Information Commissioner's Office

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

Response of the Information Commissioner's Office to the Consultation on a New Pro-Competition Regime for Digital Markets

About the Information Commissioner's Office

The Information Commissioner's Office (ICO) has responsibility for promoting and enforcing the UK General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA18), the Freedom of Information Act 2000 (FOIA), the Privacy and Electronic Regulations 2003 (PECR) and the Environmental Information Regulations 2004 (EIR).

The ICO is independent from government and upholds information rights in the public interest, promoting transparency and openness by public bodies and organisations and data privacy for individuals. It does this by providing guidance to individuals and organisations, solving problems where it can, and taking appropriate action where the law is broken.

Introduction

The ICO welcomes the Government's consultation on a new pro-competition regime for digital markets presented by the Department for Digital, Culture, Media & Sport and the Department for Business, Energy and Industrial Strategy.

We recognise that the concentration of power in a small number of dominant online firms poses serious challenges for markets, businesses and, most importantly, consumers. We consider that the Government's proposals for a new pro-competition regime, as a whole, will form a critical plank in the UK's overall framework for digital regulation by preventing and addressing abuses of market power. Together with the data protection regime, we consider that this package will promote trust in the digital economy and help the UK remain a global hub for competitive and innovative digital services.

These proposals will not just deliver improvements to competition: they have the potential to deliver significant improvements to data protection in digital markets, as people benefit from greater choice and control over how their data is used. The ICO and the Competition and Market Authority (CMA) have initiated an ambitious programme of regulatory collaboration to examine and leverage the synergies between the objectives of competition and data protection, both bilaterally and through the Digital Regulation Cooperation Forum (DRCF). We welcome the opportunity that the new pro-competition regime brings to expand on this collaboration.

To promote alignment and coherency between privacy and competition regimes, **we recommend the Government establish formal mechanisms for collaboration between the ICO and the Digital Markets Unit** (DMU). Specifically, we recommend the ICO be formally consulted prior to:

- the design of principles in the Code of Conduct, and
- the implementation of pro-competitive interventions,

when the exercise of these functions is likely to significantly impact the processing of personal data. Incorporating these recommendations will better enable the ICO to work alongside the DMU in the interests of UK consumers.

Interactions between Competition and Privacy

Many of the harms that the ICO and CMA seek to address are rooted in the same challenge: the role of personal data in the digital economy.[1] The value of personal data increases as firms collect and analyse more information and access to this resource allows firms to optimise services, sell advertising and drive in-house innovation. These activities bring enormous benefit to consumers and the ICO recognises the importance of ensuring individuals have access to effective digital services.

However, the value of personal data creates clear incentives to collect and retain exclusive data holdings and leverage information for financial gain. Sometimes this can result in the unlawful processing of personal data and prevent individuals from taking effective control of their information. The sheer volume of data held by some firms also creates risk for people's privacy and enables them to wield significant power over data-driven markets and erect barriers against competitors. In these respects, it is clear that data protection and competition have common regulatory objectives.

The synergies between these regimes was outlined in detail in the publication of the ICO-CMA Joint Statement on Competition and Data Protection in Digital Markets on 19 May 2021.[2] This Statement acknowledges that both regimes play a fundamental role in protecting consumer rights and sets out how they complement each other by:

[1] See Joint Statement between the CMA and the ICO, pages 11-13
[2] See Joint Statement between the CMA and the ICO

- ensuring consumers have ample choice between digital services, including services that offer strong privacy protections and limit the exploitation of personal data

- harnessing competitive pressures to support the development of privacy-friendly technologies and promote the use of clear, user-friendly controls, and

- promoting trust in digital markets by assuring consumers not only that their data is being handled securely, fairly and lawfully but also through reducing information asymmetries.

