people based on protected characteristics) or unintentionally (as a result of biases resulting from algorithmic decision making or from the process of “auctioning” adverts).

**Box 3: Discrimination on Facebook**

In 2019, Facebook settled a case brought by the American Civil Liberties Union (ACLU) for bias by allowing advertisers to exclude groups based on race, age and sex from opportunities for housing, employment, or credit.122 Facebook changed its US advertising policies to restrict advertisers from targeting users based on age, ethnicity or gender and limit geographic targeting for opportunities for employment, housing, and credit.123 This restriction also applies to lookalike audiences.

120 ‘How Social Media Companies are Failing to Combat Inauthentic Behaviour Online’, NATO Strategic Communications Centre of Excellence, 2019; www.stratcomcoe.org/how-social-media-companies-are-failing-combat-inauthentic-behaviour-online
122 ‘Facebook Settles Civil Rights Cases by Making Sweeping Changes to Its Online Ad Platform’ ACLU, 2019; www.aclu.org/blog/womens-rights/womens-rights-workplace/facebook-settles-civil-rights-cases-making-sweeping
123 ‘Summary of Settlements Between Civil Rights Advocates and Facebook’ ACLU, 2019; www.aclu.org/other/summary-settlements-between-civil-rights-advocates-and-facebook
Why does online targeting matter?

Research has also shown that online targeting algorithms have discriminated against women and people from ethnic minority groups in the targeting of job ads. This has resulted, for instance, in young women seeing fewer STEM related job ads, and Asian men being more likely to see ads to become taxi drivers.\(^{124}\)

More recently, Neutah Opioitenionne, a 54-year-old woman from Washington, D.C., has alleged that Facebook has deprived her of financial services adverts and information because of her age and gender.\(^{125}\)

Other concerns have been raised about “lookalike” targeting. Through lookalike tools, advertisers do not know which of their customers’ characteristics will be used by the platform to identify other users to target with adverts. They may not be aware that their customers share common features, which could be identified by the targeting system and lead to discrimination or exploitation of people’s vulnerabilities. On the other hand, malicious actors may use lookalike targeting tools specifically to target people with certain shared characteristics without the platform’s knowledge.\(^{126}\)

In the UK, the Equality and Human Rights Commission (EHRC) has confirmed that adverts that are targeted in a way that discriminates against people with a protected characteristic are unlawful.\(^{127}\) Indeed, the UK Parliament’s Joint Select Committee on Human Rights has recently argued that there is a real risk of discrimination against some groups and individuals through online targeting.\(^{128}\) It points out that, unlike traditional print advertising where discrimination may be obvious, the targeting of content online means that people have no way of knowing how what they see online compares to what others see – and therefore whether they have been discriminated against, and on what basis.

---

125 Jonathan Stempel, ‘Facebook sued for age, gender bias in financial services ads’, in ‘Reuters’, 31 October, 2019;
Why does online targeting matter?

**Biased content moderation and recommendation**

There is also a risk that content recommendation systems de-prioritise content produced by people on the basis of their protected characteristics. For instance, content moderation systems employed by major platforms have been found to reflect harmful social biases. Recent studies have shown that leading AI models are 1.5 times more likely to flag tweets written by African Americans as “offensive” compared to other tweets.129

The CDEI is carrying out a separate review of bias in algorithmic decision-making, which is due to be published in spring 2020 with recommendations to the government.

**Conclusion**

Online targeting systems are responsible for determining who sees what content and in what contexts. This can be beneficial in many ways. But in the context of likely upcoming online harms legislation, it is important to be clear that *online targeting influences the severity of risk of harm posed by online content of any type.*

In many cases, the mere existence of legal but potentially harmful content online poses little risk. If a conspiracy video has been uploaded to a video-sharing service but is only seen by 10 people it is unlikely to represent a significant risk. If the same service disseminates the same conspiracy video to millions of people (especially those people who have been predicted to be most likely to engage with it), and if it systematically places the video alongside other, similar content also promoting the same conspiracy, then the risks associated with the video are likely to be much greater.130

Equally, some types of content such as health misinformation pose a high risk of harm if they are targeted at people who may be vulnerable to them, even if they are not viewed by large numbers of people.131

Online targeting systems can cause harm even when the content being targeted does not appear at all harmful. By predicting what content a user is most likely to engage with, online targeting systems may overwhelm people with specific material. This could be manipulative, especially when the people being targeted may be vulnerable, leading them to interact with the content in a way that may be harmful.

---

Why does online targeting matter?

The following table sets out at a high level the role of online targeting in some prominent online harms.

**Table 1: The role of online targeting in a number of online harms**

<table>
<thead>
<tr>
<th>Type of content</th>
<th>Online targeting is less likely to be a feature of</th>
<th>Online targeting is more likely to be a feature of the problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal but harmful content</td>
<td>Trolling</td>
<td>Promotion of extreme, violent content Radicalisation</td>
</tr>
<tr>
<td></td>
<td>Bullying</td>
<td>Disinformation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Polarisation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Exploitation of vulnerability</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(such as the promotion of self-harm or exposure of children to age-gated content)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Bias in content recommendation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unlawful discrimination</td>
</tr>
<tr>
<td>Illegal content</td>
<td>Child sexual exploitation and abuse</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Promotion of terrorism</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hate speech</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Incitement to violence</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Selling of illegal goods</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fraud</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Harassment</td>
<td></td>
</tr>
</tbody>
</table>

132 This broadly aligns with the content-based harms in the OHWP (described as “Harms with a clear definition” and “Harms with a less clear definition”), though also includes economic harms that may occur online, such as fraud and mis-selling.
3. Public attitudes towards online targeting

**Summary**

- We undertook extensive qualitative and quantitative research to explore public attitudes to online targeting.

- Most dialogue participants saw the convenience of online targeting as a desirable feature of using the internet. However, they were concerned about their lack of awareness, understanding, and control over online targeting systems, and about the potential negative impacts of online targeting on people’s lives. Their principal concerns focused on autonomy and vulnerability, and democracy and society.

- Almost all dialogue participants, including the people who were most positive about online targeting, wanted changes to be made to the use and governance of online targeting systems. There was consensus that change is required from online platforms (and other service providers), the government, and users. There is strong public support for increased regulatory oversight of online targeting (61% support regulation and 17% favour self-regulation).

- Dialogue participants typically supported changes that aimed to empower and protect users, to increase transparency, and increase the ability of the government and regulators to hold online platforms to account. They expected these should be introduced proportionately to respect users’ online experience, wellbeing, and rights to freedom of expression and privacy.
Public attitudes towards online targeting

We have undertaken extensive qualitative and quantitative research to explore public attitudes towards online targeting. This chapter is a summary of our findings and we have separately published a full report of this research.

Our research into public attitudes builds on an existing body of research into areas related to targeting. Highlights from previous research, which is reviewed in more depth in our landscape summary of online targeting, published in July 2019, focus on:

- **Awareness**: Awareness is generally low as to how data is used to shape online experience. For example, a 2018 report from Doteveryone found that 45% of respondents were “unaware that the information they enter on websites and social media can help target ads”. It also found that 62% of respondents did not “realise that their social networks can affect the news they see”. The Pew Research Center survey found that around 53% respondents did not understand the role of algorithms in arranging the contents of their Facebook News Feeds.

- **Attitudes**: A Communications Consumer Panel / Ipsos MORI survey on consumer privacy and security found that only 5% of people felt that targeted marketing benefits them a “great deal”, and 43% felt it was neither of benefit or otherwise. Research for Which?’s “Control, Alt, or Delete” report found that “people become more concerned as they learn about the other uses of data, how targeting happens and how the use of the data could affect them”. More recently, research commissioned by Ofcom and the ICO found that the percentage of people who thought that adtech was acceptable fell from 63% to 36% once it was explained to them what it is and how it works.

---

133 In the public dialogue, Ipsos MORI brought together three groups of 30 people over two full-day workshops in Tamworth, London, and Cardiff. Ipsos MORI also convened four groups of special interest of approximately 15 people per group over two evening workshops in Southampton, Falkirk, Newcastle, and Bradford. These groups included: young people aged 16–17; people from minority ethnic groups; people with experience of financial vulnerability; and people with experience of poor mental health. Based on the findings from the public dialogue, Ipsos MORI carried out an online survey to supplement our qualitative analysis. Two waves of online survey research were conducted in December 2019 and January 2020, with a sample of c2,200 adults aged 16–75 living in Great Britain.


137 ‘Many Facebook users don’t understand how the site’s news feed works’, Pew Research Center, 2018; www.pewresearch.org/fact-tank/2018/09/05/many-facebook-users-dont-understand-how-the-sites-news-feed-works/


Public attitudes towards online targeting

Through the public dialogue, we sought to explore people’s attitudes towards online targeting, the benefits and harms it poses, and potential governance solutions that might facilitate beneficial uses and minimise harms. Over the course of the dialogue, participants became more aware and informed, exploring areas of interest in more detail through deliberation, practical exercises, and interaction with experts.

Our findings address people’s views on the benefits and harms of online targeting; and the changes they would like to see over how these systems are governed.

Perceived benefits of online targeting

Most dialogue participants saw online targeting as a desirable feature of using the internet, and integral to the user experience of many different online services. With some exceptions, dialogue participants were generally positive about their own experiences of online targeting. When asked to design their own online services at the start of the dialogue, most dialogue participants built some form of personalisation into their designs. Our polling shows broad support for a range of uses of online targeting, with 54% of respondents finding the personalisation of online adverts acceptable and 68% finding it acceptable to recommend music in apps.

The primary benefit dialogue participants associated with online targeting was the ease of access to relevant information. Dialogue participants also identified other benefits of online targeting. They thought that it could broaden their horizons by showing them content they wouldn’t otherwise have sought out. They thought it enhanced their ability to find like-minded individuals. And they thought that it had economic benefits for people and businesses, by helping people find relevant products and giving them targeted offers or discounts.

These benefits were also seen to extend to public service delivery, with broad support for the responsible use of online targeting by public sector organisations in both the dialogue and survey research. 68% of people believe that public services should use data about people to target their services and advice. Dialogue participants were broadly supportive of online targeting case studies that involved the NHS or other public sector organisations. In both cases, support for online targeting appears highest in cases where it seems to clearly benefit them or other people. But the level of acceptability was also related to their level of trust in the organisation and the invasiveness of the data used to target specific groups.
Concerns about online targeting

However, dialogue participants raised several concerns. In particular, they were concerned about their levels of awareness, understanding and control, and about the potential negative impacts of online targeting on people’s lives. While many of these concerns were raised spontaneously at the beginning of the dialogue, the seriousness of concern grew as dialogue participants’ awareness and understanding increased over the course of the dialogue.

Perceived levels of awareness, understanding and control

1. Awareness and understanding of online targeting

Dialogue participants’ awareness of online targeting was limited. They were aware of personalised adverts and clearly labelled content recommendations (such as music or products marked as “recommended for you”). There was very limited awareness of the use of online targeting systems when it was not obvious or clearly labelled such as content that they see in a social media “feed”.

Dialogue participants’ understanding of online targeting was also limited. They tended to be aware that their browsing activity and location data could shape the adverts and recommendations they see. Beyond this, there were very low levels of understanding about the processes which drive most online targeting systems. The survey research shows only 7% of people believe that information about who people interact with online could be used in online targeting systems.

As their understanding grew, all dialogue participants reported being shocked at the prevalence and sophistication of online targeting systems, including those who described themselves as “data savvy”.

2. Control over online experiences

Dialogue participants perceived a lack of control over their online experiences. Few participants had heard of the various facilities to change their preferences and settings provided by many online services. When asked to attempt to change their settings on a number of major online platforms, most dialogue participants found them difficult to find and to use, and some failed this task outright. They reported finding user controls difficult to find, complicated in their layout, biased and positive in their language in favour of online targeting, and overly burdensome to navigate. Many dialogue participants thought that user controls were purposefully designed this way.

The survey shows only 36% of people believe they have meaningful control over online targeting systems. In part, this is driven by a low level of belief that companies will do what users request through their settings and preferences (only 33% believe this is the case). The graph below shows the level of trust in several major social media and video-sharing platforms to use targeting responsibly.
Dialogue participants also perceived a **lack of choice** in many aspects of their online experiences. Many felt that there were no “real” alternatives to major platforms like Facebook and Google, and that they had no choice but to accept their terms and conditions. They also showed limited awareness of products that might increase their privacy, such as “incognito” browsing or competitor search engines like DuckDuckGo.

### The impacts of online targeting

Dialogue participants were concerned about the potential negative impacts of online targeting on people’s lives. Some were primarily concerned with the way data is collected and processed to support online targeting, which they viewed as an invasion of privacy and infringement on data rights. However, beyond issues of privacy and data protection, dialogue participants were concerned about a range of other issues. Their key concerns typically focused on the impact of online targeting on autonomy and vulnerability, and democracy and society.

These concerns were mirrored by the results of survey analysis showing significant variation in people’s views about the acceptability of targeted advertising based on the circumstances. This relates to their trust in the organisation, support for the objectives of the targeting, and acceptance of the way that data is being used. For example, four-in-five (82%) people believe it would be acceptable for the NHS to target people to encourage them to get a flu jab, whereas one-in-five (19%) believe it would be acceptable for a gambling company to target people most likely to want to place a bet.
Autonomy and vulnerability

Dialogue participants were concerned about the potential for online targeting systems to undermine people’s autonomy and influence their behaviours or attitudes. They thought that online targeting systems might identify and exploit people’s first-order preferences (or their “susceptibilities”). They were also concerned that people’s attitudes or behaviours could be influenced through sustained exposure to particular perspectives or content.

Dialogue participants’ key concern was the potential for online targeting systems to exploit vulnerable people. They generally viewed groups such as older and younger people, people with poor mental health or addictive tendencies, and people with limited financial capability as vulnerable. They thought that vulnerable people have limited capacity to make informed judgments and are more likely to be unduly influenced by online targeting systems. Dialogue participants rarely considered themselves vulnerable, but as discussion developed they did begin to challenge this initial perception and consider the extent to which online targeting systems might be able to identify more transitory vulnerabilities that most people experience, like bereavement.

Democracy and society

Dialogue participants had some concerns that online targeting systems could reduce the range or variety of information and perspectives that people see. With regard to news and political messaging, most thought that this represents a risk to the democratic process. Some thought that this could lead to wider social fragmentation, although this view was not shared by all dialogue participants.
Dialogue participants’ other principal concern was that online targeting systems could expose people to “problematic” content, especially where content is targeted to maximise user engagement. They thought that the cumulative and sustained impact of exposure to “problematic” content increased risks of polarisation and radicalisation significantly. This was supported with real examples given by some dialogue participants about close family members developing extreme views towards anorexia and conspiracy theories, which they associated with the use of online targeting systems.

**Appetite for change**

Almost all dialogue participants wanted change to how online targeting systems work and are governed to minimise the risk of harms posed by online targeting. Given the seriousness of their concerns, dialogue participants expected action to be taken quickly.

**Differences in dialogue participants’ appetite for change**

Dialogue participants could be broadly divided into three groups, based on their appetite for change. These groups differed in terms of the extent and nature of change they thought needed to happen.

The majority of dialogue participants saw significant value in online targeting systems but were sufficiently concerned about them that they were unsure whether they supported their use. If steps could be taken to resolve their concerns, they would likely become supportive of online targeting.

There were a smaller number of dialogue participants who were clear that the benefits of online targeting outweigh the harms (although most still wanted change). These people typically placed significant value on the positive role of technology in everyday life. At the other end of the spectrum, a similar proportion of dialogue participants believed that the harms of online targeting outweigh the benefits. This belief was largely driven by concerns about privacy and data protection.
Change required from companies, the government, and users

Dialogue participants thought that change needs to come from users themselves, online platforms, and the government. For online targeting systems to work in the best interests of users and wider society, they thought that these actors all need to make coordinated and complementary changes.

There was broad consensus that people should be considered responsible for their online behaviour, but that for this to work they need to be genuinely empowered to understand and control their experience, and there should be support for vulnerable people.

Dialogue participants generally agreed that significant changes were required in the design of online services and the information and controls afforded to users. Given the prevalence and complexity of decisions and judgments people have to make online, dialogue participants also thought that companies should reduce the burden on users, for example by reducing the prominence of “problematic” content.

However, dialogue participants did not trust online platforms to act in the interests of individual users or society more widely. They thought that it was critical for the government to direct online platforms to change, and to scrutinise and enforce this work. This would require increasing the level of transparency afforded by online platforms and the government’s powers to hold them to...
account. Dialogue participants also raised concerns that giving too much power to the government risked having a negative impact on the rights of individuals to express themselves and to access content freely online.

Survey respondents overwhelmingly (61%) favour giving an independent regulator oversight of the use of online targeting systems, rather than self-regulation (17%).

Figure 10: Dialogue participants’ views of the responsibilities of individuals, companies and the government

Solutions
Dialogue participants considered a range of changes that might address their concerns. They typically supported changes that aimed to empower and protect users, to increase transparency and to increase the government’s ability to hold online platforms to account. In this context, they wanted more information to be available across society to scrutinise the operation and
impacts of online targeting systems. Establishing an appropriate mechanism for independent scrutiny of online platforms to help ensure they are working in the best interests of users was seen as a priority.

However, they also identified both pragmatic and principled limits to the steps that should be taken to minimise risks of harm. This was particularly the case where proposed changes risked having a significantly negative impact on users’ experience, wellbeing, or rights. In particular:

- Dialogue participants valued their user experience and wanted changes to create as little additional friction as possible. In spite of this, dialogue participants reacted positively when shown a mock-up stimulus to illustrate how features that might give users more information and control could look and work in practice.

- They were also concerned that new rules should not impinge on people’s ability to access content and express themselves online. They generally favoured reducing the prominence of “problematic” content, rather than taking it down or banning it altogether.

- They were positive but cautious about suggestions that online platforms should proactively identify and support vulnerable groups, due to privacy concerns, risks of false positives and negatives, and other possible unintended consequences.

Figure 11: Example prompt for information reported as unreliable by users

141 'Public Attitudes Towards Online Targeting', CDEI, 2020; www.gov.uk/government/publications/cdei-review-of-online-targeting
Awareness, understanding and control
168 Dialogue participants were clear that they saw increased levels of awareness and understanding as critical for user empowerment. They thought that greater transparency for users about when online targeting was taking place, and clearer information on the source and nature of the content, would help dialogue participants make informed decisions about how they engage with it.

