Competition and data protection in digital markets: a joint statement between the CMA and the ICO

19 May 2021

CONTENTS

Foreword

The digital economy has the potential to have a hugely positive impact on people's lives, from improvements to public services to companies driving innovations that can make us healthier and happier. We think that this can best be achieved where digital markets are competitive, consumer and data protection rights are respected, and citizens are empowered to exercise meaningful control over their own data.

In our view, there are strong synergies between the interests of data protection and competition, as demonstrated by the close working relationship our regulators have developed in the last two years. This paper sets out how we will enhance the synergies between our policy agendas and, where we do identify the potential for tensions, explains how we will seek to address them.

Our aim is to build on the ambitious workplan published recently by the Digital Regulation Cooperation Forum. The workplan sets out in concrete terms how we are adopting a joined up approach to regulation across the digital regulatory landscape，with practical steps to reinforce our ability to cooperate and ambitious plans to support capability sharing, including secondment programmes, colocation of teams and the development of a shared centre of excellence. We are committed to developing and fostering a culture of cooperation and collaboration between our two organisations, and our offices are already working together on some of our most high-profile investigations, demonstrating how consumers will benefit from a collaborative approach.

The CMA's Competition Act investigation into Google's proposals to phase out support for third party cookies on its Chrome browser and replace them with a 'Privacy Sandbox' approach is a good example. As well as considering the impacts of the proposals on competition in digital advertising markets and on user experience, the investigation will build in consideration of data protection aspects by the ICO.

The ICO's investigation into the use of personal data in real time bidding in digital advertising is another example. The ICO's focus is on the data protection aspects of a system that processes the personal data of millions of people every day, with a series of audits underway, and the investigation will include consideration of the impact on competition by the CMA.

Our ambition, in these cases and more broadly, is to ensure our regulatory approaches can work together to benefit the UK. We want to ensure a digital ecosystem where people have a genuine choice over the service or product they prefer, with a clear understanding of how their data will be used to inform that decision. And we want businesses to compete on an equal footing to attract custom, with transparency in the way they operate to inform meaningful choices.

This is an ambitious goal, and one we are committed to achieving.

Andrea Coscelli and Elizabeth Denham

Introduction

Context

1. The rapid emergence and expansion of online services that now function on a global scale has posed substantial new challenges to governments and regulatory authorities around the world. This is, in part, due to the way the products and services offered by these firms cut across the previously well-established boundaries of markets, jurisdictions, and regulation. As a result, governments and regulatory authorities are having to think hard about the rules and laws that apply to the digital economy and its business models, including how they should be enforced, and where interventions can be made most effectively.

2. A consequence of this is that previously separate policy areas become interlinked, and different regulatory authorities are increasingly required to consider a given set of issues from the perspective of contrasting policy aims and objectives. A prime example of this is the intersection that has developed in the digital economy between the policy aims of promoting and protecting competition in digital markets and protecting the personal data of the users of digital products and services. There are many circumstances in which these two objectives are fully aligned, but we also benefit from recognising that this may not always be the case.

3. This joint statement from the Competition and Markets Authority (CMA) and the Information Commissioner's Office (ICO) sets out our shared views on the close and often complex relationship between these issues and on the importance of close working between our two organisations on these matters in the coming years, as well as highlighting the progress that we have already made. The matters addressed in this document are complex and rapidly evolving, and we therefore expect our views and responses to these challenges will need to evolve as well. Nevertheless, this statement represents a significant step forward in our collaboration on these issues, and in the articulation of the synergies and potential tensions posed by the intersection of our policy objectives.

4. The overarching aim of this work is to promote and support outcomes which are competitive, empower consumers through enhanced choice, transparency and service design, and safeguard individuals' rights to privacy. We believe that the best way to achieve this is by working together to enhance the synergies between our two agendas, and to anticipate and address tensions where they arise.

5. We began to engage regularly on these issues during the CMA's market study into online platforms and digital advertising, which was finalised in July 2020, and have worked closely together in the period since publication to share perspectives and develop our shared thinking. The expansion in our regulatory remits following the UK's exit from the European Union has created new opportunities for us to work together. Our collaboration has helped inform the broader work carried out between the ICO, the CMA and Ofcom through the Digital Regulation Cooperation Forum (DRCF)[1] that has aimed to enhance regulatory coherence between the three organisations, as set out in the recently published DRCF workplan.[2]

6. The public expect regulators to work together to address their concerns. We are confident that our holistic approach will meet these expectations and deliver clear benefits for citizens, businesses, and the wider digital economy. It will enable companies to better understand their overall regulatory responsibilities and provide the public with the confidence that they can engage with online services in the knowledge that they are protected.

This document

7. The remainder of this statement sets out our shared views on the following areas:

   - the interactions between competition and data protection in the digital economy, highlighting the synergies and potential tensions between these policy areas;
   - how our two organisations are working together to maximise regulatory coherence, illustrated by two ongoing projects we have recently launched concerning the use of personal data in digital advertising; and
   - the next steps we will take together, including through the DRCF, to understand and promote outcomes in the digital economy that simultaneously promote competition and enhance data protection and privacy rights.

[1] https://www.gov.uk/government/publications/digital-regulation-cooperation-forum. The FCA joined the DRCF on 1 April 2021.
[2] https://www.gov.uk/government/publications/digital-regulation-cooperation-forum-workplan-202122.

Competition and data protection in the digital economy

8. The digital economy has the potential to bring about huge, positive impacts on people's lives in the UK and globally. We think that this can best be achieved where:

    - digital markets are competitive, giving users a genuine choice over the service, product, or provider they prefer;
    - consumer rights are protected, and consumers are supported in making informed choices including through the use of choice architecture and default settings;
    - the rights of citizens to privacy in relation to their personal data are protected, so that they have appropriate control over their data and can make meaningful choices over whether and for what purposes it is processed; and
    - organisations are accountable for, and are able to demonstrate, how their products and services protect the personal data of their users.

9. The links between competition, consumer protection, data protection and privacy are particularly important in the digital economy because of the central role that data – and in particular personal data – plays in the business model of firms providing online services.

10. While the terms 'data protection' and 'privacy' are often used interchangeably, it is important to note that these concepts are complementary but not identical in their meaning or scope. Data protection originates from the right to privacy, and supports the broader objective of preserving those fundamental rights in the context of personal data. When we speak about 'privacy' in this statement, we refer narrowly to dimensions of privacy that engage the right to data protection, and situations in which achieving the objectives of data protection law results in enhanced privacy and control in respect of personal data processing.

