

Response of the Information Commissioner's Office to the consultation on the Online Advertising Programme

About the Information Commissioner's Office

The Information Commissioner's Office (ICO) has responsibility for promoting and enforcing the UK General Data Protection Regulation (UK 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 the Online Advertising Programme (OAP). Addressing the issues present within online advertising will deliver clear benefits for the public and industry, including reducing risks arising from illegal and harmful advertising, combating fraud, and improving outcomes for legitimate advertisers promoting goods and services to individuals.

The complexity and opacity of the online advertising ecosystem described within the OAP consultation aligns with the ICO's own understanding of the advertising supply chain, which we set out within our 2019 update report into adtech and real-time bidding (RTB)¹. We agree with the government's assessment that a lack of transparency and accountability are key drivers of harm across online advertising, and we welcome measures designed to address these issues.

That being said, as the OAP develops, the government should undertake further analysis of the role existing regulatory regimes, such as that of the ICO, play in addressing harms arising from online advertising and ensure that reforms are only pursued where regulatory gaps are clearly identified, or where evidence demonstrates that an increased level of regulatory oversight is necessary. In areas of the online advertising supply chain where existing regimes provide the tools necessary to tackle harm, there should be no need to introduce additional regulatory requirements and oversight. To do so would create unnecessary

¹ <https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf>

regulatory overlap, leading to complexity and uncertainty for the public, industry and regulators.

The ICO's role complements the objectives of the OAP in tackling data-enabled harms within the online advertising industry. We encourage government to ensure that the role of the ICO is recognised throughout the development of the OAP, regulatory overlap is avoided, and interactions between our remit and that of any statutory or non-statutory regulator in the online advertising space are carefully managed to achieve a coherent regulatory framework.

The ICO has benefited from a close and effective relationship with the Advertising Standards Authority and close cooperation with the ICO will be required of any online advertising regulator. We recommend that, should reforms be pursued in order to address any identified regulatory gaps, any online advertising regulator be placed under a formal duty to consult with the ICO in respect of privacy and data protection impacts, notwithstanding the statutory duty to consult under Article 36(4) of the UK GDPR. We stand ready to help shape any future regulatory framework through collaboration with government and relevant regulators, and we are committed to working in tandem with the OAP to address harms arising from online advertising.

The ICO's role in regulating online advertising

In programmatic advertising, including real-time bidding (RTB), information is collected about the online behaviour of individuals through the use of cookies and similar technologies on online services provided by publishers. The personal data collected can be used to build profiles about individuals to analyse or predict their preferences, behaviours and attitudes, and ultimately to target advertisements to them².

Such collection and processing of personal data must take place in compliance with the rules and principles set out in UK GDPR, DPA18, and PECR. As such, there are substantial interactions between the ICO's remit and that of any online advertising regulator.

Targeting of advertisements

Harms caused by the placement and targeting of advertisements are often driven by the processing of personal data that takes place to facilitate that targeting. For example, discriminatory targeting can be facilitated by data collection and profiling that allows adverts to be shown to users on the basis of protected characteristics that they possess, or on the basis of other information that acts as a proxy for protected characteristics.

Tackling the underlying drivers of harm upstream, at the point of data collection and onward processing³, can reduce the downstream harms that can surface when advertisements are targeted at and served to users. Addressing placement

² The ICO's 2019 report into adtech and RTB provides a more a detailed explanation of the collection and use of personal data in the online advertising supply chain.

³ The ICO published an overview and taxonomy of data protection harms in April 2022: Data Protection Harms | ICO

harms in this way can also help reduce the impact of content harms, by reducing the likelihood that vulnerable users are specifically targeted with illegal or harmful content.

Audience restriction

In some cases, it may be appropriate to prevent the delivery of certain advertisements to specific groups of individuals altogether. The ICO supports the development of proportionate and effective safety measures that ensure age-restricted or harmful content is not targeted at children and other vulnerable groups.

Audience restriction, where this does not take place through contextual cues, is often carried out through profiling based on personal data. This can involve intrusive activities such as access to government-issued identification to verify age, or processing of information that identifies an individual as vulnerable.