169 Dialogue participants wanted more control over online targeting systems. They called for simple and digestible consent mechanisms and easy to use, accessible settings which would ideally be interoperable between platforms or services.

Autonomy and vulnerability
170 Dialogue participants suggested that online targeting systems should not be designed to maximise user engagement and welcomed change that would align the content recommended to them with their true interests.

171 Dialogue participants also wanted companies to do more to encourage and facilitate healthy online behaviour. They supported the use of tools such as time reminders or alerts to suggest that users spend less time doing certain activities online. For groups they thought would be vulnerable, dialogue participants thought that the default settings for online targeting systems should be “off”, along with settings for alerts and notifications.

172 Dialogue participants were supportive of features that would enable people to make online platforms and other service providers aware of their age and other vulnerabilities safely and privately; ideally, such features would also be interoperable between platforms or services. In some circumstances, most dialogue participants were willing to accept a level of risk-based monitoring of users by online platforms to identify potential vulnerabilities and risky behaviours. They wanted solid safeguards in place to prevent undue invasion of privacy and unfair uses of data, and to impose clear transparency, control, and appeal mechanisms.

Democracy and society
173 Dialogue participants welcomed changes that would make content recommendation systems provide balanced information and represent the full range of views and sources.

174 With regard to targeted online political advertising, although dialogue participants thought that users should exercise diligence, they also expected online platforms to support users by enabling wider scrutiny of political messaging, for example through the use of advertising libraries. The survey shows 40% of people believe that targeted online political advertising has a negative impact on people’s voting intentions (compared to 29% who think that it has a positive impact).
Dialogue participants initially wanted to ban “problematic” online content (such as extreme, violent, or unreliable content), but support for this subsided through deliberation. This was largely due to dialogue participants’ views that users should generally be able to access and publish content freely online, and concerns over who would decide what content should be classified as problematic.

However, most dialogue participants expected companies to do more to identify and reduce the prominence of “problematic” content. They were clear that people should be responsible for managing their own online experiences, but expected companies to help users evaluate the content they engaged with critically and to provide useful information about its source and reliability, including through informational cues such as pop-ups where appropriate (for instance when uploading or accessing potentially harmful content). There was also some support for notifications or alerts in cases where users display risky behaviours such as viewing a large volume of extreme content.

Discrimination

Unlawful discrimination caused by the targeting of online advertising was not a concern raised in the main workshops, but was explored further in a small number of follow-up depth interviews. Participants in these interviews were unanimous in their view that efforts should be made to make discrimination of this kind impossible and expected there to be a mechanism in place to establish whether the law has been broken if concerns are raised. However, participants had mixed views on the extent to which this was a concern that required further changes, given that there is already relevant legislation in place.

Conclusion

The findings of this research are highly relevant to our review, as well as to others’ work. Dialogue participants’ key priorities included improving people’s understanding and control over online targeting systems, protecting vulnerable people and improving government’s ability to scrutinise online targeting systems and hold online platforms to account.

In the next chapter, we outline our research into the current regulatory environment in the UK and its appropriateness for dealing with the issues posed by online targeting.
4. The regulatory environment

Summary

- The UK has developed a number of systems of independent expert regulation that play a role in online targeting. But regulatory coverage of online targeting is incomplete and self-regulation will not address the risks we have identified:
  - Data protection has a significant role to play in addressing some of the risks posed by online targeting, but the regulation of online harms requires decisions that may go beyond the scope of data protection legislation.
  - Competition and online harms regulation may help to prevent specific harms, but the current regulatory environment cannot tackle many of the risks posed by online targeting.
  - The proposed online harms framework could help to close the gap in regulation, but only if online targeting is recognised within the independent regulator’s remit. And that still leaves gaps in the regulation of political advertising and advertising.
  - The UK needs new regulation to address the risks of online targeting. Developments in regulation in the UK and elsewhere may be relevant for designing online targeting regulation, as may market developments, particularly the data intermediary model.
The regulatory environment

In this chapter we set out our analysis of the regulatory arrangements relevant for online targeting. The UK does not have a specific regulator responsible for overseeing use of online targeting systems. But there are a number of regulators whose powers and duties are relevant to online targeting in some way.

Regulatory coverage of online targeting is currently incomplete. We identify gaps in the regulation of online targeting and discuss some of the challenges involved in regulating online targeting.

The current regulatory framework

In the following paragraphs we set out a high-level summary of the current regulatory framework relevant for online targeting. We include a more detailed review of current regulation at Appendix 4 of this document.

The regulators that may be relevant for online targeting are:

- The Information Commissioner’s Office (ICO)
- The Competition and Markets Authority (CMA)
- The Advertising Standards Authority (ASA)
- The Office of Communications (Ofcom)
- The Financial Conduct Authority (FCA)
- The Gambling Commission
- The Electoral Commission
- The Equality and Human Rights Commission (EHRC)

The ICO is the UK’s independent regulator for data rights. It is responsible for the implementation and enforcement of the Europe-wide General Data Protection Regulation (GDPR) in the UK. All forms of online targeting involve some, if not all, of the features of data processing specified in the GDPR, so the ICO is an important part of the current regulatory framework around online targeting. A clear example of this is the ICO’s recent publication of its age appropriate design code (see Box 4). The ICO is also currently assessing the adtech ecosystem that supports personalised online advertising. The ICO has a cross-sectoral remit and coordinates closely with other regulators.

142 ‘Age appropriate design: a code of practice for online services’, Information Commissioner’s Office, 2020;
The regulatory environment

Box 4: The ICO’s age appropriate design code

The ICO is required to produce an age appropriate design code of practice to give guidance to organisations about the privacy standards they should adopt when they process children’s personal data, for example for social media, online gaming and connected toys.

Following the code will help online platforms ensure they are compliant with the GDPR, which provides that children “merit special protection with regard to their personal data”.

The code is based around a set of 15 standards that online platforms should meet to protect children’s privacy. Of particular relevance for the applications of online targeting that we consider in this report is the profiling standard. This means that unless the provider can demonstrate that profiling is essential for providing “core services” (the service would not work without it), it must be switched off by default.

The ICO identifies some cases where profiling may be acceptable even where it is not essential for providing core services, for example ensuring that services are accessible to disabled users, or personalising news content (as children have the right to access information). The ICO also identifies the potential of profiling to support the best interests of children, for example to “help establish or estimate the age of a user”.

The CMA is an independent non-ministerial government department. It has a statutory duty to seek to promote competition for the benefit of consumers across all sectors. Under its digital markets strategy, the CMA is conducting a review of online platforms and digital advertising and has published an interim report which concluded that:

- Lack of competition may be preventing market entry, leading to lack of choice and higher prices for consumers, and may potentially be undermining the viability of publishers including newspapers.

- Default settings (for example, Google as the standard search engine on Apple devices) strengthen market positions, as does the collection of personal data, which allows Google and Facebook to target ads more effectively.

- Users do not feel in control of their data: they can’t always opt out of personalised advertising and find it difficult to access privacy settings. This means most people use default settings, which may result in them giving up more data than they would like.143

185

143 ‘Online platforms and digital advertising market study’, Competition and Markets Authority, 2019; www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study
The ASA regulates advertising in all media. It is funded by industry and is largely self-regulatory. Personalised online advertising is covered by the rules in the CAP code. Advertisers, not the online platforms they use to advertise, are primarily responsible for following the CAP code, but publishers and other intermediaries share a secondary responsibility for compliance. The ASA’s current strategy aims to improve the regulation of online advertising. It does not regulate political advertising. The ASA is responsible for regulating advertising on on-demand programme services, and this is expected to extend to advertising on video-sharing platforms with the new provisions in the AVMSD (see below).

Oftcom is the independent regulator for broadcasting, telecoms, post and the radio spectrum. Its remit includes:

- Protecting the public from “offensive and harmful” material in television and radio broadcasting.

- Implementation in the UK of the Europe-wide Audio-visual Media Services Directive (AVMSD) which currently imposes requirements for online broadcasters in relation to harmful material and will impose separate obligations on video-sharing platforms from 2020.

- Promoting media literacy via its Making Sense of Media programme.

- Protecting the interests of consumers in communications markets, particularly through its Fairness for Customers programme.

- Competition regulation in communications markets.

The FCA regulates financial services firms and financial markets in the UK. It has rules which require financial services firms to ensure that their financial promotions are clear, fair and not misleading. It regulates a large and valuable sector and has experience of regulating markets that rely on large-scale use of data-driven systems. Its approach to vulnerability may also be a good model for harms caused by online targeting, where feedback loops mean that content recommendation systems can inadvertently target users’ vulnerabilities (as we discussed in Chapter 2).

The Gambling Commission regulates gambling providers in Great Britain and works in partnership with the ASA and others to secure responsible advertising of gambling. It collects data and conducts research on the impact of (online) advertising on children, young people and vulnerable people.144

The regulatory environment

The Electoral Commission oversees elections and regulates political finance in the UK. Targeted online political advertising presents challenges for the Electoral Commission's campaign finance role, as it makes it more difficult to identify the source of funding, and whether adverts are compliant with registration and spending requirements.

The Equality and Human Rights Commission (EHRC) is a statutory body responsible for enforcing the Equality Act 2010 and encouraging compliance with the Human Rights Act 1998. Targeted online job adverts could unlawfully discriminate against people on the basis of the protected characteristics defined in the Equality Act 2010. This is relevant for the EHRC as one of its goals is to ensure that people have equal access to the labour market and are treated fairly at work.

Other regulation in the UK

1. European regulation

The AVMSD gives Ofcom a role in regulating online content. The e-Commerce Directive, which sets Europe-wide rules for online markets including transparency and information requirements for online service providers, provides for certain liability protections for online platforms acting as "intermediary service providers" where they host user-generated content neutrally. EU copyright rules (the Directive on Copyright in the Digital Single Market and Directive on television and radio programmes) have recently been updated. The Directive on combating terrorism requires online platforms to take down terrorist content.

2. Self-regulation

The broader regulatory framework for online targeting includes rules that have been voluntarily adopted by the industry without statutory direction, which we refer to as "self-regulation".

The platforms have developed their own policies (Facebook Community Standards, YouTube Community Guidelines, Twitter Rules and so on), which address potential online harms, including harms that may be caused or exacerbated by online targeting. These policies reflect the nature and ethos of the platforms, and so vary considerably. But they have some common elements: for example, platforms generally have policies that restrict the targeting of content about self-harm and suicide.

145 In relation to the hosting of content, online platforms are protected so long as they have no actual knowledge of illegal activity or information or where, upon obtaining such knowledge, they expeditiously remove or disable access to the content.

The regulatory environment

Other self-regulatory initiatives include:

- Facebook is setting up an Independent Oversight Board, with the power to make independent binding judgments about content. It will be funded by Facebook but set up as an independent entity. Facebook has also partnered with third-party fact-checking services, including FullFact and FactCheckNI in the UK, to tackle the spread of misinformation.147

- The Data Transfer Project, launched in 2018, aims to build “a common framework with open-source code that can connect any two online service providers, enabling a seamless, direct, user initiated portability of data between the two platforms.” Current contributors include Google, Facebook, Microsoft, Twitter and Apple.148

- As we discuss in our recommendations chapter below, Facebook has also developed a partnership called Social Science One to offer academic researchers privacy-preserving access to Facebook’s data.

There are also some coordinated self-regulatory initiatives that have been adopted by a number of platforms. Examples include the ASA system (and equivalent models in other countries) and the European Commission’s Code of Practice on Disinformation, which was developed by the European Commission but adopted on a voluntary basis by platforms including Facebook, Google, Twitter and Microsoft. The Code of Practice on Disinformation attempts to address the spread of online disinformation and “fake news”, and includes commitments such as the establishment of publicly accessible political advertising archives.149

Future regulation

The regulatory framework is not fixed. As well as the Online Harms White Paper150 (see Box 5), the UK government has committed to looking at how to establish a Digital Markets Unit to support greater competition and consumer choice in digital markets,151 following a recommendation made by the independent Furman report. Technological change and innovation may lead to new applications for online targeting, which could fall within the scope of other regulators not considered in our analysis. And under the current regime, case law from enforcement of GDPR and competition law will continue to develop.

148 ‘Data Transfer Project’, 2018; https://datatransferproject.dev/
Box 5: The Online Harms White Paper

The 2019 Online Harms White Paper (OHWP) set out the UK government’s plans for online safety measures that also support innovation and a thriving digital economy.

It proposes establishing in law a new duty of care towards users, overseen by an independent regulator. The proposed duty of care will relate to services that facilitate hosting or sharing of user generated content or user interaction.

The OHWP identifies several categories of online harm: “Harms with a clear definition” (content and activities that tend to be illegal under UK law already), “Harms with a less clear definition” (potentially harmful, but not illegal) and “Underage exposure to legal content” (children accessing inappropriate material).

The government proposes that the regulatory framework should apply to all companies that allow users to share or discover user-generated content or interact with each other online. It proposes that the regulator will take a risk-based and proportionate approach. This will mean that the regulator’s initial focus will be on those companies that pose the biggest and clearest risk of harm to users, either because of the scale of the platforms or because of known issues with serious harms.152

Review of Online Advertising Regulation

The UK government has also announced a review of online advertising regulation.153 The review will assess the impact of the online advertising sector on both society and the economy, and will consider the extent to which the current regulatory regime is equipped to tackle the challenges posed by rapid technological developments seen in online advertising. We welcome its recent publication of a call for evidence, in particular the focus on vulnerability and discrimination.154

The regulatory environment

How effective is current regulation?

The UK has developed a number of systems of independent expert regulation that play a role in online targeting. Horizontal regulators such as the ICO and CMA help to secure a consistent and balanced approach across all sectors. Sectoral regulators including Ofcom have developed deep knowledge of the industries they regulate. Guidance and enforcement decisions provide clarity to regulated organisations, while the right of appeal (and specialist courts such as the Competition Appeal Tribunal) has led to case law that informs best practice by regulators.

Regulation has developed in all sectors to reflect the growing importance of the online world, as our summary of the current framework shows. But it does not yet address many of the risks posed by online targeting systems set out in Chapter 2. Online targeting also presents specific challenges for regulation:

- By its nature, online targeting is not transparent to users or regulators. As people may not even be aware that they are being targeted, individual complaints may not be a good indicator of the nature or scale of any harms. And targeted online content cannot be subject to public scrutiny in the same way as broadcast content or the press. This means that regulators may have limited visibility of any problems. Transparency provisions in the GDPR require transparency to users over data processing, but in implementation to date this has often been limited.

- Online platforms are international businesses. Regulators in Europe have limited influence in Silicon Valley or Beijing. In the EU, companies may not be regulated in the same country as their users and the future of these arrangements now that the UK has left the EU is still to be determined.

The limits of self-regulation

While the platforms have developed their own systems to establish accountability and protect users, self-regulation alone may be insufficient to address these challenges. The French government commissioned an “inter-ministerial mission team” to explore a general framework for the regulation of social media, relying on the voluntary cooperation of Facebook. The team of eight, led by Benoît Loutrél (a former Director General of the French communications regulator ARCEP), worked with Facebook over several months to carry out the research for its report. The team’s report identified the limits of self-regulation:155

- Information asymmetry: the “extreme asymmetry” of information between platforms and regulators means public authorities and civil society organisations have access to “practically the same level of information

155 ‘Creating a French framework to make social media platforms more accountable: Acting in France with a European vision’, Direction interministérielle du numérique et du système d’information; 2019; https://minefi.hosting.augure.com/Augure_Minefi/fr/ContenuEnLigne/Download?id=AE5B7ED5-2385-4749-9CE8-4E1B36973E48&filename=Mission%20%e0%CC%81gulation%20des%20re%CC%81seaux%20sociaux%20ENG.pdf
as a user”. They do not have the information they need to carry out objective analysis, particularly given the role of algorithmic processing. This makes it difficult to establish whether and to what extent platform systems and processes may be leading to harm to users: in the words of the report, “to prove the existence of a systemic failure [to protect users] by the platform.”

- **Inward-looking**: the platforms “hold all the cards: they draw up their terms of use, decide to what extent to be bound by them, modify them as necessary without any public formalities, interpret them without the possibility of appeal and report on their implementation in the form and frequency they consider appropriate.” No external agency has the ability to assess objectively whether platform approaches to address online harms are appropriate or effective.

- **Incentives not aligned with public policy**: the platforms take action to manage their reputation and avoid regulation, rather than to address public policy objectives.

### The limits of current regulatory environment

1. **Online harms**

   The AVMSD will impose new obligations on video-sharing platforms (VSPs) from 2020. It will require VSPs to develop systems to protect their users rather than regulating the content of VSP services, because VSP service providers do not have editorial control of the content (this is in contrast to the detailed standards that apply to broadcasters, as set out in Ofcom’s Broadcasting Code). The rules for VSP services cover protection of children, incitement to hatred, product placement and sponsorship, terrorism and pornography.

   Platforms (including VSPs) will not be subject to regulation in relation to other user-generated content. In addition, Facebook and YouTube are regulated in Ireland. Following the UK’s withdrawal from the EU, UK regulators may need to coordinate closely with their European counterparts to reflect the interests of UK users.

   **The UK government’s proposed independent online harms regulator could provide regulatory coverage** for risks posed by the targeting of content online, if its remit and duties are scoped accordingly.

2. **Data protection**

   The processing of personal data, which is regulated under the GDPR and the Data Protection Act 2018, drives online targeting. The ICO also enforces the Privacy and Electronic Communications Regulation (PECR), which give people specific privacy rights in relation to electronic communications including cookies and similar technologies.
The regulatory environment

The ICO has outlined that, among other things, data protection regulation aims to ensure that personal data about people stays safe, and is only used in ways that people would expect and can control. The GDPR safeguards individual rights, and aims to provide individuals with transparency over the processing of personal data. It requires that data is processed fairly, in ways that are not unduly detrimental, unexpected or misleading to the individuals concerned. Its accountability provisions make data controllers responsible for demonstrating compliance with the GDPR, following data protection by design and by default principles, and carrying out data protection impact assessments.

The ICO has recently published its age appropriate design code and a draft framework code of practice for the use of personal data for political campaigning, both of which are clearly relevant to online targeting. It is also conducting an investigation into real time bidding and adtech.