Importantly, the Statement dispels misconceptions about the misalignment between the interests of competition and data protection, noting that perceived conflicts are exaggerated. For example, rather than blocking competition remedies designed to equalise access to data, data protection law can facilitate data sharing by reassuring consumers that disclosure of their personal information is occurring lawfully, transparently and fairly. Some data sharing initiatives, such as the data portability schemes increasingly being adopted in the UK and abroad, have the potential to both foster competitive pressures in markets and increase an individual's control over of their data, meeting key objectives for both regulators.

The expectation (and need) for coordination on competition and privacy issues will only grow as personal data becomes increasingly intertwined with questions of market dominance. Indeed, a number of recent cases have highlighted the complex and multifaceted ways in which antitrust and data privacy law are meeting. For example, in 2019 the German Bundeskartellamt, for the first time in a competition case, drew a direct link between the processing activities of Facebook and its abuse of market power.[3] Similarly, in an ongoing antitrust case the United States Federal Trade Commission alleges that Facebook bought-or-buried competitors, suppressing innovation and subjecting users to lower levels of data protection and more intrusive advertisements.[4]

The relationship between competition and privacy is now taking on a new dynamic. Companies that grew in market share partly due to the collection and processing of significant volumes personal data have begun to introduce measures ostensibly aimed at protecting user privacy. However, these same measures have prompted concerns that leading firms are using data protection

[3] See the Bundeskartellamt case file
[4] See the Federal Trade Commissioner press release

as a vehicle to reduce third-party access to data, preference their own competing services and entrench their market power. Close collaboration between competition and data protection authorities is needed to identify where privacy measures are required by law, and where they may be a smokescreen for anticompetitive behaviour.

For example, the CMA's investigation into Google's Privacy Sandbox, assisted by the ICO, was in part instigated by complaints the CMA received that, if implemented, Google's proposals would amount to an abuse of its dominant position.[5] Similar concerns have been raised about Apple's App Tracking Transparency update, rolled out earlier this year in iOS 14.5. The update requires applications to request user permission if they want to track their online activity by default and led to a joint inquiry by the French competition and data protection authorities as well as a complaint before the German Bundeskartellamt.[6] This matter is also being considered by the CMA as part of their Mobile Ecosystem Market Study, launched 15 June this year.[7]

These cases demonstrate the need for close formal coordination between regulators to understand the complex dynamics at play. To identify and adopt a coherent regulatory approach in the consumer's best interest, data protection and competition authorities can no longer work in isolation.

The Need for Formal Collaboration

While the ICO and CMA have been able to achieve much through our existing bilateral partnerships and under the auspices of the DRCF, there are limits to such voluntary coordination mechanisms. As the above cases demonstrate, the intricacy, breadth and significance of the interactions between our regimes in the digital economy necessitates a statutory basis for our collaboration.

A reliance on methods of informal cooperation risks placing too much emphasis on relationships and leaves critical regulatory outcomes vulnerable to changes in personnel, shifting priorities and resource constraints. Further, the lack of a clear legislative framework to guide joint-work on privacy and competition can create legal uncertainty, particularly with regards to information disclosure and the scope of matters regulators can take into account when undertaking a regulatory intervention. A mandate for the DMU to consult on, and account for, privacy and data protection interests would do much to resolve current ambiguities,

[5] See the Notice of intention to accept binding commitments offered by Google
[6] See the Autorité de la concurrence summary
[7] See the Mobile ecosystems market study Statement of Scope

encourage necessary information sharing and ensure both regulators are not unduly restricted by existing statutory frameworks and legislative objectives.[8]

Industry and the public expect regulators to work together on these matters. Formal mechanisms for cooperation between ICO and CMA would provide additional clarity on how these two regimes interact and add welcome transparency to the regulatory process. For instance, statutory provisions that facilitated ICO input into the design of a pro-competitive intervention would establish a single channel to consider and communicate the relevant privacy dimensions to the affected firm and give other digital firms and consumers confidence that the broader implications for data protection had been considered.