11. In this section, we first summarise the importance of data in the digital economy, and highlight how its use in these markets affects competition, data protection, and privacy. We then present our shared views on how competition and data protection considerations interact, outlining where we see synergies as well as possible tensions.

The importance of data in the digital economy

12. Data plays a central role in the business model of many firms operating in digital markets, and in particular of online platforms.

13. Examples of digital businesses relying on data to optimise their services include: online stores monitoring sales volumes for their products; search engines that collect and analyse search queries to train their algorithms and improve future search results; social media platforms that observe user behaviour to improve the content displayed in feeds; and news media publishers that adapt their content to draw and retain users on their pages.

14. Enabling greater access to data that can be used to improve a product or service can in principle enhance choice and the user experience. Similarly, ensuring services can communicate freely with one another (ie making them interoperable) can facilitate integration of a wide range of products, services, and applications, for example allowing for cross-posting from one platform to another, or for connecting various devices produced by different firms. This can improve consumer experience overall, and avoid consumers being "locked in" to a particular ecosystem by enabling them to move more freely between services.

15. Data is also a critical input for digital advertising. While the services described above are typically offered to users for free, the providers of these services, mainly large platforms, seek to make money through the selling of inventory to advertisers.[3] The value of this inventory can be enhanced by data that supports improved targeting, measurement, and attribution of adverts that are displayed. Google and Facebook are by far the largest two platforms that are funded by digital advertising. This advertising-funded business model is also adopted by a range of other online content and service providers including for example many online newspapers and mobile apps.

Personal data

16. In many cases, and in particular the use of data for personalisation of services or targeted advertising, the data that digital businesses process is personal data and therefore data protection law applies. Box A explains how data protection law distinguishes between personal and non-personal data.

17. It is important to note that data protection law recognises the function that personal data has for the economy and wider society, and as such the right to data protection is not absolute. The overall objective is to strike a balance

[3] In an online setting, inventory is essentially empty space on a web page or mobile app, which can be filled with text (including links to other websites), images, and videos.

between protecting these rights, ensuring processing is fair and lawful, individual rights are upheld, and organisations responsible for processing are accountable for the decisions they make and can demonstrate how they comply with the law.

Box A: what is personal data?

Data protection law defines personal data as any information relating to an identified or identifiable natural person.[4]

An individual can be identifiable directly (e.g. from the information itself), or indirectly (e.g. by using information in combination with other information). If someone is distinguishable from someone else, then they will be identifiable, even if their name is unknown.

The ICO has provided detailed guidance on personal data[5]. It should also be noted that the UK GDPR also treats certain types of personal data as more sensitive, requiring additional protection. This is 'special category data'.[6]

Personal data relating to children also merits specific protection.

18. The processing of personal data is a common feature in the provision of user-facing services such as those discussed above, and in a range of digital advertising services. In the current digital advertising ecosystem, personal data can make digital advertising inventory more attractive to advertisers in two ways. First, the use of personal data to target advertising, in particular display advertising, towards individuals who are most likely to make a purchase can result in a higher return on investment for advertisers, and a willingness to pay higher prices.[7] In addition to targeting, personal data can be used to provide evidence that users exposed to adverts on a website went on to make a purchase, which in turn can also increase advertisers' willingness to pay higher prices.[8]

19. Personal data therefore plays a very important role in the way that digital advertising markets currently function. However, we note that this may not be

[4] An identifiable natural person is one who can be identified, in particular by reference to a name, an identification number, location data, an online identifier, or one or more factors specific to the physiological, mental, economic, cultural or social identity of that individual.

[5] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/

[6] Special category data includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, as well as the processing of genetic data, biometric data for or the purposes of uniquely identifying a natural person, data concerning health, or data concerning someone's sex life or sexual orientation.

[7] Appendix F of the CMA's market study into online platforms and digital advertising presents an analysis of a trial carried out by Google, the results of which show that, where publishers in the open display market are not able to offer personalised advertising (using third party cookies) but compete against others who can, their revenues fall by around 70% in the short run.

[8] This is referred to as measurement and attribution.

the case in the future, as the importance that is placed on personal data within certain digital advertising markets may be diminished by the development of privacy-enhancing technologies.

Other classifications of data

20. There are many different and often overlapping ways of categorising data that are used in the digital economy. These categories are not always the same as the relevant definitions from data protection law, and can often include both personal and non-personal data.

21. For example, in online advertising a wide variety of different categories of data are commonly referred to, including:

- user data: data about users' attributes or online activity, as used, for example, for targeted personalised advertising or measurement;
- contextual data: data derived from the context in which an online action is performed (eg content of a website or individual's location) – also used for targeted advertising; and
- analytics data: data that conveys information about an advertising campaign, such as on the number of users who have seen it, and how many went on to make a purchase

22. One distinction that is sometimes drawn, both in the context of online advertising and the wider operation of the web, is between first-party and third-party data. These concepts are explained in Box B.

Box B: what is the difference between first-party and third-party data?

Data is sometimes categorised according to the relationship between the party collecting and processing it and the individual or circumstance it relates to:

- **First-party data**: data that is collected by a business through direct interaction with an individual providing or generating the data. For example, data collected by an online retailer regarding purchases made by consumers on its site.
- **Third-party data**: data collected by a business not in direct interaction with the individual providing or generating the data, for example, through business partners. Digital firms that do not have a direct relationship with users frequently rely on third-party data.

The boundaries between first and third-party data according to the above definition are not always clear, particularly when large companies own a variety of businesses, some of which have a relationship with the user and some of which do not.

Both first-party and third-party data as defined above can include personal and non-personal data. Whether information is personal data depends on whether it relates to an identified or identifiable individual. There is no explicit reference to the distinction between first-party and third-party data in data protection law.[9]

The descriptions of 'first party' and 'third party' are also used (though with a different meaning) in the context of cookies and similar technologies,[10] which collectively form the key means by which information (including personal data) is collected and disseminated in online advertising. A cookie is generally identified as being first-party if the domain of the cookie matches the domain of the page visited and as being third-party in instances where the domain of the cookie does not match the domain of the website. This is not a rigid distinction. Some functions typically delivered through third party cookies can be done via first party cookies, even if a third party's code and associated service is still involved.