Under the age appropriate design code, online platforms should by default switch off features that rely on profiling for children, unless there is a compelling reason to do otherwise. Where profiling is on, platforms should put appropriate measures in place to safeguard children. The ICO considers that under data protection law, organisations are responsible for the content they target and recommend to children online when this is based on personal data about them. This means that online platforms should not promote harmful content (such as adverts that are contrary to the CAP code provisions on marketing to children, or pro-anorexia content generated by users) or encourage harmful behaviours to children (such as through strategies to extend user engagement).

However, while the ICO has a significant role to play in addressing some of the risks posed by online targeting, there are limits to the effectiveness and appropriateness of data protection regulation. The government’s Online Harms White Paper notes that the increased use of data and AI is giving rise to complex, fast-moving and far-reaching issues that cannot be addressed by data protection laws alone. We believe that there are two principal reasons for this: the need for regulation to consider harmful content together with the way it is targeted; and the reliance of data protection regulation on individual consent and control (albeit within a broader framework of accountability).

---

157 The ICO explains that data controllers exercise overall control over the purposes and means of the processing of personal data, and have the highest level of compliance responsibility. ‘Controllers and processors’, Information Commissioner’s Office; https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/processors-and-processors/
159 The Secretary of State is now required to lay the age appropriate design code before Parliament as soon as reasonably practicable for its approval, following which it will come into force.
The regulatory environment

The scope of data protection regulation

209 The ICO already has a broad, cross-sectoral remit. It is focused on the challenge of overseeing new legislation: the interpretation and application of the GDPR is still evolving; case law under this legislation remains limited; and organisations and the public are still adapting to the new regime. Along with other regulators, it is likely to have to adapt following the UK’s withdrawal from the EU. The UK government has said that the ICO will continue to be the independent supervisory body regarding the UK’s data protection legislation, and that it will continue to work towards maintaining close working relationships between the ICO and the EU supervisory authorities.161

210 With regard to online targeting, the ICO is responsible for overseeing online targeting practices that are inconsistent with data protection legislation. As such, the Online Harms White Paper recognises that harms suffered by individuals that result directly from a breach of data protection legislation will be out of scope of the proposed online harms regulator.

211 However, the ICO does not have the remit to address other online harms. As set out in Chapter 2, the way that online content is targeted is an intrinsic feature of many online harms. The regulation of online harms requires setting standards and guiding industry to define “good” content recommendation or mitigate associated risks; assessing compliance with these standards; and making judgments about the appropriate balance between privacy and other human rights, notably freedom of expression, in relation to the targeting of online content. These decisions may go beyond the scope of protection legislation.

Individual consent and control

212 The CMA reports that it is essential for regulation to put consumers in control of their own data. This would enable people to make informed decisions about whether and how they use online platform services, which they pay for with their attention and data.162

213 While there are a number of requirements for processing personal data under the GDPR (including compliance with fairness and accountability principles), GDPR requirements for processing based on consent are of particular importance in the context of online targeting.

214 Consent is particularly important in relation to online targeting. Where targeting relies on the use of cookies and similar technologies, PECR requires that people consent, as the ICO clarifies in its update report on its investigation into real time bidding and adtech, and its guidance on the use of cookies. Where targeting does not rely on the use of cookies and similar

162 ‘Online platforms and digital advertising market study’, Competition and Markets Authority, 2019; www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study
technologies (and therefore PECR does not apply), consent is still likely to be the appropriate basis for processing in practice, though this depends on the specific circumstances.

However, people are not often able to give meaningful consent in practice. As discussed in Chapter 3, participants in our public dialogue generally felt that they could not control how their data is used online. This view is reinforced by the CMA, which found in its market study that:

- Consumers have some control over their data, but frequently platforms do not give them full control and some do not allow consumers to turn off personalised advertising.

- Consumers are served with personalised advertising by default, making it difficult to exercise what controls they do have due to a strong tendency to accept default settings presented by platforms. This nudges consumers to make choices that are in the best interest of the platforms.

- Consumers must engage with long, complex, terms and conditions, and must make several clicks to access their settings. Consumers rarely engage with these terms and when they do, they spend very little time reading them.

- Platforms do little to measure user engagement with their policies or test what would increase it. They rely on the fact that very few consumers alter the default settings to increase their ability to use personal data.

Our analysis of public attitudes suggests that there is limited awareness of data rights. If people do not know their rights, they are unlikely to report any breaches or harms that they have experienced. In addition, there is a limit to people’s ability to understand the data processing involved in many online targeting systems, which can be highly complex. People are also largely unable to assess how the use of personal data about them in online targeting systems is likely to impact them. Expecting people to make informed judgments about consent in these cases is unreasonable.

Even when people give meaningful consent to the use of personal data about them, online targeting systems can still cause harm. For instance, a content recommendation system may show people the content they want to see in a given moment, but over time this may lead to potentially harmful effects the user has not consented to, such as being drawn into a filter bubble.
3. Competition

The Furman report considered the state of competition in digital markets in the UK and made recommendations to change competition policy and regulation. The government has committed to looking at how it can implement the recommendation to create a new Digital Markets Unit.

The CMA, in the interim report of its online platforms and digital advertising market study, also considers three categories of possible interventions to improve competition. In its final report, it will make formal recommendations to the government, which will then decide next steps. Its three categories of intervention are:

- Rules to govern the behaviour of platforms with market power, including an enforceable code of conduct for firms with “Strategic Market Status” as recommended by the Furman report.
- Rules to give consumers greater control over data and to improve transparency.
- Interventions to address market power and promote competition (including data access, consumer default, interoperability and structural interventions).

The CMA is also developing recommendations to the government on the development of an ex ante pro-competitive regulatory regime to regulate the activities of online platforms. This would update the UK’s regulatory environment for competition in digital markets.

While competition regulation may lead to improved outcomes for consumers, it may be less effective in addressing some of the risks posed by online targeting systems. For example, it is unclear whether more competition will incentivise online platforms to sufficiently address the risks their systems pose to users, at least in the short term. Greater competition between online platforms may create an incentive to improve user safety, leading to the implementation of widespread measures to reduce the spread of disinformation. Equally, competitive pressure may lead to a race to the bottom, with high user engagement prioritised over user safety.

The GDPR may also act against initiatives to support competition. The CMA and others note that some stakeholders believe that data protection regulation may unduly favour the business models of large, vertically integrated platforms over smaller publishers. The CMA notes that some proposed interventions to increase competition, such as requiring Google to provide click and query data to third-party search engines, may create risks to people’s privacy, and states that competition and data protection authorities should consider jointly the interface between consumer, competition and data protection law. The ICO and the CMA are engaging constructively on this issue as part of phase two of the CMA’s market study.

163 Madhumita Murgia, ‘Backlash over sweeping UK regulations to protect children’s data’, in ‘Financial Times’, 22 January 2020; www.ft.com/content/7abc452c-3d38-11ea-a01a-bae547046735
4. Political advertising

While several regulators have a role in regulating political advertising, there are significant regulatory gaps. As recognised in the ICO’s draft framework code of practice, political campaigning has become increasingly sophisticated. The ICO regulates the use of personal data for political campaigning and has carried out enforcement action. However, online targeting may facilitate non-compliance with political financing regulations as it allows groups to quickly set up and spend on election materials with limited oversight or audit: the same group could be funding different campaigns simultaneously with no obvious link between them. People who are targeted by a cause they are likely to support are also possibly less likely to report this to a regulator.

The Electoral Commission’s role is to oversee political finance in election campaigns. Spending on campaign activity must be provided to the Electoral Commission under broad categories such as “advertising”. The Electoral Commission says that this broad category makes it hard to know the value, time period, and location of campaigners’ digital advertising. The Electoral Commission cannot require the platforms to collect or share data on how online political adverts are targeted, so researchers and campaigners do not have enough information to understand how campaigns are using online targeting.

There are other types of online political advertising that are not regulated by the Electoral Commission. This includes targeted advertising by advocacy groups and lobbyists that is not campaigning for an explicit electoral outcome, but is intended to influence legislative or other forms of political change. The government’s Registrar of Consultant Lobbyists, which is intended to increase transparency of lobbying companies, does not require lobbyists to declare their spending on digital campaigning.

There is no content regulation for electoral advertising, including online. The Committee of Advertising Practice and Electoral Commission have both warned against content regulation for electoral advertising, citing concerns over freedom of expression and the subjectivity of political claims. ASA rules requiring claims to be “legal, decent, honest and truthful” apply to other political adverts that are not intended to influence voters in elections or referendums.

Existing regulation does not meet public expectations for more transparency over political advertising. Transparency is essential for the “marketplace of ideas” of a democracy to function. Politicians make countervailing public claims, and media and civil society hold them to account, with the voters having

---

167 ‘Who regulates political advertising?’, House of Commons Library, 2019; https://commonslibrary.parliament.uk/insights/who-regulates-political-advertising/
The regulatory environment

the final say. However, there is no regulation requiring transparency in political advertising, making it harder for claims to be held to account. The Electoral Commission has called on the government and social media companies to make it clear to voters who is paying to influence them online.168

The major platforms that allow political advertising have responded to pressure by introducing publicly accessible political advertising archives which include the content of adverts. However these have only received limited support. They are criticised for providing insufficient information about how adverts are targeted and, in the case of less well known campaign groups, who paid for them.169 In addition, there are inconsistencies between the technical standards on platforms. This makes it harder for media and researchers to meaningfully analyse the thousands of political adverts that are placed.170 Finally, the platforms adopt different definitions of “political”, meaning that different types of advertising appears in archives. Some platforms have highlighted the problems of self-regulation.171

Our recommendations, set out in Chapter 5, include measures to improve the transparency of political advertising.

5. Commercial advertising

The ICO regulates the use of personal data for targeting adverts online. Its current work on real time bidding in programmatic advertising is considering how data is collected and shared in the advertising industry. Beyond data protection, the ASA regulates the content and targeting of online adverts.

The ability to use online targeting systems is available to all advertisers at low cost. This has created a “long tail” of small advertisers, which may have less incentive to comply with the ASA’s rulings than companies with big brands to protect. Online targeting systems can also be used by actors based abroad, reducing the effectiveness of the ASA’s reputation-based sanctions (and any statutory decisions, for example by the Gambling Commission, Trading Standards).

170 ‘Facebook and Google: This is What an Effective Ad Archive API Looks Like’, Mozilla, 2019; https://blog.mozilla.org/blog/2019/03/27/facebook-and-google-this-is-what-an-effective-ad-archive-api-looks-like/
Online targeting makes breaches of the ASA’s rules more difficult to detect. As with other regulators, the smaller the audience, the less likely someone is to complain and the more difficult it is to identify breaches of compliance with the CAP code. This is made more challenging given that targeted adverts may be difficult to find after the event, and it is not easy to verify who was targeted with the adverts. This could make it challenging for the ASA to demonstrate that an advert was targeted inappropriately. As we discuss in Chapter 5, the ASA has begun to develop new approaches to attempt to address this challenge, though these are limited in their effectiveness (see Box 6).

Online advertising platforms are not regulated under the ASA system (which is different to broadcasting, where the channel hosting the advert is responsible for ensuring compliance with ASA rules). But the ASA needs the cooperation of the platforms to effectively regulate online advertising. It relies on voluntary provision of information by the platforms to assess the compliance of adverts targeted using their systems, particularly as advertisers may not have accurate information about who their adverts reached. It also relies on platforms to raise awareness of the provisions of the CAP code among the “long tail” of small advertisers referred to above. The ASA’s voluntary funding model has not changed sufficiently to take into account the development of the online advertising market, the role of the platforms and the long tail of small providers.

The following table summarises regulatory coverage in each of the thematic areas we discuss above.

Table 2: Regulatory coverage of online targeting: summary

<table>
<thead>
<tr>
<th>Theme</th>
<th>Current effectiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self-regulation</td>
<td>While the major platforms have all adopted individual policies, there is some consistency for certain types of content, such as suicide and self-harm.</td>
</tr>
<tr>
<td></td>
<td>Self-regulation by the platforms (individual and collective) suggests that the platforms acknowledge the need to address some of the risks we have identified.</td>
</tr>
<tr>
<td></td>
<td>However, self-regulation is insufficient to manage the risks of online targeting. The French Facebook mission suggests this is a result of three factors: information asymmetry, insularity and lack of incentives on the platforms to pursue public policy goals.</td>
</tr>
<tr>
<td>Theme</td>
<td>Current effectiveness</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Data protection</td>
<td>Data protection legislation has a significant role to play in addressing some of the risks posed by online targeting. The ICO has made significant progress in addressing online targeting practices that are inconsistent with data protection legislation, including through its age appropriate design code. Improved compliance with the GDPR will help keep users safe online, not only through consent mechanisms but also through its provisions on fairness, accountability and risk minimisation. However, the regulation of online harms requires setting standards and guiding industry to define “good” content recommendation or mitigate associated risks; assessing compliance with these standards; and making judgments about the appropriate balance between privacy and other human rights, notably freedom of expression, in relation to the targeting of online content. These decisions may go beyond the scope of data protection legislation. In addition, as our public engagement work and the CMA’s work show, people do not feel that they can control the way their data is used online. This means that where consent is given it may not be meaningful. And even meaningful consent does not fully address risks of harm to users.</td>
</tr>
<tr>
<td>Competition</td>
<td>The Furman report considered the state of competition in digital markets in the UK and made recommendations to change competition policy and regulation. Government has committed to looking at how it can implement the recommendation to create a new Digital Markets Unit. The CMA is actively considering a range of possible interventions to increase competition in online markets, including recommendations to the government on the development of an ex ante pro-competitive regulatory regime to regulate the activities of online platforms. However, competition regulation has limited potential to address many of the risks posed by online targeting, for example fragmentation and polarisation of political views.</td>
</tr>
<tr>
<td>Online harms</td>
<td>The AVMSD will impose new obligations on video-sharing platforms (VSPs) from 2020. However, the VSP provisions only apply to platforms where they enable users to share video content, and the VSP provisions are limited compared to rules for broadcasters. In the UK, the proposed online harms regulator could provide regulatory coverage for online targeting if its remit and duties are scoped accordingly.</td>
</tr>
</tbody>
</table>
The regulatory environment

<table>
<thead>
<tr>
<th>Theme</th>
<th>Current effectiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Politics</td>
<td>Online targeting may enable political actors to evade the Electoral Commission’s campaign financing rules.</td>
</tr>
<tr>
<td></td>
<td>The Electoral Commission’s role is to oversee campaigning by registered political actors during election periods.</td>
</tr>
<tr>
<td></td>
<td>Online political advertising more broadly is unregulated, making it difficult to assess its impact.</td>
</tr>
<tr>
<td></td>
<td>There are no common definitions or standards for flagging political content online, which means that users may not be aware that they are seeing targeted political content.</td>
</tr>
<tr>
<td>Advertising</td>
<td>Online targeting could make it more difficult to detect non-compliance with ASA rules. Small online advertisers may have fewer incentives to comply with ASA rules than big brands that also advertise offline.</td>
</tr>
<tr>
<td></td>
<td>The ASA system depends on industry funding, and the ASA relies on voluntary provision of information and cooperation by the platforms.</td>
</tr>
</tbody>
</table>

Regulatory tools

235 The ICO, the CMA and Ofcom have broad information gathering powers, which they have used to obtain information from some platforms in carrying out their work, notably in the CMA’s market study and in the ICO’s investigation into real time bidding and adtech. However, the opacity of online targeting, and information asymmetry between platforms and regulators, means it may not be obvious what information platforms hold, whether it is relevant or where it is kept, and regulators’ powers are limited to requesting information in connection with specific functions.172

236 Our analysis of current regulators suggests that **broad information gathering powers are essential for effective regulation of online targeting**. These include the power to require documents and other information, to carry out searches, and to require organisations to provide explanations. The FCA has a power to commission reports from “skilled persons” in support of both its supervisory and enforcement functions.173 A similar provision may be particularly useful for the regulation of online targeting as it would enable technical experts to support regulators in understanding how online targeting systems operate. Regulators also have the power to impose sanctions for non-compliance with information requests, which can have strong reputational effects.

---

Sanctions are also important. The ICO, CMA and Ofcom have the power to impose large fines. However, even maximum financial penalties may have a limited financial impact on the major platforms, given their value, and other remedies may not be effective where a company already has market power.\textsuperscript{174} Investigations and appeals can be lengthy, and by the time proceedings are concluded business models may have shifted, with fines and legal proceedings seen as a cost of doing business. But companies may still see them as damaging to their reputations, creating a valuable deterrent effect. In other areas, sanctions are weaker: the maximum financial penalty that the Electoral Commission can impose is £20,000.

Regulators can also require companies to change their practices where they break the law. The CMA can require structural changes where markets are not working following a market investigation. The ICO has the power to order an organisation to stop processing activities. The Gambling Commission, Ofcom and the FCA can withdraw the right to operate in the UK for providers they have licensed in their respective sectors. Some or all of these powers will support effective regulation of online targeting.

Regulators have recognised the need to recruit and nurture data science experts to effectively regulate data-driven businesses, offline as well as online. This need will only grow and these experts will need tools to support their work, for example the IT systems and support to develop regulatory sandboxes. However, capability and capacity is still developing. The CMA DaTA unit has been running for just over a year and Ofcom’s Data Hub was established in late 2019. The CMA and Ofcom are also larger regulators: while the ASA for example recognises the need for expertise to regulate online, it may not have the scale to develop an equivalent function. The FCA, which has an established a RegTech and Advanced Analytics department, may be an important partner for other regulators as they develop their data capability. It has been engaged in extensive big data analysis for some time and is in the process of expanding its data science capability further. However, regulators will still face challenges recruiting people with the right skills and getting access to the data they need to carry out their work.
The regulators we have considered already work together to develop coordinated policy responses, as seen in the ICO and Ofcom’s collaboration on research into consumer attitudes to online harms, as well as more formal arrangements like the concurrency model for competition law enforcement and the formal co-regulation arrangement between Ofcom and the ASA. They have also established relationships with their international counterparts, for example between the ICO and the Irish Data Protection Commission.

**Summary of the effectiveness of the regulatory environment**

Above, we set out the current gaps in regulation of online targeting in the UK. **We conclude that the current UK regulatory environment cannot adequately address the harms we identified in Chapter 2**, as we summarise in the following table.