Any requirement to introduce methods of audience restriction should ensure that technical solutions are developed in a manner that is proportionate to the harms they are designed to address, have measures in place to mitigate any privacy risks arising from their use, and ultimately comply with data protection law. The ICO has issued an opinion on data protection expectations for age assurance technologies⁴ and stands ready to work with government and any online advertising regulator on any proposed use of profiling.

Interactions between the data protection and online advertising regimes

In summary, the ICO's remit complements that of any online advertising regulator but, should reforms be pursued, the interactions between the two regimes will need to be carefully managed to ensure the development of a coherent regulatory framework. We recommend that any online advertising regulator be placed under a formal duty to consult with the ICO in respect of privacy and data protection impacts, notwithstanding the statutory duty to consult under Article 36(4) of the UK GDPR.

Key elements of data protection law

Below, we set out elements of the laws overseen by the ICO that play a critical role in mitigating harms arising from the data processing elements of the online advertising ecosystem.

PECR, data collection and consent

PECR requires organisations to provide clear and comprehensive information about the purposes of any cookie or similar technology that stores information (or accesses information stored) on user devices, and to obtain prior consent for such storage and access, which must be to the UK GDPR standard. The exemption from this requirement for cookies which are 'strictly necessary' does not apply to cookies used for advertising purposes.

⁴ Age Assurance for the Children's Code (ico.org.uk) (p.32)

PECR rules take precedence over the UK GDPR. In practice, this means that as explicit consent is required to collect data under PECR, consent will also be the appropriate lawful basis for processing under the UK GDPR. Consent should be given as a positive opt-in, and it should be as easy to withdraw consent as to provide it. In the context of online advertising, PECR consent requirements mean that users should easily be able to prevent data collection for the purposes of targeted advertising. These existing legislative requirements provide a check on intrusive or harmful targeting of online advertising, which cannot take place where personal data has not been collected to enable it.

Transparency

The UK GDPR transparency provisions require organisations that process personal data, including those within online advertising, to provide users with clear information about the personal data that is collected, what they do with the data they collect, the organisations that it is shared with, and how individuals can exercise their data protection rights⁵. Due to the complexity and opacity of the online advertising ecosystem, the ICO has observed that organisations are often unable to provide the information required, and may themselves not know with whom the data will be shared.

Transparency requirements under data protection law are closely linked to the broader issue of transparency in online advertising. The requirement to provide clear information to internet users about how their personal data will be processed to target and serve advertisements necessitates that the organisations involved understand the nature of their processing, and that the processing itself be reasonably comprehensible. The transparency provisions of the UK GDPR play a critical role in mitigating the risks presented by the complexity and opacity of the online advertising ecosystem.

Lawfulness and fairness

The UK GDPR's provisions on lawfulness and fairness require that the processing of personal data takes place in ways that comply with the law (not limited to data protection law) and that users would reasonably expect. Individuals should not be misled about processing and organisations should consider the effect their processing may have on individuals and justify any adverse impact.

Fairness is intrinsically linked to transparency around data collection in the online advertising ecosystem; the processing that takes place should match the information provided to users when their consent is obtained. Where processing is not fully explained to users, or would not be expected by users, it will fail to meet the requirements of the first data protection principle.

To guarantee that personal data is processed fairly and lawfully, organisations within the online advertising ecosystem must ensure that they have sufficient oversight of the processing taking place, both by themselves and by any other organisations that personal data is shared with.

⁵ <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/>

Organisations must also anticipate and justify any adverse effect that their processing has on individuals. The fairness principle therefore provides an existing requirement for organisations to anticipate and mitigate any harms that might arise from discriminatory targeting or mis-targeting of users.

Accountability

The UK GDPR's accountability principle holds organisations responsible for complying with the law, and requires that they are able to demonstrate their compliance⁶. The accountability principle introduces an obligation on organisations, including those within the online advertising ecosystem, to take appropriate action to achieve compliance, maintain records about how they process personal data, and be able to provide information to individuals about how their data is processed. The accountability principle therefore plays a crucial role in providing additional transparency around the processing of personal data within the online advertising ecosystem.

Special category data

Special category data under the UK GDPR is personal data that requires additional protection due to its sensitive nature and the increased potential for harm arising from processing⁷. Several protected characteristics fall within the bounds of special category data, including sexual orientation, race, ethnicity, and health. The UK GDPR provisions on special category data act as an important tool in limiting the harm that can be caused by discriminatory targeting of online advertising as, in practice, such activity can only take place with the explicit consent of the user.