The rules on the use of cookies and similar technologies are specified in Regulation 6 of the Privacy and Electronic Communications Regulations 2003 (as amended) ('PECR'), and oversight of these rules is one of the ICO's regulatory functions. PECR provides more specific rules than the UK GDPR in a number of areas such as cookie use. It is also important to note that PECR's provisions in this area apply whether or not personal data is processed.

Economic characteristics of data

23. From an economic perspective, data, including personal data, has a number of distinctive characteristics that are relevant to the dynamics that have developed in the digital economy.

24. As outlined above, data has value for digital businesses. This data may be unrelated to individuals, for example where it refers to technological performance, financial information, or sales figures for different products and

services. Value is also frequently derived from data that relates to knowledge of users' interests and preferences – both individually and in aggregate – as it can help providers of online services to customise and improve user experience for their user-facing products and services. Further, for businesses that are funded by digital advertising, having extensive and up-to-date knowledge of users' characteristics, preferences and behaviour is often an important aspect of the value of their digital advertising inventory.

25. While the initial costs of collecting data can sometimes be substantial, the marginal cost of sharing data, be it through copying or providing access to it, is typically very low. Further, data is not used up or deteriorated when it is copied. Once collected, sharing data does not, therefore, decrease its value for the initial collector (economic theory uses the term 'non-rivalrous' to describe this characteristic).[11] Data can also give rise to 'externalities' (spillover costs or benefits to third parties), for example when insights about the preferences of one user or group of users can benefit other users through tailoring content and improving user experience.

26. Value from data can also stem from the combination of datasets, which can yield insights that would not be gained from keeping data separate, sometimes in unexpected ways. These 'economies of scope' are complemented by 'economies of scale' in data collection, due to the disparity in the cost of creating or collecting this data and the cost of sharing and copying it, as explained above.

27. The initial costs of collecting data and the value that its features give it mean that collectors of data have an economic incentive to prevent access to what they have collected, rather than sharing it. Additionally, legal requirements or technical feasibility can also determine the extent to which data can be shared with third parties.

28. These characteristics mean that there is a value in aggregating data, either to make use of directly or to sell on to others, and a tendency to concentration, leading to problems of market power. Differential access to data can be a barrier to competition.

29. Data sharing can create significant efficiencies. Conversely, exclusionary behaviour regarding data may be inefficient as there could be large social

[9] Article 4(10) of the UK GDPR does define 'third party', but not in the sense of the term 'third party data' in digital advertising.

[10] Cookies are small text files stored on the user's computer on request of a website by the browser. These files can be sent back by the browser to the website at subsequent visits thereby enabling a website to recognise and identify a user and tracking them over various websites. "Similar technologies" can involve tracking pixels, fingerprinting techniques and use of local storage.

[11] In cases where the data is personal data, the data protection principles apply.

gains if data was widely shared and available. This finding underpins many general arguments for the importance of the free flow of data, which can create value for others and for society.

30. However, where the data in question is personal data, this rationale can be perceived to be in tension with the requirements of data protection legislation, and more generally the incentives to collect, aggregate and use personal data in different ways can raise a range of data protection concerns. We explore this and the interplay with competition in more detail in the following sections.

Data and competition in digital markets

31. Given the economic characteristics and potential uses of data in the digital economy outlined above, access to relevant data at scale by existing or potential market participants can have a substantial bearing on their ability to grow or sustain their market share, and on their ability to generate revenue. This is particularly in the case of services that are funded by advertising.

32. While access to data is important to the dynamics of digital markets, it is important to note that fair and effective competition does not rely on companies processing and/or sharing ever increasing amounts of personal data. Instead, the most important factor from a competition standpoint is that market participants compete with one another on a level playing field. In circumstances where competitors in a digital market have significantly differential access to data, then competition 'on the merits' is likely to be undermined. As a result, consumers will have less choice, and will ultimately lose out through higher prices, lower quality, and reduced innovation.

33. In its market study into online platforms and digital advertising, the CMA found evidence that Google and Facebook enjoyed significant data advantages in the provision of their user facing and advertising services. It concluded that these advantages are self-reinforcing in their nature and currently exist at such a scale that they are insurmountable without regulatory intervention.

34. The following are examples drawn from the CMA's market study of where differential access to data in digital markets prevents competition from taking place on a level playing field:

    - Access to search 'click and query' data: search engines collate data to train their algorithms – including what users search for, the results they select, and the time spent on a page ('click and query' data). Generally speaking, the more of this data they have, the more effective their algorithms become at understanding what users are looking for, in turn resulting in more relevant search results being returned. The CMA

concluded that, with around 90% of search traffic over the last decade, Google's advantage in this regard is self-reinforcing: more data leads to more relevant results, which in turn brings greater demand and generates further data.[12]

- Access to user profiling data for targeted advertising: both Google and Facebook have large ecosystems of interconnected consumer services, from which they are able to gather and aggregate personal data to build detailed profiles of users' interests and online activities. Rival publishers of display advertising, including smaller social media platforms or news publishers, have access to substantially less personal data about each individual user and hence less detailed profiles.[13] The CMA concluded that, as a result, Google and Facebook can offer a greater degree of personalisation for advertising inventory than their rivals.[14]

- Access to advertising analytics data for performance and attribution measurement: the CMA found that both Google and Facebook have an advantage in terms of being able to track users across their own ecosystems and across a large number of third-party sites and apps. This means they can better track user actions online and demonstrate to advertisers the effectiveness of using their platforms relative to their rivals.[15]

35. Based on these findings, many of the potential interventions considered by the CMA in its market study related to access to data, including options for greater sharing of non-personal data between businesses, increased interoperability between services, and data separation within large integrated companies.

36. While some of the data-related interventions considered by the CMA could involve greater sharing and processing of data, others could have the

[12] CMA's market study into online platforms and digital advertising, Final report, Appendix I: https://assets.publishing.service.gov.uk/media/5fe4957c8fa8f56aeff87c12/Appendix_I_-_search_quality_v.3_WEB_.pdf

[13] As set out in more detail in paragraphs 44-47, this is not to suggest that the data processing in the open RTB ecosystem is unproblematic. In its 2019 Update Report the ICO expressed concern that, among other matters, the profiles created about individuals were extremely detailed and repeatedly shared and that this profiling was disproportionate, intrusive and unfair.