*Table 3: Effectiveness of the current regulatory regime*

<table>
<thead>
<tr>
<th>Risk</th>
<th>Effectiveness of current regime</th>
<th>Gaps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autonomy and vulnerability</td>
<td>Data protection regulation will address some harms, for example data profiling of children (under the ICO’s age appropriate design code). The data protection regime fosters user knowledge and empowerment around data, and provides guidance for companies (for example on cookies) that can help to address user harms.</td>
<td>Online targeting can lead to harms that are not captured by current regulation. There is insufficient empirical evidence available to assess the harms and benefits of online targeting. Regulators and researchers do not currently have access to the information they need to assess topics including users’ mental health, filter bubbles and echo chambers.</td>
</tr>
<tr>
<td></td>
<td>Ofcom’s Making Sense of Media programme is building understanding of how people engage with online media.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Existing regulators have policies on vulnerability. There are some rules to protect specific vulnerable groups, for example the ICO’s age appropriate design code and the CAP code.</td>
<td></td>
</tr>
</tbody>
</table>
## The regulatory environment

### Risk | Effectiveness of current regime | Gaps
--- | --- | ---
**Democracy and society** | The Electoral Commission oversees elections and regulates political finance. This can include targeted online political advertising for elections and referendums. The ICO’s proposed Code of Practice for the Use of Personal Data in Political Campaigning will complement the Electoral Commission’s role and help to ensure that political campaigners comply with data protection law. | Targeted online political advertising could make it more difficult for the Electoral Commission to assess compliance, and could even be used deliberately to evade regulatory oversight. The Electoral Commission only regulates registered campaigners, which are not the only organisations to target political content. There is no commonly agreed or legal definition of political content. The Electoral Commission is only concerned with the regulated period before and during elections, but targeted online political advertising can happen at any time. Lack of transparency of online political advertising means traditional sources of accountability (the media and Parliament) may be less effective.

**Discrimination** | One of the EHRC’s priority aims is to ensure that people have equal access to the labour market. To support this aim, it will investigate discriminatory recruitment practices. All statutory regulators have to follow the Public Sector Equality Duty.175 | The EHRC’s investigations can cover online recruitment advertising. However, the EHRC is a strategic enforcer of equality law, and cannot enforce against all breaches of the Equality Act, so it is unclear whether it has sufficient resource to carry out wholesale assessments of discrimination in targeted online employment advertising.

---

### Potential developments

We have also considered regulatory models outside the UK, proposed changes and critiques, and other developments that will influence the regulatory environment for online targeting and are relevant to our recommendations.

---

The regulatory environment

Content regulation

Different approaches to content regulation reflect different traditions of freedom of expression. Article 10 of the European Convention on Human Rights (and the UK Human Rights Act 1998) provides that the right to freedom of expression, "since it carries with it duties and responsibilities", may be limited by law. In the USA, the First Amendment to the Constitution provides for freedom from government interference and case law protects various types of speech. However, public attitudes differ.

In Germany, the Network Enforcement Act (Netzwerkdurchsetzungsgesetz or NetzDG) of 2018 applies restrictions on expression to the major online platforms. They must enable users to report illegal content. After receiving a complaint, if platforms judge that content is “manifestly unlawful” they must remove it within 24 hours. Other illegal content must be taken down within seven days. Platforms that fail to comply are liable for fines of up to €50 million. However, this gives (moderators of) platforms the responsibility to determine if content is “manifestly illegal” and may create incentives for platforms to over-remove content, which has the potential to limit freedom of expression. Some have argued that this creates a precedent that makes it easier for authoritarian states to justify censorship. NetzDG appears to have influenced the development of French legislation passed in 2019 which aims to curb online hate.

Under European law (the e-Commerce Directive), platforms have certain liability protections when they host user-generated content neutrally. The European Commission’s proposed new Digital Services Act is likely to update the EU’s liability and safety rules for online platforms. In the United States, platforms are not legally responsible for content in most cases. While many civil liberties groups support this law, some politicians have argued that it represents a subsidy to platforms, allowing them exemption from responsibility for the negative externalities of their business models, and have argued for its removal or limitation.

176 Human Rights Act 1998, Schedule 1, Article 10; www.legislation.gov.uk/ukpga/1998/42/schedule/1
177 ‘5 ways Americans and Europeans are different’, Pew Research Center, 2016; www.pewresearch.org/fact-tank/2016/04/19/5-ways-americans-and-europeans-are-different/
180 ‘France adopts tough law against online hate speech’, EURACTIV Network, 10 July 2019; www.euractiv.com/section/politics/news/france-adopts-tough-law-against-online-hate-speech/
182 Communications Decency Act 1996, Section 230; www.law.cornell.edu/uscode/text/47/230
183 ‘Section 230 of the Communications Decency Act’, Electronic Frontier Foundation; www.eff.org/issues/cda230
Others are concerned that platforms are politically biased in their approach to content recommendation. They have proposed that liability protections should be conditional on proving that their content recommendation is politically neutral. Concerns have also been raised in the United States about censorship and control of the information environment by Chinese-owned platforms. Following reports that leaked TikTok moderation guidelines encouraged takedowns of content relating to the 1989 Tiananmen Square protests and that reports on the Hong Kong protests may have been censored, Senator Marco Rubio called on TikTok to be investigated for censorship. In November 2019, the Committee on Foreign Investment in the United States was reported to have opened an investigation into TikTok. TikTok has said that American user data is not shared with its Chinese parent and that its content guidelines have been updated.

Others have proposed new structures to democratise decisions about how to treat certain items of online content, reducing the power of platforms over expression. One model is an online court system or other independent body to adjudicate content moderation decisions. These “e-courts” would focus on whether content removal violated freedom of expression (based on local law); use specially trained magistrates; and publicise a record of published decisions.

Another proposal, building on self-regulatory proposals by Facebook to introduce an independent content oversight board, is “social media councils”, which would externalise content decisions and involve a bigger role for civil society.

Concerns about false claims in political advertising have led some to call for this content to be fact-checked.

---

191 Heidi Tworek, ‘Social Media Councils’, Centre for International Governance Innovation, 2019; www.cigionline.org/articles/social-media-councils
Ben Bold, ‘IPA condemns Facebook’s refusal to ban or fact-check micro-targeted political ads’, 10 January 2020; www.campaignlive.co.uk/article/ipa-condemns-facebooks-refusal-ban-fact-check-micro-targeted-political-ads/16704287
The regulatory environment

Systemic accountability and transparency

250 In the UK and France, high-profile proposals have focused on the introduction of accountability for the risks posed by online platforms’ systems and processes, rather than specific rules about certain types of content. This includes the recommendations of the Carnegie UK Trust193 and French Facebook mission.194 These approaches would require online platforms to protect their users from reasonably foreseeable harms that might arise from use of their services. These approaches would apply principles-based regulation and accountability provisions similar to those in the GDPR to the regulation of online harms and the targeting of content online.

251 Proposals for systemic accountability require greater levels of transparency from platforms. For example, the French Facebook mission proposed that platforms should be transparent about the operation of their recommendation systems and personalised advertising services.195 This addresses the mission’s concern that despite Facebook’s engagement, “at the end of three months we had nothing tangible [and no way of telling whether what we heard was] true or not.”196 The regulator proposed by the French team would have the authority to enable detailed study of the workings and impacts of algorithms by third-party experts.

252 There is support for increased platform transparency in both Europe and North America. In the UK, the Online Harms White Paper proposes that the regulator should have the power to require (and publish) annual transparency reports from companies in scope, outlining the prevalence of harmful content on their platforms and what countermeasures they are taking to address these. The European Commission’s Code of Practice on Disinformation, a self-regulatory initiative, included a range of commitments for platforms to improve the transparency of political advertising and to provide annual reports about their approaches to

194 ‘Creating a French framework to make social media platforms more accountable: Acting in France with a European vision’, Direction interministérielle du numérique et du système d’information; 2019; https://minefi.hosting.augure.com/Augure_Minefi/r/ContenuEnLigne/Download?id=AE5B7ED5-2385-4749-9CE8-E4E1B36873E4&filename=Mission%20Re%CC%81gulation%20des%20re%CC%81seaux%20sociaux%20-ENG.pdf
195 ‘Creating a French framework to make social media platforms more accountable: Acting in France with a European vision’, Direction interministérielle du numérique et du système d’information; 2019; https://minefi.hosting.augure.com/Augure_Minefi/r/ContenuEnLigne/Download?id=AE5B7ED5-2385-4749-9CE8-E4E1B36873E4&filename=Mission%20Re%CC%81gulation%20des%20re%CC%81seaux%20sociaux%20-ENG.pdf
The regulatory environment

dealing with disinformation. While there are limits to the effectiveness of these voluntary measures, the Commission reports that the Code has led to modest improvements.

In Germany, NetzDG has resulted in the publication of significant reporting by large online platforms. However, these measures have been criticised by the platforms for being too onerous and prescriptive, and by civil society for not containing enough detail to be empirically useful. In France, fake news laws would require platforms to make it clear in published statistics what proportion of content relating to elections is directly accessed and what proportion has been recommended by an algorithm.

In Germany, NetzDG has resulted in the publication of significant reporting by large online platforms. However, these measures have been criticised by the platforms for being too onerous and prescriptive, and by civil society for not containing enough detail to be empirically useful. In France, fake news laws would require platforms to make it clear in published statistics what proportion of content relating to elections is directly accessed and what proportion has been recommended by an algorithm.

253 In Germany, NetzDG has resulted in the publication of significant reporting by large online platforms. However, these measures have been criticised by the platforms for being too onerous and prescriptive, and by civil society for not containing enough detail to be empirically useful. In France, fake news laws would require platforms to make it clear in published statistics what proportion of content relating to elections is directly accessed and what proportion has been recommended by an algorithm.

In California, the Bolstering Online Transparency (BOT) Act, which took effect in 2019, created requirements for automated online accounts to identify themselves as such to users. The BOT Act defines a bot as an “automated online account where all or substantially all of the actions or posts of that account are not the result of a person”. The Canada Elections Act (2019) requires platforms to provide a register of election adverts on their platforms.

The Santa Clara Principles is a civil society initiative led by a coalition of organisations and academics, which aims to improve the accountability and transparency of platforms’ moderation of user-generated content. The initiative requests that platforms provide users who have had their content removed or accounts suspended with more explanation and opportunity for appeal. It also requests more aggregate data is released by platforms about violations of their content guidelines.

Consumer protection and data protection

In response to Cambridge Analytica and other scandals, there have been calls to impose restrictions on online targeting systems. These include proposals to restrict the types of data used by online targeting systems (such as psychometric data); the types of tools used to identify target audiences (such as custom audiences and lookalike targeting); the number of people that can be

199 LAW n° 2018-1202 of December 22, 2018 relating to the fight against the manipulation of information, Article 14; www.legifrance.gouv.fr/affichTexteArticle.do?cidTexte=JORFTEXT000037849782&categorieLien=id&dateTexte=
200 California Senate bill 1001 (Bolstering Online Transparency Act), 2018; https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1001
targeted in advertising campaigns;204 and changing default settings for online targeting systems.205 Several of the major online platforms have taken steps to restrict targeting options for advertisers206 and to adjust their content recommendation systems.207

There have also been proposals to update consumer protection regulation to respond to the growth of online platforms and their use of online targeting systems. One suggestion is “performance-based” consumer protection regulation, in which online platforms would be assessed on the basis of the average level of user understanding of key elements of the service.208 The CMA's ongoing market study is also considering various potential interventions to improve consumer information and people’s control over their online experiences. These include requirements on online platforms to: enable consumers to use their services without requiring in return the use of data about them for personalised advertising; change their default settings to require an “opt-in” to personalised advertising rather than the current default “opt-out”; and design consent and privacy policies in a way that facilitates informed consumer choice through a principle of “fairness by design”.209 Civil society organisations including Doteveryone have advocated for improvements to people’s access to redress for online harms.210

As noted above, it is likely that greater clarity and understanding about the views and interpretations of the GDPR by data protection authorities and domestic and European courts, and its interaction with competition regulation, will emerge over the coming years. Some have suggested that rigorous enforcement of the GDPR principles of data minimisation and purpose limitation will reduce the ability of major online platforms to leverage user data assets.211 But, as noted above, others are concerned that data protection regulation may unduly favour the business model of large, vertically integrated platforms over smaller publishers, which could increase their market power.

204 Kari Paul, ‘Facebook employees ‘strongly object’ to policy allowing false claims in political ads’, 28 October 2019; www.theguardian.com/technology/2019/oct/28/facebook-employees-strongly-object-to-policy-allowing-false-claims-in-political-ads
205 ‘Online platforms and digital advertising market study’, Competition and Markets Authority, 2019; www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study
207 ‘Continuing our work to improve recommendations on YouTube’, Youtube, 2019; https://youtube.googleblog.com/2019/01/continuing-our-work-to-improve.html
209 ‘Online platforms and digital advertising market study’, Competition and Markets Authority, 2019; www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study
211 ‘Dr Ryan and Dr Lynksey’ in ‘Responses to Statement of Scope’ of the ‘Online platforms and digital advertising market study’, 2019; www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study#responses-to-statement-of-scope
The regulatory environment

The DCMS Select Committee on Disinformation and ‘fake news’ recommended in 2019 that “digital literacy should be a fourth pillar of education, alongside reading, writing and maths”. Both the Select Committee and the Cairncross Review recommended that the government should develop a media and digital literacy strategy involving greater coordination of existing efforts (for example Ofcom’s Making Sense of Media and the ICO’s Your Data Matters programmes) and a focus on locating gaps, such as adult provision. The government’s Online Harms White Paper outlined plans for the online harms regulator to have oversight of industry activity and spend, and a responsibility to promote online media literacy. Ahead of the establishment of an online harms regulator, the government plans to develop an online media literacy strategy.

Competition

In addition to the potential consumer protection measures discussed above, the CMA is considering a number of interventions to address its competition concerns. These include specific pro-competitive ex-ante rules for companies with “strategic market status”, set out in an enforceable code of conduct, which the CMA says should take the form of high-level principles rather than detailed and prescriptive rules.

The CMA is also considering potential interventions to address sources of market power and promote competition. To address Google’s position in search, it is exploring a requirement that Google provide click-and-query data to rival search engines, a possible restriction on Google’s ability to be the default search engine on devices and browsers, and a requirement to offer choice screens to consumers on devices and browsers. In relation to social media, it is considering measures to increase the interoperability of Facebook and potentially other social media platforms. To address concerns about display advertising, it is considering the case and options for separation remedies on Google.

While these potential developments are likely to support competition in the longer term, some argue that immediate and dramatic interventions are needed to reduce the market power of the major platforms and increase competition. Some academics have argued that anti-monopoly regulation needs to be applied “as a check on power as necessary in a functioning democracy before it’s too late.” The European Commission has mounted multiple investigations of big technology companies leading to record fines, if not blocks on acquisitions. The CMA has found the five largest firms have made over

---


400 acquisitions globally in the last decade. None were blocked²¹⁶ (although we note that the CMA is currently investigating the proposed acquisition of certain rights and a minority shareholding in Deliveroo by Amazon).²¹⁷ American competition policy has focused on protecting consumers from increased prices, leading to limited action being taken against platforms which are often offering free services or cheaper products to consumers. This has led to proposals to reform the principles of American competition policy.²¹⁸

**Market developments**

**1. Data intermediaries**

Some recent initiatives have focused on increasing people’s ability to control the way they are targeted. Some of these proposals aim to allow people to own their data (such as Tim Berners-Lee’s proposals for a new type of web infrastructure).²¹⁹ However, focusing on data ownership has been criticised for failing to take account of the cognitive burden on users that comes with managing settings and understanding consent policies across the internet. There are also concerns that they may encourage the poorest and most vulnerable people to “sell” their privacy. In response, some organisations have argued for the development of data intermediaries (also referred to as data representatives) to provide them with stronger rights over data about them.

Data intermediaries would interface with multiple digital services to manage personal data on behalf and in the interests of individual users. They could provide centralised consent management and authentication services, and help users exercise their rights under data protection legislation.²²⁰ They could also collectively negotiate on behalf of their members’ interests, advocate for improved terms and conditions, and create standardised user controls that apply across different products. They could be set up as companies, like the British start-up Digi.me, or as trusts or cooperatives with fiduciary responsibilities to their members’ interests.²²¹

---

²¹⁹ K.G Orphanides, ‘How Tim Berners-Lee’s Inrupt project plans to fix the web’, 16 February 2019; www.wired.co.uk/article/inrupt-tim-berners-lee
²²⁰ ‘Online platforms and digital advertising market study, Appendix L: Potential approaches to improving personal data mobility’, Competition and Markets Authority, 2019; www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study
However, attempts to establish data intermediaries have met with limited success to date due to technical challenges and commercial viability. They may also create new privacy and data protection risks that would need to be managed. As such, new regulation or standards may be necessary to support their development.222

2. Privacy and encryption

There are signs that businesses are responding to developments in data protection and privacy rules, including the GDPR and new regulation in other parts of the world such as the California Consumer Privacy Act. Any changes to EU privacy rules may also influence these developments.223

Browsers such as Safari and Firefox have adopted new third-party tracking prevention techniques by default. Smaller competitors like Brave use such techniques as a major selling point of their business. And Google has announced that it plans to abandon third-party cookies in Google Chrome, currently the world’s most popular browser.224 Privacy preserving features are also being introduced into mobile operating systems like iOS and Android,225 and techniques to encrypt communications and data exchanges226 are being more widely used across online platforms.227

While such moves are likely to protect privacy, they may also entrench the major platforms’ market positions by making their ability to target advertising more attractive relative to other publishers, who will no longer be able to use third-party cookies. In addition, many major platforms are developing the infrastructure and technology to enable them to continue to conduct online targeting at scale without extensive third-party tracking.228

---

222 See upcoming report by Onward on “The People’s Internet”; www.ukonward.com
International governance

For most of the 1990s and 2000s, there was broad acceptance that the internet should be global and open, and its governance should be on the basis of multi-stakeholder cooperation involving civil society, business and academia. This governance has taken the form of a United Nations (UN) multi-stakeholder forum called the Internet Governance Forum. International technical standards have been introduced through bodies such as the Internet Engineering Task Force (IETF) and the Institute of Electrical and Electronics Engineers (IEEE), a professional association.

However, as we discuss above, concerns about online harms have led many liberal democracies to take steps to regulate content at the national level. While these governments continue to support the principle of multi-stakeholder governance, human rights groups have argued that these governments’ actions set precedents that undermine this model.