In considering privacy matters, it will not be sufficient for the DMU to only take account of whether a firm with Strategic Market Status (SMS) is compliant with data protection law. The largest tech platforms are hugely influential players in the wider digital economy; through their functions as the 'gatekeepers' of digital bottlenecks such as app stores or as operators of key digital platforms, like browsers and online marketplaces, they are able to set the terms by which smaller firms engage with their customers or handle personal data. For instance, Google's move to remove support for third party cookies in Chrome (the Google Privacy Sandbox) is likely to significantly influence how AdTech market participants process personal data. The DMU will need to be empowered to consider the impacts of its interventions on privacy in the wider ecosystem, supported by analysis by the ICO. Ultimately, coordination on such interventions will help address both regulators' goals jointly and reduce the need for further intervention in the wider market.

Importantly, the inclusion of formal coordination mechanisms that allowed the DMU to benefit from ICO expertise on data protection issues would complement parallel proposals for the ICO (and other regulators) to adopt a secondary competition duty. However, the ICO is not suggesting that the DMU be subject to broader duties or responsibilities in relation to data protection or privacy; indeed we consider that early and meaningful consultation with the ICO on specific aspects of the proposed regime would do much to enable positive and coherent regulatory outcomes.

The Enforceable Code of Conduct

[8] Legislative proposals are now being developed in other jurisdictions that formally recognise the interaction between competition and privacy regimes. For example, the Open App Markets Act , a bipartisan Bill introduced into the United State senates to curb the impact of market dominance in app stores, includes a provision which shields a company from violation of the law if the alleged anticompetitive conduct in question was necessary to achieve user privacy, security or digital safety

We welcome proposals for an enforceable Code of Conduct (the Code) for SMS firms and agree that such an ex-ante regime could help prevent firms from engaging in anticompetitive behaviour. We note that the Code objectives of Fair Trading, Open Choices and Trust and Transparency have been developed and refined over an extended period – starting with the recommendations of the Digital Competition Expert Panel, and continuing via the CMA Online Platforms and Digital Advertising Market Study, the Advice of the Digital Markets Taskforce, and now this consultation.

However, there are clear parallels between the ICO's remit and the principles, guidance and regulatory activities that would underpin the Code. For instance, Code principles that set benchmarks for transparency, accessibility or accuracy could conflict with an SMS firm's obligations under Article 5 of the UK GDPR, which require organisations to meet standards of transparency, fairness, accuracy when processing personal data. Equally, Code requirement for SMS firms to secure some form of consent from its users for a particular activity could be inconsistent with the standards for consent in Article 6 of the UK GDPR or Regulation 6 of the Privacy and Electronic Communications Regulations (PECR).

Given the above, we are of the view that across the Code objectives there is significant potential for ex-ante competition regulations to interact with the UK's data protection framework and for existing data protection regulation to influence the design and application of any Code principles. In light of the potential for overlap, **we recommend that the Government ensures that the ICO is formally consulted when a Code principle is designed or updated in cases where that principle may impact the processing of personal data**. We note that in any consultation requirement there will be a need to mitigate the potential for administrative burden.

Of course, the above recommendation assumes that the Code principles will not be established in legislation. Consistent with the Advice of the Digital Markets Taskforce we consider that a sufficient level of flexibility would be achieved if the objectives of the Code of Conduct are set out in legislation and the remainder of the content of the Code (i.e. the principles and guidance) are determined by the DMU, subject to the needs of procedural fairness. This approach will ensure that the DMU has appropriate discretion to apply an agile regulatory approach to SMS firms who are operating in complex, fast changing digital markets and allow the DMU, in consultation with the ICO, to design Code principles that deliver optimal competition and privacy outcomes.

Pro-Competitive Interventions

The ICO recognises the capacity for pro-competitive interventions (PCIs) to drive change in digital markets and create opportunities for innovation and economic growth. Importantly, we recognise the potential for PCIs to address the same root causes of market power in digital markets that also lead to data-protection and privacy harms. For example, if an SMS firm operated a suite of online messaging services and used its dominant position to unlawfully process personal data or restrict the privacy protections available to individuals, a PCI that functionally separated these services and promoted consumer choice may deliver significant competition *and* privacy benefits. Equally, a data access intervention that facilitated the transfer of personal data to competitors may increase the risk of a data breach if implemented without prior ICO input.