[14] CMA's market study into online platforms and digital advertising, Final report, Appendix F: https://assets.publishing.service.gov.uk/media/5fe495438fa8f56af97b1e6c/Appendix_F_-_role_of_data_in_digital_advertising_v.4_WEB.pdf.

[15] CMA's market study into online platforms and digital advertising, Final report, Appendix F: https://assets.publishing.service.gov.uk/media/5fe495438fa8f56af97b1e6c/Appendix_F_-_role_of_data_in_digital_advertising_v.4_WEB.pdf.

opposite outcome. A common feature across them all is the objective of creating a more level playing field so that competition can thrive.

Protecting personal data in the digital economy

37. As outlined above, many of the outcomes organisations in the digital economy seek to achieve involve processing of personal data as defined by data protection law. In particular, digital businesses use personal data to respond to consumer preferences, to personalise the services they offer, and for targeted advertising.

38. Learning about users' preferences, behaviours, interests or actions may enable improvements in products and services. As noted above, where personal data is processed, data protection law applies, as do its objectives of balancing the right to the protection of personal data with the function that this data has in society. The data protection framework aims to safeguard individual rights and ensure that the processing of personal data is fair, transparent, and lawful.

39. UK data protection law takes a flexible, risk-based approach that puts the onus on the organisations that decide to process personal data – "controllers" – to think about and justify how and why they use that data. For example, under the UK GDPR organisations have to take account of the risk to the rights and freedoms of individuals, and the likelihood and severity of the harm that may arise from the processing they intend to undertake. This involves consideration of the nature, scope, context and purposes of the processing. The assessment of privacy and data protection harms that the ICO carries out in line with the UK GDPR is therefore a 'risk-based' approach, which considers the type of harm and potential damage caused.[16]

[16] These harms can be wide-ranging and include individual tangible harms such as financial or bodily harm, or the cost of avoiding or mitigating harm; individual intangible harms such as discrimination, unwarranted intrusion, misuse of personal information, or loss of control of personal data; and societal harms such as loss of trust, damage to the rule of law or democracy.

Box C: Overview of data protection law and other relevant legislation

The UK data protection framework is made up of the following:

- The Data Protection Act 2018. This sets out three separate data protection regimes: general processing (Part 2 – the UK GDPR), law enforcement processing (Part 3) and intelligence services processing (Part 4).

- The UK GDPR, which sits alongside the DPA 2018. It is UK law that came into effect on 1 January 2021, and is based on the EU GDPR with some changes to make it work more effectively in the UK context.

The ICO's Guide to Data Protection has more detail on the UK legal framework and its various elements.[17]

As well as the DPA and UK GDPR, there is also PECR. As described in box B above, PECR complements and particularises the UK GDPR in a number of areas, providing specific rules for certain types of processing. Of most relevance in the context of the digital economy are the rules on processing terminal equipment information (often called the "cookie law"), as well as the direct marketing provisions and restrictions on the processing of location data.

40. The dynamics of the digital economy and characteristics of data use within it mean that there is a tendency to ever-increasing data collection and data processing among participants in digital markets, be it because they want to adapt user-facing services to users' preferences or for purposes such as improving the accuracy of digital advertising to increase conversions. The economies of scale and scope described above further incentivise the collection and processing of personal data and this creates potential risks for user privacy and data protection.

41. The data protection framework also seeks to ensure that individuals have effective control over the processing of their personal data and are empowered to make informed and granular choices over that processing. For example, by requiring organisations to ensure their processing is fair, lawful and transparent and that individuals have appropriate information about the choices they can make alongside an ability to exercise their rights easily, key types of harm such as lack of autonomy and power/information asymmetry can be mitigated. The ICO therefore places great importance on ensuring users can appropriately exercise their rights.

42. In this regard, the ICO has had a focus on information rights in digital advertising for a number of years. As detailed in boxes B and C above, the

[17] https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/

data protection framework and related legislation applies to the processing in digital advertising. Additionally, the ICO's Technology Strategy 2018-2021 included "web and cross-device tracking" as a key priority area[18].

43. In late 2018 the ICO commenced a detailed review of the digital advertising ecosystem, focusing on programmatic advertising and real-time bidding. This included significant industry engagement., The ICO also commissioned research from Harris Interactive into individuals' attitudes towards the processing of personal data in RTB which showed that when people are made aware of how their data is used, there was a "notable shift in perceptions towards websites showing adverts as unacceptable"[19].

44. In its subsequent "Update report into adtech and real-time bidding" published in June 2019, the ICO summarised key areas of concern with how data, including personal data, is processed in RTB[20]. These included:

- Applicable law: market participants exhibited a lack of understanding of the law that governs the use of cookies and similar technologies, with some relying on legitimate interests to set cookies for advertising purposes despite Regulation 6 of PECR requiring consent.

- Consent and lawful basis for processing: the consent requirement under Regulation 6 of PECR means consent is also the most appropriate lawful basis for related processing activities. In the context of legitimate interests, market participants did not demonstrate that they met the requirements. Additionally, processing of special category data within RTB requires explicit consent under data protection law, but consent mechanisms do not enable the collection of this type of consent.

- Transparency: privacy information lacked clarity and did not give individuals a sufficient picture of what happens to their data.

- Profiling: the profiles created about individuals were extremely detailed and repeatedly shared. They were enriched with information gathered

[18] ICO (2018). *Technology strategy 2018-2021*, 27 February 2018, page 9. Available at: https://ico.org.uk/media/about-the-ico/documents/2258299/ico-technology-strategy-2018-2021.pdf. Priority Area 3 states that "new online tracking capabilities are becoming more common and pose much greater risks in terms of systematic monitoring and tracking of individuals, including online behavioural advertising".

[19] ICO/Ofcom/Harris Interactive (2019). *Adtech Market Research Report*, 20 March 2019, pages 5 and 19. Available at: https://ico.org.uk/media/about-the-ico/documents/2614568/ico-ofcom-adtech-research-20190320.pdf.

[20] ICO (2019). *Update report into adtech and real-time bidding*, 20 June 2019. Available at: https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf.

from other sources. This profiling was disproportionate, intrusive and unfair, and in many cases, individuals were unaware it was taking place[21].