At the same time some authoritarian countries have been advancing a model of “internet sovereignty”. This model holds that states should control the architecture of their “national” internets, usually resulting in a censored or unfree space. For several years, China has sought to build support for this vision at the United Nations and its affiliate organisations. Analysis for the Council of Foreign Relations shows that in 2019, more governments sided with Chinese and Russian proposals for internet sovereignty in the UN, and countries including Vietnam, Kazakhstan, and Indonesia increased control over the flow of online content. There are significant technological and infrastructural challenges to the delivery of a sovereign internet. According to Freedom House, at least 36 governments have received closed-door Chinese training on “new media and information management.”

In this environment, there is a risk that national regulation by liberal democracies will inadvertently provide support to authoritarian models of governing the internet. Chatham House has highlighted “an urgent need for coordinated rule-making at the international level” to ensure the internet helps to advance...
rather than undermine human rights. New America, a think tank, has suggested that UK domestic policymaking will play a particularly important role in the development of international governance. Regulation of online targeting in the UK must consider its potential influence on international norms and ensure that the UK continues to promote human rights globally.

**Conclusion**

We conclude that the current UK regulatory environment cannot adequately address the harms we identified in Chapter 2. There are a number of potential developments that may help to strengthen competition and protect users, but we believe the government and regulators need to take action as well. In the next chapter, we outline our recommendations on online targeting to the UK government, which are designed to increase accountability, transparency, and user empowerment.

238 ‘Tackle the ‘Splinternet’, Chatham House, 2019; www.chathamhouse.org/expert/comment/tackle-splinternet
5. Recommendations

Summary

Accountability
- The government’s new online harms regulator should be required to provide regulatory oversight of targeting:
  - The regulator should take a systemic approach, with a code of practice to set standards, and require online platforms to assess and explain the impacts of their systems.
  - To ensure compliance, the regulator needs information gathering powers. This should include the power to require platforms to give independent experts secure access to platform data to undertake audits.
  - The regulator’s duties should explicitly include protecting rights to freedom of expression and privacy.
  - Regulation of online targeting should encompass all types of content, including advertising.
  - The regulatory landscape should be coherent and efficient. The online harms regulator, ICO, and CMA should develop formal coordination mechanisms.
  - The government should develop a code for public sector use of online targeting to promote safe, trustworthy innovation in the delivery of personalised advice and support.

Transparency
- The regulator should have the power to require platforms to give independent researchers secure access to their data where this is needed for research of significant potential importance to public policy.
- Platforms should be required to host publicly accessible archives for online political advertising, “opportunity” advertising (jobs, credit and housing), and adverts for age-restricted products.
- The government should consider formal mechanisms for collaboration to tackle “coordinated inauthentic behaviour” on online platforms.
User empowerment

- Regulation should encourage platforms to provide people with more information and control:
  - We support the CMA’s proposed “Fairness by Design” duty on online platforms.
  - The government’s plans for labels on online electoral adverts should make paid-for content easy to identify, and give users some basic information to show that the content they are seeing has been targeted at them.
  - Regulators should increase coordination of their digital literacy campaigns.
  - The emergence of “data intermediaries” could improve data governance and rebalance power towards users. Government and regulatory policy should support their development.

The CDEI would be pleased to support the UK government and regulators to help deliver our recommendations.

Our approach: limiting harms and enabling beneficial uses of online targeting

In this chapter we outline our recommendations. They have been designed to enable people, businesses and society to benefit from the use of online targeting, while mitigating the key risks posed by online targeting systems across the themes of autonomy and vulnerability, democracy and society, and discrimination. They are also relatively easily implemented and take account of likely developments in government and regulatory policy, particularly the proposed Online Harms Bill and the establishment of the Digital Markets Unit.

The recommendations are in line with public attitudes. Our research, outlined in Chapter 3, shows that people value online targeting, but want changes to be made to the use and governance of online targeting systems. Participants in our public dialogue supported changes that aimed to increase the ability of the government and regulators to hold online platforms to account, increase transparency, and empower users.
Our recommendations fall into three categories:

- **Accountability**: making operators of online platforms accountable for how they approach risks associated with their online targeting systems. This includes public sector organisations.

- **Transparency**: ensuring that there is adequate information for people, regulators, independent researchers and civil society to be able to assess the impact of online targeting where this would enable harms to be addressed.

- **User empowerment**: giving people greater control over how their data is used and encouraging the development of solutions that rebalance power between large platforms and their users.

Much of the harm that may result from the use of online targeting systems is a symptom of current market structures. Reshaping online markets to create incentives for the emergence of companies that are more closely aligned with the interests of customers, such as data intermediaries, will take time. Our aim has been to balance the need for proportionate regulatory remedies that can take effect rapidly against the need for measures designed to encourage longer term changes in the market.

**Appropriate and proportionate**

Our recommendations strike an appropriate balance between protecting users and imposing costs on online platforms, while enabling responsible innovation. We have favoured interventions that increase transparency to ensure that policymaking and regulation is capable of assessing and responding to harms as they emerge.

Our proposals are also designed to be coherent with the broader regulatory environment. Digital regulation is in flux and there is overlap between regulators. There must be clear and effective coordination mechanisms between the online harms regulator and other regulators, particularly the ICO and CMA.

The regulatory approach must respect human rights, including privacy and freedom of expression, and be considerate of its impact on international norms.

**Address risks and harms**

Our proposals aim to provide the most effective means to address risks and harms caused by online targeting, in direct response to public calls for greater protection online. They will enable major online platforms to be held to account for how they recommend content and target people online. And they are designed to be flexible and able to reflect rapid changes in technology or uses of the internet and online targeting.
Critically, they enable research to be done at scale to increase the evidence base about the nature, extent, and severity of the harms we identify in this report. This will support regulatory action and the development of effective and proportionate policy.

**Encourage innovation**

Our proposals aim to enable growth and innovation in the use of online targeting, maximising the benefits of data and AI for the UK society and economy. Improving the governance of online targeting will support the development and take-up of socially beneficial applications of online targeting. It will also facilitate greater public sector use of online targeting, securing greater efficiency and better value for money, with the UK government setting the standard for safe, transparent and accountable use of online targeting. Online targeting could be used to encourage young people to take up training opportunities, working people to save for their future, or parents to vaccinate their children.

In addition, our recommendations will support the UK to grow as a global leader in responsible innovation in data-driven technology. They will help to create an environment that fosters:

- **Evidence-based policymaking and research**: the UK can build capability in regulation and independent research into the impacts of online targeting, which will allow it to benefit from a deep understanding of complex social issues.

- **Data intermediaries** that can manage the use of personal data on behalf of individual users. Data intermediaries would be just one potential model in a wider online safety ecosystem, which could also include third-party age verification systems.

- **An AI audit market** to support operators in understanding and mitigating the risks posed by their use of online targeting systems, and to support regulators in understanding and assessing the actions of providers of online services.

We believe that these businesses and areas of expertise would be an important part of a society that can fully benefit from AI and data-driven technologies.

Concern about the risk of online targeting systems is shared by many democratic governments around the world. Our recommendations are designed to enable the UK to play its part in a coordinated international response that enables the oversight of online targeting systems in a way that is consistent with democracy and human rights.

Wide-ranging legislative and regulatory change takes time. But the UK needs to start implementing changes immediately to protect users from harm while retaining the benefits of online targeting, and we are determined to make progress towards these recommendations. The CDEI will be publishing its programme of work for 2020 shortly, which will include further work to develop the proposals set out here. We would be pleased to support the UK government...
and regulators to help deliver our recommendations. As an independent expert body, we would be pleased to bring together relevant stakeholders and help to guide the development of policy and regulation as the landscape evolves.

## Accountability

Addressing issues related to online targeting is critical to the success of an online harms duty of care. As we discussed in Chapter 2, online targeting is an integral part of many online harms, and our analysis of public attitudes demonstrates a clear expectation of greater oversight and accountability. But as we set out in Chapter 4, the current UK regulatory environment cannot fully address the risks posed by online targeting.

### A code of practice for online targeting

We recommend that the government introduces regulatory oversight of organisations’ use of online targeting systems through the proposed online harms regulator. Regulation of online targeting should take the form of a code of practice developed by the regulator. For convenience we refer to this below as “the code” although in practice these principles may form part of a wider system of online regulation and could be distributed in different ways. The online harms regulator will need to coordinate closely with other regulators such as the ICO and the CMA or Digital Markets Unit, to avoid possible duplication of work. We discuss measures to improve regulatory coordination in more detail below.

Online targeting systems are highly complex and can lead to a wide range of harms. The code should be systemic, focused on the processes organisations use to target content. This will help to make organisations more accountable and ensure regulation is future-proof. It should set out at a high level the risk management and transparency processes that online platforms will need to adopt in order to demonstrate that they are meeting their obligations. This type of approach would avoid some of the challenges posed by the regulation of content at scale. It should also reflect the regulator’s duties in relation to freedom of expression online, which we discuss below.

In practice, this means that online platforms should be prepared to:

- Monitor and document the impact of their online targeting systems.
- Carry out and document risk assessments for their online targeting systems.
- Justify their decision making.
- Explain, with examples, how their systems and processes work in practice.

The code could include requirements on online platforms to document:

- The purpose and desired outcomes of the online targeting systems.
- How the online targeting systems work, what data they use, and any key design features.
The code would need to be developed by the online harms regulator. It should take the form of high-level principles, rather than detailed or prescriptive rules. The regulator should work with online platforms, civil society organisations and other regulators to develop an understanding of best practice in the areas set out above. The regulator should use examples of best practice to demonstrate how online targeting systems could meet the duty of care.

Organisations that use online targeting systems would be expected to demonstrate that they have considered these examples and, where relevant, justify their decisions to employ different solutions that meet a similar standard of care and diligence. They may choose to support their compliance work by using expert third-party auditing services to provide an independent assessment of compliance. This would also support the regulator in assessing compliance. This also creates an opportunity for the UK to take first-mover advantage in a new global industry of AI auditing, building on the country’s strengths in professional services.

The regulator may also develop additional detailed guidance on areas of particular complexity where there is potential for harm. The needs of children and people who may be vulnerable should be a priority.
Over time, with a better evidence base and improved regulatory understanding, the regulator may create more prescriptive requirements for online targeting systems. This might include specific information providers are required to provide to the regulator or publish, which may enable the regulator to create a dashboard of common metrics and facilitate comparisons between providers.

**Regulatory scope and approach**

As we discussed in Chapter 2, the risks of online targeting include harms caused by the targeting of commercial and political advertising. We recommend that the UK’s online harms regulatory regime is not limited to user-generated content.

The regulator should take a risk-based approach in determining its priorities for regulatory action and enforcement. It should also take into account the costs that regulation imposes on companies, and ensure that it does not unduly favour larger and better resourced companies, as compared to SMEs and new entrants. On a day to day basis, we suggest that the regulator adopts a dynamic approach, involving risk-based monitoring and oversight of the activities of organisations in scope and regular discussion with industry and civil society.

In assessing compliance with the code of practice for online targeting, we suggest that the regulator focus its activities on organisations that:

- Use "open" content recommendation systems.
- Have significant reach among the UK public, or among vulnerable populations such as children.
- Have significant user data assets.
- Derive a substantial proportion of their revenue from targeted advertising.
- Have positions of significant influence in the online information environment.

We would expect that major platforms such as Google and Facebook would be in scope, but it will be up to the regulator to determine appropriate thresholds and define what constitutes “significant”. Other approaches have set precedents for this, for example the thresholds adopted in NetzDG, or the proposals of the French Facebook mission report which would apply based on numbers of monthly users. Given that these are major global companies, the UK government should ensure that the Online Harms Bill gives the proposed new regulator jurisdiction over global companies that provide services to UK citizens. We discuss international cooperation between governments and regulators below.

---


243 ‘Creating a French framework to make social media platforms more accountable: Acting in France with a European vision’, Direction interministérielle du numérique et du système d’information, 2019; https://mineti.hosting.augure.com/Augure_Mineti/Content/EnLigne/Download?id=AE5B7ED5-2385-4749-9CE8-E4E1B36873E4&filename=Mission%20de%CC%81gulation%20des%20re%CC%81seaux%20sociaux%20-%20ENG.pdf
Regulatory duties and powers

301 Regulation to tackle online harms must be consistent with the rights of users, especially freedom of expression and privacy. In addition to its responsibilities under the Human Rights Act 1998 and Public Sector Equality Duty, we recommend that the regulator’s statutory duties include protecting and respecting rights to freedom of expression and privacy. In this light, the UK government should continue to uphold the principle in the e-Commerce Directive that platforms should not generally be liable for neutrally hosting content, and should not have general monitoring duties or incentivise the removal of legal content.

302 In relation to the right to privacy, the regulator should work closely with the ICO to ensure that users’ privacy is appropriately protected online. This should include coordinating (and not duplicating) on enforcement of areas of common interest such as the ICO’s age appropriate design code. The regulator should ensure that it does not create incentives on companies to collect more user data than they need.

303 In relation to freedom of expression and other human rights, the regulator should work closely with the EHRC to ensure that the regulator meets its duties. The Carnegie UK Trust argues that the online duty of care model allows for the appropriate balancing of rights considerations. Our proposed code of practice, which focuses on the safe and responsible distribution of content, rather than the regulation of content itself, goes some way to address risks to freedom of expression. Consistent disclosure of platforms’ content recommendation policies, achieved through the code, would also enable comparison of platforms’ approaches to free expression.

304 The regulator must be able to understand the organisations it regulates and their impact on users, so that it can shape and enforce regulation that will achieve its objectives. It therefore needs powers to obtain the information that it needs to carry out its prescribed functions, including assessing compliance with the code of practice. In some cases, the regulator may need access to personal data for its analysis, and must use this in a way that conforms with data protection legislation.

305 The regulator should also have the power to require online platforms to give independent experts secure access to their data to enable further testing of compliance with the code of practice. We discuss this recommendation in more detail below in relation to transparency. A possible model is the FCA’s power to require reports from third parties (skilled persons) about a regulated firm’s activities where it is concerned or wants further analysis. This kind of power would enable the regulator to carry out expert analysis of online targeting systems that it does not have the skills or capacity to do in house.

245 ‘Skilled person reviews’, Financial Conduct Authority; www.fca.org.uk/about/supervision/skilled-persons-reviews
Recommendations

The regulator also needs effective sanctioning powers. As well as powers to issue fines, it should be able to name and shame companies in breach of its codes and issue enforcement notices where there is evidence of a significant compliance failure – requiring organisations to take steps to ensure compliance.

The legislation establishing the regulator should set limits on the exercise of these powers to ensure that the regulator acts in a transparent, accountable and proportionate way. The regulator’s powers must be subject to due process.

Regulatory coordination and coherence

As set out above, the risks posed by online platforms and online targeting span multiple areas of regulation, including competition, consumer protection, data protection and content regulation. Regulatory functions relevant for online targeting are spread across different regulators, and regulatory interventions in any of these areas may lead to consequences elsewhere. As discussed above, measures to protect personal data online may reduce the competitiveness of online markets, and measures to increase competition in online markets may reduce or increase the spread of harmful content online.

In this context, it is important that the regulatory system is coherent, and includes mechanisms to ensure that regulators avoid duplication in practice while ensuring comprehensive coverage of risks. In addition to existing regulatory functions, these will need to capture new regulatory responsibilities such as those proposed in the Online Harms White Paper and the Furman report. A lack of coherence risks causing confusion, decreasing the effectiveness of regulation, and reducing incentives to innovate.

While different regulators have different areas of responsibility and expertise, there are areas of potential overlap. The ICO is responsible for addressing targeting practices that may be inconsistent with data protection legislation and/or PECR. The CMA or Digital Markets Unit would be responsible for addressing targeting practices that may be inconsistent with its remit to promote competition for the benefit of consumers. The online harms regulator should be responsible for addressing targeting practices that may cause harm to people or society.

In light of this, there needs to be a system for determining which regulator will develop a policy or investigate a complaint. Regulators should develop formal coordination mechanisms to enable decisions about which regulator is best placed to act to be made quickly and clearly.

Examples of coordination mechanisms that may be relevant for developing a system for online targeting include the UK’s concurrency framework for the enforcement of competition law, under which the CMA and “concurrent” regulators (sectoral regulators, for example Ofcom and the FCA) agree which is “best placed” to consider a case. In Europe, the European Data Protection

---

Supervisor has proposed the establishment of a “digital clearing house” to bring together agencies from the areas of competition, consumer and data protection willing to share information and discuss how best to enforce rules in the interests of the individual.247

Regulators should also collaborate on wider strategic policy questions. The CMA, the ICO and Ofcom have a long history of coordinating their regulatory approaches. Over the past few years, they have increasingly formalised their joint and collaborative work on online services, to meet both current and future regulatory challenges. Regulators also work together through strong bilateral relationships, larger groups including the UK Regulators Network, and specialist groups such as the AI Regulators Working Group, convened by the ICO. Regulators should consult each other where policy developments may have an indirect impact on another regulator’s work, even where there is no immediate question over jurisdiction.

Given the global nature of many of the organisations in scope of regulation, the UK government should contribute to the development of similar regulatory regimes in other countries. The UK government should be mindful of developments in the European Union, including the proposed Digital Services Act, and in North America. The UK’s regulators, including the online harms regulator, the ICO, and the CMA, should also coordinate and collaborate with their counterparts and other relevant organisations internationally.

Finally, the new regulator needs sufficient resources to do its job properly. This is also the case for other regulators with important remits relating to online targeting, such as the ICO and the CMA. Funding needs to be able to address the possibility of expensive litigation that may come about as regulators enforce new laws and exercise new powers. And regulators need to be able to attract talent, especially people with the data science skills required to scrutinise platform operations. Given that these skills are scarce, the UK’s regulators, in particular the CMA, the ICO and the new online harms regulator, should consider mechanisms for sharing data science resources. They should also consider the possibility of sharing data and infrastructure in privacy-preserving ways to deliver better outcomes for UK citizens.

Accountability for online advertising

In Chapter 2, we discussed the harms that can arise from online targeting, including personalised online advertising. Our public engagement found that people think there should be greater accountability for the targeting of adverts online. The ICO’s work on real time bidding and adtech is likely to reduce the data protection risks associated with advertising targeted outside of platform environments, and the AVMSD covers advertising on on-demand services and VSPs. But as we discussed in Chapter 4, the UK regulatory environment may be unable to address the risks posed by targeted online advertising delivered

by major online platforms. In particular, the ASA system may be less effective at influencing the long tail of small advertisers than big brands that also advertise offline.