Prior consultation on a PCI would also limit the ability of any SMS firm to raise data protection concerns as a smokescreen to oppose the intervention. Working with the DMU, the ICO could test the veracity of any claim and limit the impact of any true privacy risks. Relevantly, the ICO-CMA Joint Statement on Competition and Data Protection stressed that where data access interventions have been identified as an appropriate remedy, collaboration between both regulators is critical to ensure any intervention is necessary and proportionate and does not facilitate harmful practices.[9]

As with the Code of Conduct, any PCI that has the potential to impact the ICO's remit would benefit from our scrutiny. Accordingly, **we recommend that the Government ensures that the ICO is formally consulted in the development of PCIs with an impact on the processing of personal data**. As before, we note that in any consultation requirement there will be a need to mitigate the potential for administrative burden.

Designation of firms with Strategic Market Status

In addition to the points raised on specific powers for the DMU and CMA, the ICO **would welcome further discussion with Government** on particular aspects of the regime design, specifically:

- The scope of the SMS designation assessment, where we are eager to understand how a designated activity would apply to the processing of

[9] See Joint Statement between the CMA and the ICO, page 24

personal data by a SMS firm and whether it might capture processing functions that are indirectly related to the activity in question.

- The distinction between SMS firms and data controllers. While in many cases we understand an SMS firm is likely also to be a data controller, there may be instances where controllership rests with another organisation. We would like to understand more about how the regulation of SMS firms might impact the data protection obligations of an associated controller.

Merger Review

The ICO supports merger reforms that strengthen the CMA's ability to prevent concentration and market power manifesting in digital markets. We consider these reforms will help reduce power asymmetry between individuals and dominant firms, empower consumers and prevent the potential dampening of innovation.

In the Advice of the Digital Markets Taskforce the ICO considered it already has the requisite powers to enforce data protection and e-privacy concerns identified in mergers and we did not propose that the merger regime account for non-competition concerns.[10] The ICO maintains this position.

However, we note that privacy has sometimes been considered in the wider context of merger review, chiefly by treating privacy as an element of quality-based competition, i.e. will the merger reduce the level of privacy protection afforded to consumers and thereby impact the quality of the service.[11] Indeed, privacy was considered 'an important parameter of competition between professional social networks on the market' in the European Commission's review of the Microsoft / LinkedIn acquisition.[12] In instances where privacy is being treated as an aspect of quality-based competition, the CMA may benefit from our privacy expertise and **we would encourage the CMA to consult the ICO on such matters.**

We are also aware of broader privacy concerns associated with data-driven mergers in which the data of the acquired firm is combined with the data of the acquiring firm.[13] While such concerns are typically considered beyond the

[10] See the Advice of the Digital Markets Taskforce, page 64
[11] See Digital Crossroad: The Intersection of Competition Law and Data Privacy, page 83
[12] See the European Commission's press release
[13] Google's acquisition of Fitbit is illustrative, see the European Commission's case file

purview of antitrust authorities, their potential data protection impacts, particularly with regards to enhanced sharing of sensitive data and user profiling, are of regulatory interest to the ICO. As above, **we would encourage the CMA to consult the ICO where these merger cases arise** and reiterate the Taskforce's position that information exchange and close cooperation is needed.[14]

The ICO is committed to continuing to support the Government and the CMA on the implementation of the pro-competition regime (including through the DRCF). We look forward to engaging further on the issues highlighted and on any other areas where the ICO's experience and expertise would assist the Government.

Elizabeth Denham
Information Commissioner
30 September 2021

[14] See Appendix F of the Advice of the Digital Markets Taskforce, page F38