- Data supply chain: the complex and opaque nature of the data supply chain meant that there were no guarantees about how data was used or secured once passed on to counterparties.

- Assessing Risk: there was a lack of understanding about the need to assess the risks involved in data processing e.g., by undertaking data protection impact assessments and implementing mitigations.

45. As a result of its concerns, the ICO is currently progressing its work with a series of mandatory audits, initially focusing on data management platforms[22] operating in the RTB ecosystem. This forms part of the ICO's ongoing assessments of compliance in the RTB sector.

46. The report's focus was RTB as implemented via protocols such as OpenRTB and Authorized Buyers. However, the ICO stated that this focus did not mean other areas of online advertising were "issue-free" in terms of data protection, or that related matters such as ad fraud or market dominance of large digital businesses were not also areas of concern.

Synergies and tensions between the aims of competition and data protection

47. The objectives of competition law and data protection are sometimes characterised as being in opposition. We do not agree. There are fundamental synergies underpinning our respective policy goals and we believe that, although tensions may arise, they are surmountable.

48. In the following sections we highlight the synergies between our respective regimes before recognising where challenges might occur.

Synergies

49. We believe that there are strong synergies between competition and data protection objectives, and that many regulatory interventions in digital markets can be designed in a way that supports both objectives. These synergies can be considered under three main categories: user choice and control;

[21] The report also detailed that information included in bid requests will be personal data where it enables an individual to be identified or identifiable, directly or indirectly - either from the information itself (alone or in combination) and in respect of any additional information market participants may possess. This is particularly relevant in the context of data matching, combination and enrichment after the initial collection of data.

[22] ICO (2021). *Adtech investigation resumes*, 22 January 2021. Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/01/adtech-investigation-resumes/.

standards and regulations to protect privacy; and data-related interventions to promote competition.

User choice and control

50. Meaningful user choice and control are fundamental both to robust data protection and effective competition. The interests of both policy objectives are best met where users have a genuine choice over the service or product they prefer, providers compete on an equal footing to attract their custom, and where individuals have control over their personal data and can make meaningful choices over whether and for what purposes it is processed.

51. In this context, effective competition can enable stronger privacy protections, and weak competition can undermine those protections. In its recent market study, the CMA identified a significant concern where social media platforms offered users no choice over whether to have their personal data used for personalised advertising. It concluded that concerns around such 'take it or leave it' terms regarding the use of personal data were particularly acute where the platform has market power, such that the user has no meaningful choice but to accept the terms.[23,24]

52. Effective data protection can also support competition as rival companies seek to build consumer trust and confidence in the way that their personal data is used, and by helping to ensure that competitive pressures help drive innovations that genuinely benefit users. We discuss this in more detail below.

53. Many users care strongly about their privacy and want more control over their personal data. Putting users in control of their personal data is not only important for safeguarding their privacy but can also help mitigate harms such as power asymmetry, which has impacts on the objectives of both competition and data protection. For example, reducing this asymmetry by giving individuals control over the use of their personal data can improve trust and confidence in the digital economy and contribute to a more effective use of personal data while still providing controls and safeguards. From a competition perspective, this can foster healthy competition that benefits users, since it can help reset the balance between digital businesses and

[23] Facebook was identified as a platform enjoying significant market power on account of factors including network effects. If a user wants to contact their friends and family on Facebook, they have no choice but to agree to receive personalised advertising.

[24] 'Take it or leave it' terms can pose concerns from a data protection perspective – irrespective of the existence of market power – in circumstances where consent is relied upon – or is required by PECR – as that consent must be freely-given. The ICO's guidance on consent, and on cookies, both discuss the concept of the 'take it or leave it approach' in more detail.

users, putting the onus on the business to do more to engage users and give them greater benefit from their personal data.[25]

54. Where individuals are given meaningful choice and control in a competitive digital economy, 'privacy' itself may increasingly become an area in which businesses compete for new customers. This could incentivise responsible innovation and become the catalyst for the development of alternative, privacy-protective business models.

55. For example, by providing an appropriate level of privacy by default, and options that allow individuals to control the processing of their data (and permit additional data collection if they are comfortable with it), such models will enable individuals to be in control, and digital businesses will in turn benefit from fair, lawful and transparent data processing undertaken in a trustworthy way. Enhanced user control will build user trust and confidence, which in turn will support a flourishing digital economy.

56. For this reason, we are both strongly supportive in principle of measures that enhance users' ability to control their personal data, decide for what purposes and how it should be processed, and exercise their rights.[26] We are also aware that users may have limited time and inclination to choose between complex options and that their choices can be heavily influenced by choice architecture and default settings. Therefore, requiring providers of digital services to design choice architecture in a way that allows users to choose freely, and to deploy default settings that are in the user's interest rather than those of the service provider, can be highly valuable in supporting both competition and data protection goals.

57. Indeed, data protection law requires organisations that process personal data to adopt a 'data protection by design and by default' approach to the development of products and services that process personal data.[27] By implementing the data protection principles effectively (such as fairness, purpose limitation, data minimisation and security), and integrating necessary safeguards into the processing to protect individual rights and ensure

[25] It should be noted that in data protection terms, where a service bases its processing on consent it must take care that it does not unduly influence the individual – this does not, however, mean that incentivisation is impossible under the legal framework. The ICO's consent guidance provides more detail on this point.
[26] It is also important to observe that consent (in terms of the lawful basis for processing) and control (over that processing) are not contiguous. It is possible to have control in other contexts, however the interaction between PECR and the UK GDPR will often entail that consent is required upfront (e.g. due to the processing in online advertising engaging Regulation 6 of PECR in many cases). In practice, there are also situations where consent is inappropriate; the key is ensuring transparency, control, and safeguarding individual rights.
[27] UK GDPR, Article 25.

compliance with other obligations,[28] users' ability to control their data and preserve their privacy can be strengthened.

58. Reflecting the importance of this topic, the ICO and the CMA have each recently carried out their own work on how choice architecture can support users in making meaningful choices. The ICO's statutory code of practice on age-appropriate design came into force on 2 September 2020 (with a 12-month transition period). The code sets 15 flexible standards that ensure that the best interests of the child are the primary consideration when designing and developing online services likely to be accessed by children.[29] Additionally in its market study into online platforms and digital advertising, the CMA recommended that a 'Fairness by Design' duty be placed on platforms with market power to ensure that they design choice architecture and defaults in a way that maximises users' ability to make informed choices about the use of their personal data, which has clear alignment with the data protection principles and the legal requirements of data protection by design and by default.