317 The UK government is undertaking a review of online advertising regulation. **We recommend that it considers introducing new rules for personalised online advertising that place responsibilities on the platforms.** Our view is that the best way to do this would be through the inclusion of advertising content in the online harms duty of care. This would create a responsibility for online platforms to protect their users from harm caused by personalised advertising. It would also increase incentives on advertisers to cooperate with the ASA and comply with the CAP code, including smaller advertisers, for example by requiring that online platforms raise awareness of, and improve compliance with the CAP code.

318 This would increase regulatory coherence, as the same regulator would have statutory responsibility for addressing risks associated with targeted advertising and targeted content on online platforms. This arrangement would also require regular coordination with other regulators like the ICO and the CMA or the Digital Markets Unit, as well as those that are already responsible for sectoral advertising like the Gambling Commission.

319 **We also encourage the ASA to update the CAP code to set out its expectations and expand its guidance around harms associated with the targeting of online adverts.** We welcome the implementation of the ASA’s More Impact Online strategy, including further research into online targeting and working more closely with major online platforms.

**Unlocking value through a public sector code of practice for online targeting**

320 The use of online targeting systems pose many benefits as well as risks, as set out in Chapter 2. This is true for the use of these systems by public as well as private sector organisations.

321 The public sector should use the most effective tools at its disposal to deliver public services. In our analysis of public attitudes, we found that there was broad support for the responsible use of online targeting by public sector organisations. 68% of people believe that public services should use data about people to target their services and advice.

322 However, public sector organisations must hold themselves to particularly high ethical standards. They deliver essential services to UK citizens, including people who may be vulnerable. They hold sensitive data about UK citizens, who may be concerned about risks to their privacy and risks of state control. As we will set out in our upcoming report on public sector data sharing, experience has shown that to make the most of the use of data-driven technology, the public sector needs to operate in a trustworthy way and build public support for its actions.
We recommend the development of a code of practice for public sector use of online targeting systems. This would empower the public sector to make the most of the potential of online targeting systems, and build public trust in its use of technology. Such a code should include requirements about ethical oversight mechanisms, transparency and individual control over data. It should also take into account the variety of ways in which the public sector could use online targeting systems and provide guidance around the different considerations that might apply in different circumstances.

This code would be in addition to the code of practice for online targeting that we discuss above.

Transparency

Report on Transparency

As we note above, the government has proposed that the online harms regulator should have the power to require (and publish) annual transparency reports from companies in scope. Respondents to the Online Harms White Paper have argued that reporting needs to go beyond “raw numbers of content removed”, and should also cover “how and on what basis rules and policies are made, what factors inform content-related decisions and provision of hypothetical case examples showing how rules are interpreted and applied”.248 Where companies operate online targeting systems, we recommend that reporting should explain what they use the systems for, what their policies are, and how they apply them. For example, reports could explain what factors are used to determine how the platform ranks content.

Developing an evidence base

1. Research by the regulator

To achieve its objectives, the online harms regulator will need to develop evidence-based policy and identify best practice. It will need to be able to assess the benefits and risks of online targeting in order to develop guidance about its use. To do this, the regulator will need to conduct research into the positive and negative impacts that online targeting can have on users, as well as gathering information formally and informally from industry.

We recommend that the regulator carries out regular research into public attitudes towards online targeting, and into people’s experiences of online targeting. The government should consider including this in the regulator’s formal responsibilities, but we anticipate that the regulator will develop a programme of research to inform its work in any case.

Research helps regulators understand the sectors they work in, identify emerging trends, and assess the impact of their policies. Some methods of research already available to regulators and researchers are set out in Box 6.

The online harms regulator should also carry out large-scale research and analysis of platform data, and platforms should facilitate this by enabling the safe use of tools like plug-ins. The government should ensure the regulator is adequately funded to deliver research.

**Box 6: Avatars and consumer research**

Regulators and researchers are using quantitative and qualitative consumer research to understand the impact of online targeting. Ofcom’s Media Lives series tracks individual users over time to provide a small-scale but rich and detailed qualitative complement to its quantitative work.249

The ASA has used child avatars (online profiles which simulate children’s browsing activity) to detect inappropriate targeting of gambling250 and junk food adverts251 to children online. The ASA has shown that this can be an effective approach for preliminary assessments of compliance with regulation and the severity of risks. The use of fake profiles for avatar research is currently prohibited by most large online platforms, but this could be relatively easily addressed as platforms could agree (and publish) exemptions to this policy for regulator access.

Academics have assessed the welfare effects of social media through a large-scale randomised evaluation of Facebook users.252 They show that the deactivation of users’ Facebook accounts reduced their overall online activity, reduced their factual news knowledge and their political polarisation, increased their subjective well-being, and caused a large persistent reduction in Facebook use after the experiment.

There are limits to the effectiveness of these approaches. For example, child avatars do not capture the experience of other types of users, who may be more difficult to simulate. Research tracking consumer behaviour over time (such as Ofcom’s Media Lives series) can reveal trends and help regulators understand the impact of online targeting on individuals and society, but may not enable them to assess the scale of any impact.

2. Enabling independent research on issues of public interest

As well as carrying out its own research, we recommend that the regulator facilitates independent academic research into issues of significant public interest.

Online platforms exclusively hold the information that would enable more evidence-based policymaking on issues of significant importance including:

- **Vulnerability**: the link between social media use and mental health, and “internet addiction”.

- **Democracy and society**: the extent of filter bubbles and echo chambers, and the impacts of digital campaigning on polarisation.

- **Discrimination**: the extent to which targeted advertising is leading to discriminatory outcomes.

In our public engagement, as discussed in Chapter 3, we identified significant public concern about all of these issues. The Royal College of Psychiatrists has called for platforms to be compelled to make their data available for independent research into the risks and benefits of social media use on mental health. However, the online harms regulator cannot be expected to find the answers to these questions itself. It may not have the capacity or skills to undertake large-scale research and analysis. It may also be inappropriate for the regulator to carry out this work given the sensitive nature of platform data about individual users, and potential conflicts that may arise given the relevance of this research to the regulator’s interests. This means that significant concerns may go unstudied and emerging trends may go unnoticed, reducing the evidence base for policymakers and risking poorly informed and disproportionate policy decisions on issues of long-term importance.

Online platforms have highly complex systems. It is likely to be inefficient, and maybe impossible, to replicate these for research purposes, for example in a regulatory sandbox environment. Research into the real-life impact of online targeting on people and society is likely to require the long-term application of different techniques and disciplines to platform data, and (with their full consent) the linking of that data to information about users’ real-life behaviours and attitudes.

For most major platforms (with the exception of Twitter), access to data for research purposes is extremely limited. Voluntary initiatives such as Social Science One (SS1) have had limited success. SS1 is a data sharing partnership between Facebook and social scientists launched in April 2018 to provide independent academic researchers with privacy-preserving data to study...

---


254 'Twitter data for academic research', Twitter; https://developer.twitter.com/en/use-cases/academic-researchers
“the effects of social media on democracy and elections”. To date, it has not lived up to its promise, largely due to Facebook’s failure to provide essential data that it had agreed to, citing privacy concerns (which researchers have disputed).255

We therefore recommend that the regulator has the power to require online platforms to give independent experts secure access to their data.

3. Developing a model for safe data access

The regulator must at all times use its powers in a proportionate way, subject to due process. This means it needs to develop a model for using its powers to require access to platform data, in a way that respects online platforms’ legal rights and commercial interests and users’ privacy. It must be fully compliant with GDPR and other legal requirements.

To avoid conflicts of interest, and provide for long-term research in line with public interests, the regulator may not be best placed to make these decisions itself. We therefore recommend that the government considers designating an expert independent third-party organisation to make decisions about data access, under a co-regulatory arrangement with the regulator. Facebook has recognised that its existing data access frameworks may need to become more independent in the long term.256 An expert third party body would develop strong relationships with the platforms, UK Research Councils, and others. Its role would be to assess all proposals for data access on the basis of reasonableness, considering risks to users’ privacy and platforms’ commercial interests against the case for conducting the research, and grant access to specific people for specific purposes. It would consider what data researchers may need to access. This is likely to include input and output data relating to online targeting systems, data that enables network analysis of systems, and access to tools to simulate personalised recommendations.

There should be robust checks and balances to ensure that more data is not provided than is necessary. To protect their commercial interests, platforms should have the right to appeal decisions made about access, and the right to raise concerns if they think this provision is being abused. There should be a strict liability regime for researchers who access platform data and the government may wish to consider the introduction of statutory penalties for researchers who use data inappropriately.

As researchers may be seeking access to personal data, the regulator should consult the ICO to develop a model that ensures that all access to data is provided in full compliance with the GDPR. The government could also ask the ICO to create a statutory code of practice for researcher access to platform data.

255 ‘Public statement from the Co-Chairs and European Advisory Committee of Social Science One’; Social Science One, 2019; https://socialscience.one/blog/public-statement-european-advisory-committee-social-science-one
data. This could involve clarification about the GDPR research exemption set out in Article 89, and the potential for the use of the “public task” basis for data processing.

It may be possible to adapt existing models for access to sensitive data. For example, the Office for National Statistics (ONS) Secure Research Service and the HMRC Datalab allow approved researchers access to de-identified datasets in accredited secure environments. The ONS secure research framework outlines five principles to ensure safe data access to unpublished datasets for research projects for the public good. The table below demonstrates how the ONS “Five Safes” model might be adopted in this context:

<table>
<thead>
<tr>
<th>Safety principle</th>
<th>ONS definition</th>
<th>Proposed model</th>
</tr>
</thead>
<tbody>
<tr>
<td>People</td>
<td>Only trained and accredited researchers are allowed access.</td>
<td>Only researchers affiliated with recognised academic institutions would be eligible, and they would be subject to ethics review approval by their institution.</td>
</tr>
<tr>
<td>Projects</td>
<td>Data are only used for valuable, ethical research that delivers clear public benefits.</td>
<td>Projects would secure ethical approval from researchers’ home institutions. The expert body would only approve research proposals that are aligned with public policy objectives.</td>
</tr>
<tr>
<td>Outputs</td>
<td>All research outputs are checked to ensure they cannot identify data subjects.</td>
<td>Research outputs would be checked by relevant stakeholders to ensure that they cannot disclose personal or commercially sensitive information.</td>
</tr>
<tr>
<td>Data</td>
<td>Only de-identified data is accessible.</td>
<td>Regulator would consult the ICO on approaches to de-identification and other techniques that may be used to ensure that high standards of privacy and security are met.</td>
</tr>
<tr>
<td>Settings</td>
<td>Data is only accessible via secure technology systems.</td>
<td>Different forms of secure data access would be required, depending on the security risks. At one extreme, this could involve access being restricted to specific computers in safe rooms, with the use of differential privacy techniques and the full monitoring of researcher activities and outputs. In some cases, it may only be possible to allow researchers access to partial datasets, or to require nondisclosure agreements to prevent wide publication of research on the data.</td>
</tr>
</tbody>
</table>
We recommend that the government or the online harms regulator provide funding to the body that controls access to data. This funding should also cover the costs of maintaining secure data facilities. Researchers’ time and resources should be funded via the UK Research Councils or other independent sources of funding. Platforms should be responsible for covering the costs of preparing data for access, and possibly the costs of training researchers to use the datasets and other tools.

Mandatory advertising archives

In Chapter 2 we discuss the risks associated with the lack of public scrutiny over targeted online advertising, and the limitations of voluntary approaches to enable greater public scrutiny. In Chapter 3 we explain that people want greater levels of public scrutiny over targeted online content. Only 18% of people trust political parties to personalise the content users see and target them with advertising in a responsible way.

We recommend that the Online Harms Bill includes a requirement for online platforms to enable public scrutiny by hosting publicly accessible advertising archives. This would support regulators, civil society, and the media to hold advertisers to account and increase incentives on advertisers and platforms to use online targeting responsibly. The regulator should have powers to enforce compliance with these requirements, and should be required to consult with the Electoral Commission, the EHRC, and the ASA on its activities in relevant areas.

There are three areas where higher levels of transparency should be prioritised: political adverts, “opportunity” adverts (adverts for jobs, credit and housing) and adverts for age-restricted products. In the case of political adverts, transparency over the content and targeting of adverts is necessary to avoid the undermining of democratic process. In the case of opportunity adverts and adverts for age-restricted products, it is necessary for the effective functioning of the Equality Act 2010 and the CAP code respectively.

1. Political advertising

It is essential that political advertising content is available for public scrutiny to enable the media and civil society to hold online claims to the same standard as in traditional political communications. While we welcome the progress made by a number of platforms to date, there is a need for common standards. We recommend that the government include measures about political advertising archives in its expected consultation on electoral integrity.

The full range of political advertisements should be available in advertising archives. However it is not always clear what constitutes a “political”, “social” or “issue” advert. We recommend that the regulator consults to agree a shared definition of “political” in this context. The definition of “political” should be broad enough to include adverts paid for by groups that are campaigning for political outcomes, not just electoral outcomes, such as lobbying or corporate
social responsibility campaigns. It should not be restricted to adverts in tightly-defined electoral periods. The definition should be reviewed at regular intervals.

We would be happy to work with existing regulators, platforms and civil society to develop a working definition that could be used to promote a self-regulatory approach before the Online Harms regulator becomes functional.

Political advertising archives should include data about the source of the advert, how it was targeted and who saw it, as set out in the following table:

Table 5: content of political advertising archives

<table>
<thead>
<tr>
<th>Content</th>
<th>The content of the advert itself, including an advert category and an advert description.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial transparency</td>
<td>The amount spent on the advertising campaign. Information about who paid for the advert.</td>
</tr>
<tr>
<td>Who was the intended target audience</td>
<td>Information about the intended target audience of the advert. The methods and tools used to carry out the targeting.</td>
</tr>
<tr>
<td>Impact</td>
<td>Aggregated information about the types of people who actually saw the advert. Engagements and interactions with the advert beyond viewing, such as numbers of “click-throughs” and “shares” of the advert.</td>
</tr>
</tbody>
</table>

Given the large number of adverts that are tested, it is important that the information contained in these archives should be easy to analyse. As such it should be made available through application programming interfaces (APIs) to enable information from different archives to be compiled in one place and compared. Where possible, there should be consistency in the formats and accessibility regimes across advertising archives, with similar technical specifications used for other types of advertising archives. There should also be a requirement to ensure that advertising archives function properly, especially at critical periods like elections.257

Information about who paid for the adverts should include a unique code for each organisation, which should be consistent across all advertising archives. This would make it possible to compare and examine the activities of different organisations across multiple pages or accounts on the same platform, and across multiple platforms.

The ICO is currently consulting on a code of practice for the use of personal data in political campaigning. The draft code considers that psychographic analytics and psychometric profiling could be considered a breach of GDPR. **We encourage the ICO to audit non-party campaigners as well as political parties for their use of data** to provide assurance to the public that conduct is fair and proper. This should be conducted in close cooperation with the Electoral Commission. The government should ensure that both the Electoral Commission and the ICO are able to share information.

While it is out of scope of our review, we would encourage the government’s consultation on electoral integrity to consider whether campaign finance rules need to be modernised to take into account the rise of digital campaigning.

**2. Opportunity advertising**

The Equality Act 2010 (EA10) makes discrimination against people with nine protected characteristics unlawful.258 As we set out in Chapter 2, the targeting of opportunity adverts, such as job adverts, could lead to unlawful discrimination in three ways: through direct discrimination (where advertisers choose to target people in a discriminatory way), indirect discrimination caused by market effects (where advertising auctions lead to discriminatory outcomes) and effects of algorithmic optimisation (where online targeting systems are biased). As outlined in Chapter 3, the people we interviewed all thought that discrimination of this kind should be made impossible, and expected there to be a mechanism in place to establish whether the law has been broken if concerns are raised.

Currently, it is difficult for a user or regulator to know whether a user has been targeted in an unlawfully discriminatory way. **We recommend that aggregate demographic information about the reach and impressions of these “opportunity” adverts is included in publicly accessible advertising archives.** This would allow regulators and civil society groups to identify potential unlawful discrimination and take action to hold advertisers to account.

These advertising archives should include:

- The content of the advert, including an advert category and advert description.
- Aggregated information about the types of people who actually saw the advert, including their age and sex (to enable an assessment of indirect discrimination).
- Contextual data about the industry, for example where a particular group is under-represented, such as women in construction.

258 Age; disability; gender reassignment; marriage and civil partnership; pregnancy and maternity; race; religion or belief; sex; sexual orientation.
While there are nine protected characteristics, we suggest that only those characteristics routinely collected by platforms, such as sex and age, should be included. Regulation should not incentivise platforms to process special category data to make predictions about users’ protected characteristics. Our upcoming report into bias in algorithmic decision-making will consider issues around the collection of data on protected characteristics.

The government should work with platforms, civil society and regulators to agree a shared definition of opportunity adverts based on the Equality Act.

3. Age-restricted products

The ASA’s CAP code includes requirements to restrict the targeting of certain online adverts for people under the age of 18. This includes adverts for alcoholic drinks, gambling, electronic cigarettes, and foods or soft drinks high in fat, salt or sugar (HFSS).

The lack of transparency around how these types of adverts are targeted online makes it difficult for the ASA to hold advertisers to account. While the ASA has been able to identify some inappropriately targeted adverts through its use of avatars, it has not been able to do this in platform environments. We recommend that adverts for these types of products are included in publicly accessible advertising archives so that the ASA and civil society organisations can check that advertisers are using online targeting responsibly.

Table 6: Summary of advertising archives standards

<table>
<thead>
<tr>
<th>Political adverts</th>
<th>Opportunity adverts</th>
<th>Age restricted adverts</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Content</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The content of</td>
<td>The content of the</td>
<td>The content of the</td>
</tr>
<tr>
<td>the advert,</td>
<td>advert itself,</td>
<td>advert itself,</td>
</tr>
<tr>
<td>including</td>
<td>including advert</td>
<td>including advert</td>
</tr>
<tr>
<td>advert category</td>
<td>category and</td>
<td>category and</td>
</tr>
<tr>
<td>and description.</td>
<td>description.</td>
<td>description.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Intention</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information about</td>
<td>N/A (this is likely</td>
<td>N/A (this is likely</td>
</tr>
<tr>
<td>the intended target</td>
<td>to be commercially</td>
<td>to be commercially</td>
</tr>
<tr>
<td>audience of the</td>
<td>sensitive information)</td>
<td>sensitive information)</td>
</tr>
<tr>
<td>advert.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>How the targeting</td>
<td></td>
<td></td>
</tr>
<tr>
<td>was carried out.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Recommendations

<table>
<thead>
<tr>
<th>Impact</th>
<th>Political adverts</th>
<th>Opportunity adverts</th>
<th>Age restricted adverts</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Aggregated information about the types of people who actually saw the advert.</td>
<td>Aggregated information about the types of people who actually saw the advert. (e.g. age and sex)</td>
<td>Aggregated information about the types of people who actually saw the advert. (e.g. age)</td>
</tr>
<tr>
<td></td>
<td>Engagements and interactions with the advert beyond viewing, such as numbers of “click-throughs” and “shares” of the advert.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Additional information</th>
<th>Political adverts</th>
<th>Opportunity adverts</th>
<th>Age restricted adverts</th>
</tr>
</thead>
<tbody>
<tr>
<td>The amount spent on the advertising campaign.</td>
<td></td>
<td>Appropriate data about the demographic representation in the sector, for comparative purposes.</td>
<td>N/A</td>
</tr>
<tr>
<td>Information about who paid for the advert.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Greater collaboration to prevent coordinated inauthentic behaviour

In Chapter 2 we set out how online targeting systems can also be exploited by third parties, including enabling networks of malicious actors to engage in potentially harmful coordinated inauthentic behaviour (CIB).