59. Both our institutions have together made a commitment to carry out further work, alongside Ofcom, on 'design frameworks' under the Digital Regulation Cooperation Forum, to provide greater clarity for industry regarding regulatory requirements for choice architecture and, where relevant, make compliance with them more efficient.[30]

The role of clear regulation and standards to protect privacy and ensure effective competition

60. The establishment of clear rules and widely accepted standards plays an important role in any well-functioning economy, facilitating interactions between individuals and organisations from a basis of mutual understanding. It is therefore important to recognise as a point of principle that data protection law and competition law complement each other in respect of achieving efficient market outcomes that involve processing personal data.

61. In fact, we share the view that well-designed regulation and standards that preserve individuals' privacy and place individuals in control of their personal

---

[28] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/#:~:text=Data%20protection%20by%20design%20essentially%20inserts%20the%20privacy,protection%20obligations.%20It%20is%20now%20a%20legal%20requirement.

[29] https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/#:~:text=The%20Secretary%20of%20State%20laid%20the%20Age%20Appropriate,September%202020%20with%20a%2012%20month%20transition%20period. Also known as the 'Children's Code', it is published pursuant to Section 123 of the Data Protection Act 2018.

[30] https://www.ofcom.org.uk/__data/assets/pdf_file/0017/215531/drcf-workplan.pdf.

data can serve to promote effective competition and enhance privacy. This is achieved by ensuring that competitive pressures help drive innovations that genuinely benefit users, rather than encouraging behaviour that undermines data protection and privacy rights. With appropriate regulation, competitive pressures can be harnessed to drive innovations that protect and support users, such as the development of privacy-friendly technologies, clear, user-friendly controls, and the creation of tools that support increased user-led data mobility. The incentives to deliver these forms of innovation are greater in the presence of targeted regulation than without.

62. Further, data protection law enables fair and proportionate data sharing. The ICO's publication of its statutory code of practice on data sharing outlines the benefits that data sharing can bring to organisations, individuals, the economy and wider society.[31] It gives businesses and organisations the confidence to share data in ways that comply with the law and enable those organisations to share data fairly and proportionately. Data sharing that engenders trust in how personal data is being used is a driver of innovation, competition, economic growth and greater choice for consumers and citizens.

63. Overall, where regulation and standards regarding the processing of personal data also serve to maintain (or even help to establish) a level playing field between competing businesses, the interests of both competition and data protection are strongly aligned.

Data-related interventions to promote competition

64. Given the central role of data in driving competition in digital markets, and the extent to which differential access to data can distort competition, interventions to provide or restrict access to data can be an important tool in promoting competition in digital markets.[32] Where this data is personal data, there is an important interaction to be considered between the interests of competition and data protection.

65. As noted above, a key motivating factor for the CMA in considering data-related interventions is the need to overcome significant disparities in access to data that have the potential to distort competition. This can take the form of restricting access to data, or limiting the ability to combine and integrate datasets, for platforms with market power, in order to create a level playing field with other market participants. One example of such an intervention that was considered in the CMA's market study is the potential for imposing data

[31] https://ico.org.uk/for-organisations/data-sharing-a-code-of-practice/.

[32] Data access interventions are considered further below. The focus of this section is on measures to restrict access to data.

silos on platforms with market power to restrict their ability to combine datasets for the purposes of targeting and measuring digital advertising.

66. While careful consideration has to be given to the potential efficiency costs of restricting the ability of companies to combine datasets, such interventions could in principle deliver strong synergies between the interests of competition and data protection, since they involve restricting the ability to combine and process personal data, at the same time as creating a more level playing field for all businesses to compete fairly.

67. We are exploring together the ways in which our two legal frameworks provide avenues for delivering such interventions, and the extent to which they may simultaneously support our regulatory objectives.

Potential tensions

68. We also recognise that there are some circumstances in which the objectives of data protection and competition can be perceived to be in tension. Two examples where these tensions can be highlighted are:

- in relation to data-related interventions that seek to overcome barriers to competition by providing third parties with access to personal data; and
- where data protection requirements may be interpreted by industry in a way that risks distorting competition, e.g. with the potential effect of unduly favouring the business models of large, integrated platforms over smaller, non-integrated suppliers.

69. We consider the implications of these two examples in more detail below.

Data access interventions

70. Some forms of data-related interventions explored in the CMA's market study would seek to promote competition in a market in a targeted way by requiring access to particular types of data for smaller businesses or potential new entrants. The objective would be to ensure that they can compete on a level footing with incumbents that have market power on account of their substantial access to data.

71. Where access to personal data is in scope of such a remedy, it must be designed in a way that aligns with data protection law. We discuss some of the relevant considerations in the following paragraphs.

72. As outlined above, data is non-rivalrous,[33] and the marginal cost of sharing data is very low. Sharing data can therefore create significant efficiencies from which society as a whole can benefit, particularly where such sharing allows data to be reused or combined in different ways and for different purposes.

73. In contrast to the principles of data separation discussed above, data access interventions may be seen as having the potential to create tensions with data protection objectives, for example if they may lead to more widespread processing of personal data by a larger number of controllers. However, it is important to note that data protection law facilitates data sharing where it is both fair and proportionate and complies with legal requirements.

74. The ICO's recently-published code of practice on data sharing[34] outlines the benefits that data sharing can bring to the economy and wider society and should give businesses and organisations the confidence to share data in a way that protects users' privacy and ensures they retain control over their data.[35] As the code states, 'Data protection law is an enabler for fair and proportionate data sharing, rather than a blocker.' The key is that businesses ensure any data sharing that takes place complies with the requirements of the law.

75. Should data access interventions be an appropriate remedy, we therefore think any perceived tensions can be resolved through designing them carefully, such that they are limited to what is necessary and proportionate, are designed and implemented in a data protection-compliant way, that related processing operations are developed in line with the principles of data protection by design and by default, and they do not result in a facilitation of unlawful or harmful practices.[36]

Risk of interpreting data protection law in an anti-competitive manner

76. A second area of potential tension arises where there is a risk of data protection law being interpreted by large integrated digital businesses in a way that leads to negative outcomes in respect of competition, e.g. by unduly favouring large, integrated platforms over smaller, non-integrated suppliers.

---

[33] This means that data is not used up or deteriorated when it is copied. Once collected, sharing data does not decrease its value for the initial collector

[34] https://ico.org.uk/for-organisations/data-sharing-a-code-of-practice/. The data sharing code is a statutory code of practice published under Section 121 of the Data Protection Act 2018.

[35] It should be noted that in general, the decision to share personal data is the controller's. It is also the controller that is accountable for its processing and must ask itself whether data sharing is necessary and proportionate.

[36] For example, as set out in paragraphs 43-46, in 2019 the ICO raised concerns about data sharing in the RTB ecosystem.

77. For example, such risks could arise from an interpretation of data protection law in which transfers of personal data between different businesses owned by a single corporate entity – such as a large platform company – are in principle viewed as acceptable from a privacy perspective, while transfers of personal data between independently-owned businesses are not, even if these businesses are functionally equivalent to those of the platform and the data is processed on the same basis and according to the same standards.

78. If implemented in practice, such an interpretation would clearly be problematic for competition, as it would provide strong incentives for companies to integrate horizontally and vertically in order to be able to process more personal data. It would also undermine the ability of challenger or new entrant firms that are not vertically integrated, including small start-ups, to compete in digital markets.

79. As well as being problematic for competition, any such interpretation of data-protection law could also raise privacy concerns, and could for example lead to data protection harms referenced earlier such as lack of autonomy and power asymmetry. Transmitting or disclosing data between separate business units – even when ultimately owned by the same corporate entity – must comply with data protection law.

80. While the law acknowledges that controllers that are part of a group of undertakings may have a legitimate interest in transmitting personal data within the group for internal administrative purposes, such as processing clients' or employees' personal data,[37] by its nature this interest is limited to such purposes and in any case must still include consideration of the rest of the wider principles, requirements and objectives of the data protection framework which also apply to controller-to-controller data sharing, including fairness, transparency, purpose limitation, data minimisation and security.[38]

81. We recognise that data sharing between unconnected businesses must comply with the same data protection principles, requirements and objectives as internal data sharing. As referenced above, the ICO's work on RTB found significant issues with the widespread dissemination of personal data in the open display market, e.g. by the multiplicity of companies involved in handling bid requests. This was crucially linked to the way that RTB operates. These findings related to the way in which data is processed in practice, and whether

[37] See, for example, Recital 48 of the UK GDPR as well as the ICO's guidance on legitimate interests: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/when-can-we-rely-on-legitimate-interests/.

[38] In the context of legitimate interests organisations may be able to identify such an interest and pass the "purpose test" but they still have to consider the nature, scope, context and purposes of the intended processing, the risks it poses, and any relevant laws, guidelines and codes of practice. Ultimately, if the outcome of the processing leads to negative impacts in respect of other applicable law, the interest would not be legitimate.

it is done fairly, lawfully, and transparently. While they centred on the lack of transparency and control given to individuals (particularly regarding who processes their data in the 'adtech stack'), along with the lack of risk assessment around data sharing and onward transfer (and how this relates to the lack of guarantees regarding the security of personal data), the ICO also noted that there were concerns around the amount of processing taking place, as well as the level of profiling being disproportionate, intrusive and unfair.[39]

82. It is important to note, therefore, that neither competition nor data protection regulation allows for a 'rule of thumb' approach, where intra-group transfers of personal data are permitted while extra-group transfers are not. Under both data protection law and competition law, a careful case-by-case assessment is needed, regardless of the size of a company, the business model adopted, or the nature of any processing activity.

83. As we both jointly consider the right way forward in relation to these issues, we recognise that there are significant challenges to be addressed, which will require more detailed consideration. However, we believe that competition and data protection law are strongly synergistic, and any areas of perceived tension can be reconciled through careful consideration of the issues on a case-by-case basis, with consistent and appropriate application of competition and data protection law, and through continued close cooperation between our two organisations.

Summary of our shared views on competition and data protection

84. There are strong synergies between the interests of competition and data protection, and potential regulatory interventions are capable of being designed to further both policy objectives. We think we can resolve the potential for tensions through careful consideration of the issues on a case by case basis and through close cooperation between our two organisations.

85. Overall, our view is that competitive digital markets, with appropriate, well-targeted data protection regulation, should help lead to the following pro-privacy and pro-competition outcomes:

- users have clear information about what personal data is collected and how it is used, and can make an informed decision over whether to accept the terms offered by platforms for use of their personal data;

[39] ICO update report into adtech and real-time bidding: https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf.

- choice architecture and default settings are designed in a way that reflects users' interests;
- users have more control over their personal data and can make meaningful decisions over whether to withhold access to it or share it with others;
- users have a real choice over platform and service providers, and can easily switch if they prefer the content, functionality, or data protection approach of an alternative provider;
- providers of digital services are able to compete with one another by recognising privacy as an important aspect of quality, or alternatively by offering greater benefits to those users that permit and are comfortable with greater collection of their personal data; and
- platforms are incentivised to innovate and develop new ways to deliver advertising that meets the targeting needs of advertisers using less personal data, thus protecting users' privacy to a greater extent.

86. Personal data plays a key role in the digital economy from the perspectives of both competition and data protection. To fulfil the public policy objectives of the two legal frameworks, ensuring that informed users can exercise meaningful control over the collection and use of their personal data is key. While the competition efficiencies associated with data sharing may in some cases be in potential tension with data protection objectives, we believe that appropriately targeted regulatory approaches can help produce competitive and well-functioning yet privacy-preserving digital markets.

87. The actions we are already taking to work together, as outlined in the following section, demonstrate our shared commitment to achieving such outcomes.

Working together to promote regulatory coherence

Through the Digital Regulation Cooperation Forum

88. This joint examination of the interaction between competition and data protection in digital markets has been carried out under the umbrella of the Digital Regulation Cooperation Forum (DRCF), formed last year by the CMA, the ICO, and Ofcom with the goal of supporting a coordinated and coherent ongoing approach to digital regulation. The FCA became a member of the DRCF on 1 April 2021.

The DRCF Workplan

89. On 10 March 2021, the DRCF published its ambitious workplan for the year ahead, which sets out how the respective regulators will work together to achieve this aim. Our shared experiences working together on the issues discussed in this statement have informed that broader DRCF work.