To address this, **we recommend the establishment of formal mechanisms for collaboration to tackle CIB on online platforms.** These mechanisms would facilitate greater coordination between platforms to identify and tackle CIB, facilitate sharing of best practice between platforms, and provide society with assurance that CIB is being tackled in a way that is coherent with human rights, including the freedom of expression of genuine users.

We propose the establishment of a body that connects online platforms to share information and strategies for identifying CIB, develop shared definitions, support new entrants and smaller firms, and collaborate with civil society. **The UK government should actively push for the establishment of such a body.** This could draw from existing models such as the Global Internet Forum to Counter Terrorism, and will need to embed principles of transparency and respect for freedom of expression.

---

260 ‘Global Internet Forum to Counter Terrorism: Evolving an Institution’, Global Internet Forum to Counter Terrorism; https://gifct.org/about/
In addition to this, collaboration could be improved at various other levels. These include:

- International multi-stakeholder collaboration, such as through a multilateral forum enabling authoritative civil society organisations to raise concerns and discuss with platforms. A forum like this would aim to provide assurance to wider society that the methods used by online platforms protect the rights and interests of genuine users.

- International governmental collaboration, such as through a forum involving governments with similar values. This would be a method for democracies to share insights and provide a means for coordinated governmental responses to hostile state actors operating inauthentic networks across multiple states.

- International regulatory collaboration, such as through a forum comprising relevant regulatory bodies such as electoral commissions and online regulators.

**User empowerment**

In Chapter 3, we set out the findings of our public engagement, which shows that people want to be able to better control their online experiences. Greater levels of user information, control and choice would enable users to navigate the online space more responsibly. The cognitive burden on people to do this is significant, so the government, regulators and businesses should also pursue more innovative approaches to enable people to take control as efficiently as possible.

**Online platforms’ provision of information and user controls**

Online platforms should improve the information and controls they offer to users. People should be able to find out whether content is being targeted and why. They should have more control over whether they are targeted and user controls should be easier to understand and use. Platforms’ policies, rules and appeal mechanisms need to be clearer.

Civil society organisations have proposed a range of improvements, from providing an option for users to see a different point of view\(^{261}\) to increasing informational cues (e.g. labels and pop-ups) about the type of content they may be viewing.\(^{262}\) Platforms could introduce tools to allow users to actively curate their own content, which enhances personalisation and can improve

---

261 T Garton Ash, R Gorwa, & D Metaxa, ‘GLASNOST! Nine ways Facebook can make itself a better forum for free speech and democracy’, Reuters Institute for the Study of Journalism and the Hoover Institution, 2019; https://reutersinstitute.politics.ox.ac.uk/our-research/glasnost-nine-ways-facebook-can-make-itself-better-forum-free-speech-and-democracy

Recommendations

the recommendation system. While participants in our public dialogue were keen that changes to the user experience create as little friction as possible, the broadly positive reaction among participants to the mock-up stimulus we used to illustrate how new features could look and work in practice suggests that this is achievable.

The CMA has found that platforms’ default settings have a strong influence on the ability of platforms to collect and use data about their users, and the ability of users to control their online experiences. Default settings may be of particular importance when considering the needs of children and other vulnerable people – indeed, participants in our public dialogue supported changes to default settings to protect vulnerable users.

There are a number of specific areas of relevance to online targeting that we address below.

1. Labels on political posts

People should know if political content they are targeted with online is paid for and how it has been targeted at them. This would give them the context to know if the message they see is being shared with just a small group or wider society. The government’s proposed imprints regime for online electoral adverts should establish a clear visual distinction between paid-for content and other content. It should also give users some basic information to show that they have been targeted with the content they are seeing. This could include the targeting criteria used, or the number of other people who have been targeted with the same content, with clear easy-to-use options to find more information.

“Electoral” adverts are those bought and distributed with an intention of a specific electoral outcome, such as gaining support for a political party’s candidate to be elected. “Political” adverts are intended to support more general political outcomes, such as raising awareness of a climate campaign. The government should consider extending the mandatory imprints regime to political adverts as well as electoral adverts.

---

264 ‘Online platforms and digital advertising market study’, Competition and Markets Authority, 2019; www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study
2. Signalling influencers’ advertising activity

The CMA\textsuperscript{266} and ASA\textsuperscript{267} have both produced guidance to ensure influencer compliance, including on labelling posts (consistent with consumer protection rules that prohibit unlabelled paid-for editorial content). ASA research has shown that consumers are likely to have difficulty in differentiating advertising content where it is presented in a similar style to the editorial content in which it sits. It has also shown that the wide variety of different labels currently in use, their placement and their visibility, make it more difficult for people to develop critical awareness needed to identify advertising.\textsuperscript{268} The government’s review of online advertising regulation should investigate the effectiveness of these measures to raise consumer awareness of paid for content.

3. Increased coordination of public education and awareness campaigns

Regulators, working with industry and civil society organisations, should consider increasing coordination on their planned and ongoing public education and awareness campaigns in relation to digital, data and media literacy. There are a large number of relatively small campaigns ongoing simultaneously, which could benefit from coordination and expert input to maximise their effectiveness. This is in line with our analysis of public attitudes, as participants in our public dialogue called for greater efforts to raise awareness of online targeting.

4. Third-party mechanisms

In addition to improvements to the way online service providers seek to empower their users, we believe that there is significant potential value in a third-party online safety ecosystem, in which third-party mechanisms can operate across platforms and other online service providers to support the interests of users in privacy-protecting ways. We recommend that government and regulatory policy support these solutions, especially where online service providers are required to identify users’ vulnerability, as they offer greater control to users. Third-party providers of age-verification solutions like Yoti\textsuperscript{269} and of gambling self-exclusion solutions like Gamban\textsuperscript{270} are examples of third-party mechanisms that empower users and support online safety.

Solutions like these could also help meet the desire outlined in our public dialogue for people to be able to set their preferences across multiple online service providers in one place. As the CMA has pointed out, an example of this

\textsuperscript{266} ‘Social media endorsements: being transparent with your followers’, Competition and Markets Authority, 2019; www.gov.uk/government/publications/social-media-endorsements-guide-for-influencers/social-media-endorsements-being-transparent-with-your-followers


\textsuperscript{268} ‘Labelling of influencer advertising’, Advertising Standards Authority, 2019; www.asa.org.uk/resource/labelling-of-influencer-advertising.html

\textsuperscript{269} Yoti; www.yoti.com

\textsuperscript{270} Gamban; https://gamban.com
sort of approach is in the European Commission’s original draft of the proposed ePrivacy Regulation and the accompanying impact assessment, which highlights the need to “empower end-users” via “centralising consent”.271

As we note in Chapter 4, the adoption of interoperable standards could enable the emergence of data intermediaries. We believe that this offers significant longer-term potential to improve data governance and rebalance power towards users. However, it is unlikely to happen without public policy support. **We recommend that government and regulatory policy supports the development of data intermediaries.** Public policy could explore the benefits of a regulatory or self-regulatory accreditation system for data intermediaries, and a digital sandbox to develop interoperability and open API standards between intermediaries and digital services. While implementing regulation would take time, the value of creating alternative mechanisms of data governance increases as the volume of personal data that is generated and the number of ways it is used grow and the risks of harm resulting from this increase.

**The role of regulation in user empowerment**

We were disappointed to note that the CMA found that very little testing is done by online platforms in relation to consumer control over data and use of privacy settings, in contrast to the very extensive trialling it found was carried out on a daily basis in other parts of the business.272 **We recommend that the provision of user information and controls over online targeting systems are considered a key part of compliance assessments** under the relevant regulatory regime, as decided through the regulatory coordination mechanisms detailed above. This means that organisations will need to document their testing and justify their decisions about the level of information and control given to users. Relevant regulators including the ICO, the CMA or Digital Markets Unit, and the online harms regulator should work together to develop guidance about best practice, working with industry and civil society organisations.

**In this light, we support the CMA’s proposed “Fairness by Design” duty on online platforms.** As described in Chapter 4, this is a proposal for platforms to design consent and privacy policies in a way that facilitates informed consumer choice, and which would complement existing data protection by design requirements under the GDPR. We note that the CMA or Digital Markets Unit, the ICO, and the online harms regulators may jointly regulate compliance with this in cases assigned to them through coordination mechanisms. In particular, we support the requirement for high-risk platforms to trial and test the choice architecture they adopt, which would be reviewed by the appropriate regulator to ensure that it is supported by evidence on consumer behaviour.


272 ‘Online platforms and digital advertising market study, Appendix F: Consumer control over data collection’, Competition and Markets Authority, 2019; www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study
Support for promoting competition

The CMA has found that Google has significant market power in the general search sector and that Facebook has significant market power in the social media sector.273 This reinforces the views of participants in our public dialogue who were frustrated with the lack of real alternatives to the large online platforms. We strongly support the work of the CMA and others to incentivise greater competition online and enable greater choice. As the CMA highlights: effective competition in a market is crucial for securing good outcomes for consumers; equally high standards of consumer protection drive competition on things that matter to consumers.274

273 ‘Online platforms and digital advertising market study’, Competition and Markets Authority, 2019; www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study
274 ‘Online platforms and digital advertising market study’, Competition and Markets Authority, 2019; www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study
### Appendix 1: Targeting options on major online platforms

<table>
<thead>
<tr>
<th></th>
<th>Google</th>
<th>Facebook</th>
<th>Amazon</th>
<th>Pinterest</th>
<th>LinkedIn</th>
<th>Twitter</th>
<th>Spotify</th>
<th>TikTok</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Contextual</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Search</td>
<td>Keyword</td>
<td>No</td>
<td>Keyword</td>
<td>Keyword</td>
<td>Based on Bing searches</td>
<td>Keyword</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>Declared</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Basic demographics</td>
<td>Age range, gender, parental status</td>
<td>Age range, gender, relationship status, education level, job title, location</td>
<td>Age, gender, language, location</td>
<td>Age, gender, education job experience, language, location</td>
<td>Age, gender, location</td>
<td>Age, gender, location, language</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom lists</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Declared and Inferred</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Interests</td>
<td>Yes</td>
<td>Page-likes, posts, comments, ads clicked</td>
<td>Yes</td>
<td>Yes</td>
<td>Member Interests and Member Groups</td>
<td>Interests, movie and TV shows, “tweet engager”</td>
<td>Podcast, playlist, platform preferences</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Inferred</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Behaviour</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>Behaviour, conversation</td>
<td>Playlists, activities (cooking, gym etc.)</td>
<td>N/A</td>
</tr>
<tr>
<td>Friends’ activity</td>
<td>N/A</td>
<td>Yes</td>
<td>N/A</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>N/A</td>
<td>No</td>
</tr>
<tr>
<td>Location</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>“Lookalikes”</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Appendix 2: Platform recommendation systems

<table>
<thead>
<tr>
<th>Organisation</th>
<th>Default use of content recommendation systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon</td>
<td>Amazon recommends items and categories of items, including “featured” recommendations to its users on its home page, the Your Amazon page, and on product pages, where Amazon shows users similar items, items viewed by other users, and items other users ultimately purchase after viewing the product. When adding products to the basket, sponsored and similar items are also recommended.</td>
</tr>
<tr>
<td>BBC</td>
<td>BBC iPlayer makes recommendations to signed-in users based on what content they have previously watched. Users can opt out of personalised recommendations in their account settings.</td>
</tr>
<tr>
<td>Bing (Search)</td>
<td>Bing search is a research tool that generally does not recommend content to a user. Instead it shows the results that are most relevant and authoritative as related to the specific query entered. Bing does have a “related searches” feature that recommends similar search queries that can help the user further refine their search results, which is algorithmically generated based on queries other users have typed.</td>
</tr>
<tr>
<td>Facebook</td>
<td>Facebook algorithmically curates a feed of content (News Feed) determined to be most likely to result in the user interacting with other users on the platform, referring to this goal as encouraging “meaningful social interaction”. Facebook also provides recommendations to users, for instance for pages similar to those already liked by the user, and “People you may know”.</td>
</tr>
<tr>
<td>Google (Search)</td>
<td>Google reports that its search algorithms look at “many factors”, including the words of a user’s query, relevance and usability of pages, expertise of sources and user location and settings. The weight applied to each factor varies depending on the nature of the query. For example, the freshness of the content plays a bigger role in answering queries about current news topics than it does about dictionary definitions.</td>
</tr>
<tr>
<td>Instagram</td>
<td>Instagram algorithmically ranks posts, including adverts, for users to see (unlike other platforms, Instagram provides no option for a chronological display). It also recommends other people to follow alongside the content feed. The Explore page displays a list of suggested users, recommended content, and adverts.</td>
</tr>
</tbody>
</table>

---

### Organisation | Default use of content recommendation systems
---|---
**LinkedIn** | LinkedIn recommends content based on other users’ behaviour with features like “People Who Viewed This Profile Also Viewed”, the “People Who Viewed This Job Also Viewed”, and other items of content such as company and group.

**Pinterest** | Pinterest recommends content for users based on the “pins” users have previously engaged with and topics they follow. Recommendations are shown on the home page, through search results, and alongside content.

**Snapchat** | Snapchat infers users’ interests to recommend content on Discover, its platform for news and entertainment, based on the Discover content that users have watched or engaged with. Users can view their inferred interests – called “Lifestyle Categories” – in their Snapchat settings, turn off categories which aren’t relevant to them, or opt into new ones. Discover content is provided by professional third-party publishers, and curated prior to upload, or by popular pre-moderated public accounts.

**TikTok** | TikTok recommends content on its For You feed, which is shown by default when a user opens the app. This feed features content from users who have chosen to make their account public, and includes advertisements. Recommendations are based on several factors including inferred and declared demographics and user behaviour, such as the videos users have viewed, shared and liked.

**Twitter** | Twitter algorithmically ranks tweets and retweets by followed accounts in a user’s feed, interspersing these with a selection of recommended content (likes, replies, and so on). Recommended “top tweets” are shown at the top of the user’s timeline. “Trending” topics are shown alongside the timeline, as are suggested accounts to follow.

**YouTube** | YouTube recommends videos on the home page, alongside videos, and after each video finishes (a recommended video will play automatically after a short period of time). These are based on recent uploads, popularity, and (for logged-in users) subscribed channels, the users’ interests and viewing history.
Appendices

Appendix 3: Online targeting and machine learning

How is machine learning used in online targeting?

This description is based on publicly available information at the time of publication and may not perfectly represent the intricacies of commercially confidential algorithms.

1. Deep learning is a powerful pattern recognition technique. This can be used by online targeting systems to draw relationships between content. An example of how deep learning can be applied to online targeting content is when a machine learning system takes content (e.g. natural language, images, video) and breaks it down into components, which can be assigned mathematical values as “vectors”. It then processes components in relation to each other to identify patterns in the way humans interact with the content online.

2. Google’s RankBrain, for instance, converts the text of new search queries into “word vectors”. Word vectors that are close in value, because they appear in similar sentences or contexts, are linguistically related. A system can then relate similar concepts (through common combinations of vectors) to produce a more relevant result without relying on keyword based searches, or uniquely identify content based upon differing combinations of vectors.

3. Recommendation systems like this work because they are informed by the ‘user journey’. A video site may relate a video about cooking Thai red curry to another video about cooking Thai green curry, because it processes [“Thai”], [colour], [“curry”] and recognise that users often seek out Thai green curry video recipes after they have watched Thai red curry video recipes. The vector approach means that the system will recognise high associations for the colours red, green and yellow, but lower associations for the colour blue, and will push the related videos together in recommendations.

4. The system does not assess the content like a human moderator does, or even know what the content is. What it does is map the relationship between data points.

5. Vectors, values and “dimensions” (broad kinds or contexts of vectors) may or may not correspond to the things people would naturally identify or recognise about a piece of content. In the above example it does not know what a curry is, what a recipe is, or what a colour is. If users click from Thai green curry recipes to videos of funny cats in sufficient numbers, it will make a connection between Thai green curry and funny cats, whereas humans would not.

6. When recommendation engines recommend content in a way that may cause harm, such as increasingly extreme content, there is no way for the system to recognise this unless the content is labelled. The system is simply recognising a pattern.

What does this mean for online targeting?

The operators have, in the main, recognised that they have a responsibility to understand what content is being recommended to people by their systems and to operate the system within ethical parameters.\(^\text{277}\)

Content is disseminated according to mathematical values the system has assigned it. A machine alone cannot appraise that content in context as a human can. As such, if constraints cannot be specified in a form a machine can easily interpret, it may recommend content in a way a human curator would not. A machine has no capacity to make judgments about content, let alone to understand the nuance of various interpretations of content as human curators or users have based on language, context cultural values and many other factors.

Operators can respond to this situation in different ways:

- Operators can introduce another machine learning system which has been trained to recognise illegal content. It is trained on a dataset of unacceptable content to better recognise when this content is uploaded. This automatic moderation identifies content and removes it from either the targeting results or bans it from the platform. This is the approach operators use to detect child sexual abuse images and terrorist content. There may be some false positives, but because it tends to be distinct from mundane content this is less likely. However, the nuance of categories of content like hate speech or satire make this system difficult to deploy in the case of “harmful but legal” content, where it may impact freedom of expression.

- Operators can compare the vectors to human descriptions of content, translating them to human understanding. Operators will have their own ways of doing this, and the accuracy of these translations vary. Approaches can be assessed by comparing their outputs. To have consistent application of rules about targeting of content there needs to be a way of comparing the consistency of different organisations’ approaches to defining violence based on sample output.

- Operators can impose rules on the way machines are able to represent content or the way vectors can be used or related. However, this approach – second-guessing machine learning systems – arguably defeats the point of using them in the first place.

As machine learning approaches to organising content can lead to unpredictable outcomes, it is important for policymaking to apply the correct expectations and standards to them.

\(^{277}\) Associated Press, ‘Facebook is ‘responsible for the content’ on its platform, Zuckerberg says’ in ‘PBS NewsHour’, 2018; www.pbs.org/newshour/nation/facebook-is-responsible-for-the-content-on-its-platform-zuckerberg-says
Appendices

Appendix 4: The current regulatory framework

Our analysis of current arrangements is based on publicly available information, including the relevant legislation and information published by regulators, and on interviews with seven regulators.\(^{278}\) We consider:

- The Information Commissioner’s Office (ICO)
- The Competition and Markets Authority (CMA)
- The Advertising Standards Authority (ASA)
- Ofcom
- The Financial Conduct Authority (FCA)
- The Gambling Commission are sectoral regulators
- The Electoral Commission
- The Equality and Human Rights Commission (EHRC)

We explain below what these regulators do and how it is relevant for online targeting.

The Information Commissioner’s Office

The ICO is the UK’s independent regulator for data rights. It is responsible for data privacy for individuals under the Europe-wide General Data Protection Regulation (GDPR) and the complementary UK Data Protection Act 2018 (DPA 2018).

The ICO also enforces the Privacy and Electronic Communications Regulations (PECR) 2003, which govern direct marketing carried out electronically. Where personal data (and other information) is obtained by use of non-essential cookies or similar technologies on a user’s terminal equipment this is regulated by PECR which requires informed and specific consent from the user.

The GDPR covers processing of personal data by companies and other organisations. All forms of online targeting involve some, if not all, of the operations to which the GDPR applies. The ICO is therefore an important part of the current regulatory framework around online targeting. However, under the GDPR, the lead supervisory authority for a data controller or processor carrying out cross border processing is the country of its main establishment in the EU. This means that the ICO is not currently the lead supervisory authority for all data controllers, including most of the major platforms: Facebook and Google are located in Ireland.

\(^{278}\) We did not interview the Equality and Human Rights Commission.
The ICO is required to publish various codes of practice, some of which are relevant for different applications of online targeting. These include an age appropriate design code. The code provides guidance on the design of online services that are likely to be accessed by children and includes consideration of appropriate use of children’s data for profiling, personalisation of services, and content recommendation (see Box 4). The ICO has also consulted on a framework code of practice for the use of personal data in political campaigning, including through targeted online advertising.

The ICO’s Regulatory Action Policy sets out its approach to enforcement of data privacy rules. It focuses on cases involving highly sensitive information, adversely affecting large groups of individuals, and/or impacting vulnerable individuals. As a general principle, more serious, high-impact or repeated breaches can expect stronger regulatory action. As we set out in Chapter 2, online targeting may represent a greater risk to people who may be vulnerable.

The ICO is reviewing how personal data is used in real time bidding in programmatic advertising. It published a report in July 2019 in which it concluded that “the adtech industry appears immature in its understanding of data protection requirements”, that “individuals have no guarantees about the security of their personal data within the ecosystem”, and identified illegal processing of personal data, including special category data.

The ICO has a range of powers to carry out its work:

- It can require organisations to provide information.
- It can issue assessment notices that enable it to assess whether an organisation is complying with data protection regulation.
- Where it finds a breach of data protection regulation, it can issue an enforcement notice telling the organisation what it needs to do to bring itself into compliance (including the power to instruct an organisation to stop processing).
- It can impose significant financial penalties for breaches: up to €20m or 4% of annual total worldwide turnover.

---


Appendices

20 The ICO has launched a sandbox service to support organisations that are developing products and services that use personal data in innovative and safe ways.284 Sandboxes (secure testing environments) provide a way for firms to access regulatory expertise while developing new products, and can also be used by regulators in developing policy, or assessing compliance with regulation.

The Competition and Markets Authority

21 The CMA is an independent non-ministerial government department. The CMA has a statutory duty to seek to promote competition for the benefit of consumers across all sectors.

22 One of the CMA’s priorities for 2019/20 is promoting better competition in online markets. In 2019 it launched its digital markets strategy, following the recommendations of the Furman report for regulation of digital markets.

23 In July 2019 the CMA launched a market study into online platforms and digital advertising. In December it published its interim report, which we discussed in Chapter 2.285 The interim report concluded that:

- Competition and market entry may be leading to lack of choice and higher prices for consumers, and may potentially be undermining the viability of publishers including newspapers.

- Default settings (for example, Google as the standard search engine on Apple devices)286 strengthen market positions, as may the collection of personal data, which allows Google and Facebook to target ads and content more effectively.

- Users do not feel in control of their data: they can’t always opt out of personalised advertising and find it difficult to access privacy settings. This means most people use default settings, which may result in them giving up more data than they would like.

24 Other CMA work relevant for online targeting includes its 2018 paper on algorithmic collusion and personalised pricing.287

25 The CMA has a number of different regulatory tools:

- It can carry out market studies and market investigations to explore markets that are not working for consumers.

Appendices

- It enforces competition law in the UK. It shares this work with a number of sectoral regulators (including Ofcom and the FCA) under the concurrency regime, where regulators agree which of them is best placed to carry out an investigation.

- It can assess proposed and completed mergers and their potential impact on competition.

- It has consumer protection powers, shared with other bodies, to support its competition work.

26 The CMA has broad information gathering powers to obtain the information it needs to carry out its work. It can impose significant financial penalties where it finds that companies have not complied with the law. It can impose remedies to make markets work more effectively, and can impose conditions on or block mergers where it finds that they would reduce competition.

27 The CMA’s Data, Technology and Analytics (DaTA) unit, established in 2018, is developing the CMA’s capacity and skills in data engineering, machine learning and artificial intelligence techniques. It can use the CMA’s information gathering powers to understand how algorithms work and what impact they have on users.

The Advertising Standards Authority

28 The ASA regulates advertising in all media.288 Unlike the other regulators we consider, the ASA is funded by industry. The ASA sets and enforces against a significant number of advertising rules on a self-regulatory basis.

29 The ASA also operates co-regulatory relationships with national Trading Standards, which has powers in relation to advertising in breach of unfair commercial practices legislation including misleading advertising (which makes up over 70% of the ASA’s workload); the Gambling Commission, the ICO and the CMA. In relation to broadcast advertising, Ofcom has formally contracted the ASA to carry out some of its statutory functions under a co-regulatory arrangement.289 This includes advertising on on-demand programme services and will extend to advertising on VSPs under the provisions of the AVMSD. In the financial services sector the FCA sets and enforces rules in addition to the general standards enforced by the ASA.290 The ASA describes these arrangements as “collaborative regulation”.

288 The ASA enforces the Advertising Codes, which are written and maintained by the Committees of Advertising Practice. Funding arrangements are the responsibility of the independent Advertising Standards Board of Finance (ASBOF) and Broadcast Advertising Standards Board of Finance (ASBBOF), which collect a levy from advertisers to fund the ASA’s work. These arrangements are known as the ASA system.


290 The ASA does not cover political advertising. ‘Why we don’t cover political ads’, Advertising Standards Authority, 2019; www.asa.org.uk/news/why-we-don-t-cover-political-ads.html
Paid-for online advertising, including targeted advertising, is covered by the rules in the ASA's Code of Non-Broadcast Advertising and Direct & Promotional Marketing (CAP code). The CAP code includes a number of rules preventing or restricting the targeting of certain adverts (for age restricted products and HFSS foods) to children. Advertisers, not the online platforms they use to advertise, are primarily responsible for following the CAP code, but publishers and other intermediaries share a secondary responsibility for compliance. The CAP code also covers advertising claims made on advertisers' own websites and other non-paid-for space under their control, for example organic Facebook posts, tweets, and influencer marketing in social media.

The ASA's current strategy, More Impact Online, aims to improve the regulation of online advertising. This includes addressing misleading content and inappropriate targeting, and working more closely with platforms (which provide the tools for advertisers to target their adverts online). The ASA's work to date under this strategy has included using child avatars (online profiles which simulate children's browsing activity) to detect inappropriate targeting of gambling and junk food adverts at children and take enforcement action accordingly.

As it is not a statutory regulator, the ASA does not have information gathering powers, although it works with statutory partners that do and has an established programme for gathering data informally. It does not have formal sanctions or fining powers, but its decisions have a reputational effect and can generate negative publicity for the advertisers concerned. It has a range of non-statutory sanctions for non-compliance, such as withdrawal of access to advertising space. It works with a number of regulators that have formal 'backstop' powers in different areas: the ICO, Ofcom, the Gambling Commission and the FCA. It can refer illegal advertising to Trading Standards.

The advertising industry has developed other self-regulatory initiatives not enforced by the ASA. The Internet Advertising Bureau UK (IAB UK) Gold Standard is a certification scheme, which aims to reduce ad fraud, improve the digital advertising experience and increase brand safety. The Coalition for Better Ads, whose members include the IAB as well as Google, Facebook and Microsoft, has also developed a set of standards for online advertising.

---

295 ‘Work with the Advertising Standards Authority’, National Trading Standards; www.nationaltradingstandards.uk/work-areas/work-with-asa/
296 IAB UK Gold Standard, Internet Advertising Bureau; www.iabuk.com/goldstandard
Appendices

Ofcom

Ofcom is the independent regulator for television and radio (both broadcast and on-demand programme services, like TV catch-up services), telecoms, post, and the radio spectrum. Its remit includes:

- Content standards for TV and radio programmes are captured in Ofcom’s statutory Broadcasting Code, parts of which also apply to on-demand programme services. Ofcom is expected to assume responsibility for regulating video-sharing platforms (VSPs) following the implementation of the revised Audio-visual Media Services Directive (AVMSD).298

- The AVMSD requires VSP service providers to develop systems to protect their users rather than regulating the content of VSP services (because VSP service providers do not have editorial control of the content). The rules for both on-demand programme content and VSP services cover protection of children, incitement to hatred, product placement and sponsorship, terrorism and pornography.

- Consumer protection: Ofcom has a principal duty to further citizen and consumer interests. In 2019 it announced its Fairness for Customers programme, which includes a project on personalised pricing in telecoms markets.

- Competition: Ofcom has concurrent powers to enforce competition law in communications markets where it is the regulator best placed to do so. To date, most of its competition work has been in telecoms and post markets, but Ofcom could also be well placed to act in some online markets.

Ofcom has a standalone duty to promote media literacy which covers broadcasting and electronic media. It fulfils this duty through the Making Sense of Media programme, which has included qualitative and quantitative research into people’s attitudes to online harm.299

Ofcom has broad information gathering powers. It also has various sanctions powers including fines and directions in competition and consumer protection. In broadcasting and video on demand cases, it can impose fines and ultimately remove licences.

Ofcom is building capacity in data skills through the creation of its Data Hub team300 and has launched a data science graduate scheme.

298 Where “the principal purpose of the service or of a dissociable section thereof or an essential functionality of the service is devoted to providing programmes, user-generated videos, or both, to the general public, for which the video-sharing platform provider does not have editorial responsibility.” (Article 1 AVMSD).


300 ‘Engineering careers’, Ofcom; www.ofcom.org.uk/about-ofcom/jobs/engineering-careers
The Financial Conduct Authority

The FCA regulates financial services firms and financial markets in the UK. It has powers to enforce competition law in the financial services sector. The FCA requires firms to ensure, amongst other things, that their financial promotions are clear, fair and not misleading and make any risks clear. The FCA is able to take action when these rules are breached.

The FCA may be a valuable model for the regulation of online targeting and the broader regulation of online markets because:

- It regulates a large and valuable sector: 59,000 financial services firms, and financial markets that are crucial to the UK economy.

- The financial services sector uses data-driven systems on a large scale and the FCA has developed capability to regulate in this environment, including a data science graduate programme.

- It has broad information gathering powers, in particular a power to commission reports from “skilled persons” in support of both its supervisory and enforcement functions.301

- It supports innovation: the FCA provides a number of support services to innovative firms, including the Regulatory Sandbox which enables firms to test innovative products and services on a small scale in a controlled environment.302

- Its designated senior manager regime holds individual people to account for harms caused by financial services products, even where they are the result of a “black box” effect.

The FCA has also published draft guidelines on vulnerability, which set out its view on how firms can comply with existing requirements to treat customers fairly.303 Regulators all recognise the need to protect people who may be vulnerable (and some like Ofcom are required to consider vulnerable people in their regulation). But the FCA’s approach is broader: as well as recognising groups that may be particularly vulnerable (such as people with low resilience or poor health), the FCA recognises that vulnerability can be transient and that everyone could potentially become vulnerable. This may be a good model for online harms, particularly those caused by online targeting, where feedback loops mean that content recommendation systems can inadvertently target users’ vulnerabilities as we discussed in Chapter 2.

---

Appendices

The Gambling Commission

The Gambling Commission regulates gambling providers in Great Britain, and the National Lottery in the UK. It has the power to take regulatory action, including the removal of licences, against gambling operators and can also bring criminal prosecutions for gambling related offences. It works in partnership with the ASA and others to secure responsible advertising of gambling. It collects data and conducts research on the impact of (online) advertising on children, young people and vulnerable people.304

The Gambling Commission’s regulatory model may be relevant for online targeting in other ways:

– While the harmful effects of gambling are well documented, the mechanisms of harm, and the different ways that different people can be affected, are less clear. The National Strategy to Reduce Gambling Harms aims to build a more detailed understanding of gambling harms as a basis for more effective regulation.305

– As with online targeting, the companies responsible may not be in the UK. The Gambling Commission has developed technical solutions to block non-UK operators and established relationships with other international operators ie payment systems to stop harmful activity.

The Electoral Commission

The Electoral Commission is the independent body that oversees election spending and funding by campaigners in the UK. Targeted online political advertising presents challenges for the Electoral Commission’s campaign finance role, as it makes it more difficult to identify the source of funding, and whether adverts are compliant with registration and spending requirements.

The Equality and Human Rights Commission

The Equality and Human Rights Commission (EHRC) is a statutory body responsible for enforcing the Equality Act 2010 and encouraging compliance with the Human Rights Act 1998. Targeted online job adverts could unlawfully discriminate against people on the basis of their protected characteristics. This is relevant for the EHRC – as set out in its strategic plan, it is working to ensure that people in Britain have equal access to the labour market and are treated fairly at work.306

Appendix 5: Glossary

**Adtech**
Advertising technology – refers to intermediary services reliant on programmatic technology involved in the automatic buying, selling and serving of display advertisements.

**Algorithm**
A set of precise instructions that describe how to process information, typically in order to perform a calculation or solve a problem.

**Artificial Intelligence (AI)**
An area of computer science that aims to replicate human intelligence abilities in digital computers. AI currently refers mainly to systems that use machine learning for pattern detection, prediction, human-machine dialog, and robotic control.

**Autonomy**
Self-government and the opportunity to make decisions unimpeded and free from manipulation.

**Behavioural targeting**
A form of targeting which responds to tracking of online behaviours based on the gathering of data of sites visited, search terms and app activity in order to make predictions or to match content with prior behaviours.

**CAP code**
The Advertising Standards Authority (ASA)’s Code of Non-Broadcast Advertising and Direct & Promotional Marketing is the rule book for non-broadcast advertisements (including online), sales promotions and direct marketing communications. The CAP code also covers advertising claims made on advertisers’ own websites and other non-paid-for space under their control, for example organic Facebook posts, tweets, and influencer marketing in social media.

**Code of practice**
A code of practice (or code of conduct) is a document setting out standards of behaviour for organisations or individuals. Statutory codes of practice (those that are required by law) provide detailed practical guidance on how to comply with legal obligations.

**Concurrency**
The concurrency regime is a framework for the enforcement of competition law in the UK, under which the CMA and a number of designated regulators (concurrent regulators) can agree which is “best placed” to consider a case.
Country of origin principle
This is a principle developed to resolve potential regulator disputes when companies operate across national borders. Where a good or service is produced in one country and received in another, the laws and regulations of the country where production took place apply.

Data Protection Act 2018
A piece of legislation that updates UK data protection legislation and complements the GDPR. Among other things, it sets out the role of the Information Commissioner and requires them to prepare various codes of practice which contain guidance in relation to the GDPR.

Demographic targeting
Targeting which draws upon demographic data such as age, gender, occupation and location.

Deep learning
A multi-layered neural network approach which can recognise patterns through iteratively processing large amounts of data, and extracting successively more abstract or complex features with each layer.

Display advertising
The display of static or video ads alongside the content a user is interested in.

Equality Act 2010
The Equality Act 2010 is a piece of legislation that protects people from discrimination at work and in wider society. Discrimination is where someone is treated less favourably because of a protected characteristic. The protected characteristics are age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, and sexual orientation.

GDPR
The General Data Protection Regulation (2016/679) is an EU law on data protection and privacy and also addresses the transfer of personal data outside the EU.

Harm
Circumstances in which damage, injury or disadvantage is caused to the recipient.

Hashing
A process to allow matching data values to be identified while keeping the data hidden.
**Appendices**

**Machine Learning (ML)**
A class of AI methods that take data samples as input and produce a mathematical model of the sample data. Instead of requiring explicit programming of this model, ML algorithms identify patterns in data to extract information that can be used to reproduce or predict the behaviour of the system they are trying to learn about.

**Manipulation**
Attempting to influence someone’s behaviour without them being aware of how they are being influenced.

**Network Effects**
Network effects occur when, as more users join a platform, the platform becomes more valuable or appealing for existing and potential users.

**Neural Network**
A combination of mathematical operations (or ‘neurons’) which are joined together in a network, often in layers, and generally including input, output, and one or more ‘hidden’ layers. Feeding inputs through these layers (sometimes repeatedly) allows for a kind of trial and error based learning.

**Online targeting**
Online targeting means a range of practices used to analyse information about people and then customise their online experience. It shapes what people see and do online.

**Personalisation**
The tailoring of content to the individual user. This leads to internet users seeing different content. The processes of personalisation vary from recommendations through the various types of targeting discussed in Chapter 2 of this report.

**Platforms**
A term used to describe internet spaces that host a variety of features. Individuals create profiles in order to access those various functions and services.

**Vulnerability**
Potential or predisposition to be harmed.