90. Beyond identifying three priority areas of focus over 2021/22, the DRCF workplan sets out a range of ideas that could support future cooperation between digital regulators. Specifically, the workplan commits to review existing MOU arrangements to ensure that they reflect the potential for multilateral joint projects and the aims of coordination in online regulation. We anticipate that updating our existing MoUs and information sharing agreements, across the DRCF, will facilitate an increased degree of transparency for interested stakeholders and the wider public.

91. Separately, as part of this joint project, the CMA and the ICO have updated our bilateral MoU which we are publishing to coincide with this statement.

92. Building on the cooperation mechanisms provided by the DRCF, the most important step we can take in fostering effective working relations between the ICO and the CMA is to promote a culture of cooperation and collaboration between our two organisations. We are committed to developing and fostering this culture, building on the increasingly close working relationships we have developed in the last two years.

93. We have found there is much we can agree on, and a great deal of scope within our individual remits to give consideration to each other's regulatory objectives. For example, in its market study into online platforms and digital advertising, the CMA considered privacy as a key metric of quality in the services that platforms offer users, particularly in its concerns about users' control of data and the degree of transparency in terms of how their data was used by adtech providers.

94. Similarly, as part of its original investigation into real-time bidding the ICO outlined the role that tracking technologies (including third-party cookies) play in the online advertising ecosystem. The ICO's commitment to a measured and iterative approach of reviewing the market demonstrates its understanding of the potential significant market disruption that may flow from rapid changes to the way the market operates.

95. A clear demonstration of this commitment is the approach we are currently adopting within two high profile projects that the CMA and ICO have recently launched, both of which raise fundamental questions about the appropriate

role of personal data in digital advertising markets, including who should be able to access it and on what terms.

The CMA's investigation into Google's Privacy Sandbox proposals

96. Google announced in January 2020 that it intends to phase out support for third-party cookies in Chrome within two years. This is an important development that highlights online platforms' increasing role in deciding on the appropriate application of data protection regulation for other market participants.

97. Google's announced plans – known collectively as the 'Privacy Sandbox' proposals – to disable third party cookies on the Chrome browser and Chromium browser engine and replace them with a new set of tools for targeting advertising and other functionalities that Google says will protect users' privacy to a greater extent. The development of the 'Privacy Sandbox is already under way, but Google's final proposals have not yet been decided or implemented. In its market study into online platforms and digital advertising, the CMA highlighted a number of concerns about the proposals' potential impact, including that they could undermine the ability of publishers to generate revenue and undermine competition in digital advertising, further entrenching Google's market power.

98. In January 2021, the CMA opened an investigation into Google's Privacy Sandbox proposals, intending to assess whether the proposals could cause advertising spend to become even more concentrated on Google's ecosystem at the expense of its competitors. The investigation followed complaints of anticompetitive behaviour and requests for the CMA to ensure that Google develops its proposals in a way that does not distort competition.

99. The ICO is also assessing the Privacy Sandbox proposals for compliance with data protection and ePrivacy law.

100. The CMA and the ICO are working collaboratively in their engagement with Google and other market participants to build a common understanding of Google's proposals, and to ensure that both privacy and competition concerns can be addressed as the proposals are developed in more detail.

The ICO's investigation into real time bidding and the adtech industry

101. In January 2021, the ICO announced it was resuming its investigation into real time bidding (RTB) and the adtech industry, following a pause while it responded to the COVID-19 pandemic.

102. The ICO's work will continue with a series of mandatory audits initially focusing on data management platforms, and audit notices are underway directed to specific companies. The outcome of these audits will provide the ICO with a clearer picture of the state of the industry and will inform the ICO's ongoing assessments of compliance in the RTB ecosystem. Where the ICO identifies non-compliance through these audits the Information Commissioner will consider the use of her wider regulatory powers. This could include use of enforcement notices or monetary penalties where appropriate.

103. Data broking also plays a large part in RTB. In 2020 the ICO published its findings around data broking by credit reference agencies[40]. Its investigations into data broking continue alongside the work the ICO is carrying out in adtech and RTB.

104. The ICO is committed to publishing its final findings once the investigation into RTB is concluded, and will maintain a positive dialogue with the CMA regarding competition-related points that arise during the audit processes.

Conclusions and next steps

105. This document provides our shared view that our overlapping objectives regarding competition and data protection in the context of the digital economy are strongly aligned and complementary. There are several factors that support this conclusion:

- First, more competitive markets will deliver the outcomes that consumers care about most, which increasingly includes enhanced privacy and greater control over personal data.

- Second, we have concluded that this relationship is mutually reinforcing. Well-designed regulation and standards that preserve individuals' privacy and place individuals in control of their personal data can promote positive competitive outcomes. In turn, with appropriate and targeted regulation, competitive pressures can be harnessed to incentivise responsible innovations that protect and support users.

- Third, the creation of a level playing field is fundamental for enabling effective competition to thrive. Data protection law helps to achieve a level playing field with regards to data access, by ensuring that processing of personal data by all parties is fair and lawful and individual rights are upheld.

[40] Investigation into data protection compliance in the direct marketing data broking sector, October 2020 (ico.org.uk)

106. We are confident that any areas of perceived tension between competition and data protection can be overcome through careful consideration of the issues on a case-by-case basis, with consistent and appropriate application of competition and data protection law, and through close cooperation between our two organisations.

107. Reaching these conclusions has been an important step towards achieving regulatory coherence for the digital economy, but we do not intend to stop here. We recognise that digital markets are complex and can evolve quickly, and we therefore intend to continue to work together to further develop our thinking, to ground our conclusions in the context of real-world examples, and to ensure that our approach keeps pace with market developments.

108. We also recognise that these matters are of global relevance, and we will continue to engage with our respective international counterparts and relevant fora around the world to build consensus and promote global regulatory coherence and collaboration.

109. We will also continue the work we set out to undertake in the DRCF's recently published workplan including developing a more holistic view of how the digital advertising sector, and advertising funded business models, interact with potential consumer and citizen harms.

110. Our ongoing collaboration will not be confined to building understanding. We have provided two examples in this statement of projects where we are committed to consulting one another to ensure the synergies identified in this statement can be maximised, and any tensions overcome.

111. Our views will evolve as we progress this work and we will keep under review the benefits of expanding on this statement in the future.