Children's data

The Children's Code (formally, the Age Appropriate Design Code)⁸ is a statutory code of practice prepared under section 123 of the DPA 2018, that protects children within the digital world by ensuring that online services are designed with them in mind.

Online services likely to be accessed by children should ensure that their processing of children's personal data is compliant with the UK GDPR, and that the best interests of the child are considered throughout. The Code is intended to ensure that a child-centric approach is built into the design of online services from the ground up, and many services involved in the delivery of online advertising fall within its scope.

Compliance with the Children's Code means that the best interests of the child must be a primary consideration when collecting and processing children's personal data. Services must avoid detrimental use of data, turn profiling off by-default (unless they can demonstrate a compelling reason otherwise), and

⁶ <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/>

⁷ <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/>

⁸ <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/>

provide transparency information in clear language suited to the age of the child. Conformance to the standards of the Code will limit collection, profiling, and targeting using children's personal data for delivery of online advertising.

The Code complements the aims of the OAP in protecting children by limiting the data collection and processing that facilitates online advertising, thus preventing harms to children from occurring downstream. The introduction of the Code has already prompted online services to make changes to better protect children, and we are continuing our supervisory work to ensure that online services, including those engaged in online advertising, conform to its standards.

Current ICO activity in relation to online advertising

ICO investigation into adtech and real-time bidding

The ICO resumed its investigation into adtech and RTB in January 2021 following a pause due to the early impacts of the Covid-19 pandemic. The investigation aims to develop the ICO's understanding of the RTB industry, improve industry understanding of UK GDPR and PECR compliance requirements, and take proportionate regulatory action where necessary to address harms and ensure that online advertising participants comply with the data protection provisions described above.

The investigation has continued with a series of audits focusing on the practices of relevant adtech companies. We are currently focusing on market actors that are central to data processing practices within the ecosystem to highlight the nature of issues that we expect to be widespread. Our investigation into the practices of adtech companies also links to our 2020 investigation into data broking⁹, and we are reviewing the role of data brokers within the ecosystem.

Our investigation will continue as the OAP progresses and we are committed to working with government to manage interactions and coordinate our work on adtech. This will help to ensure a coherent approach that provides clarity on regulatory expectations to industry, while delivering the benefits of a compliant online advertising system to users.

ICO expectations for future online advertising proposals

Since 2019, industry has developed several initiatives that seek to address the risks adtech poses and shift towards less intrusive tracking and profiling practices. These include proposals from Google and other market participants to phase out the use of "third party cookies" and other forms of cross-site tracking and replace them with alternatives.

The ICO has been collaborating with the Competition and Markets Authority (CMA) in assessing these developments and ensuring they meet the requirements of data protection and competition law. In July 2021, the ICO and CMA issued a joint statement outlining that the interest of consumers is best

⁹ <https://ico.org.uk/action-weve-taken/investigation-into-data-protection-compliance-in-the-direct-marketing-data-broking-sector/>

served when the objectives of both competition and data protection are achieved¹⁰.

The proposals from Google and other market participants are not yet fully realised and there is a window of opportunity for proposal developers to introduce a data protection by design approach. In November 2021, the ICO issued an opinion on data protection expectations for future online advertising proposals¹¹.

The ICO and the CMA continue to work closely together so that developments in the adtech industry operate in a data protection compliant way that ensures an appropriate level of competition. In February 2022, the CMA published its decision to accept commitments from Google in relation to its proposals to remove third party cookies, which include a commitment to evaluate its proposals for their impact on privacy outcomes and compliance with data protection principles¹².

Future legislative reforms

It will be important that the design of the online advertising regime takes account of developments in data protection law and other areas of digital regulation.

Data protection

The government's proposals for data protection reform will have an impact on the online advertising ecosystem. The ICO welcomes the recognition in the consultation that users value privacy and want control over how their personal data is used. We support data protection reforms that would improve the level of control that individuals have over the use of their personal data in online advertising, such as proposals to allow browser settings to express user preferences¹³ and to bring the ICO's PECR enforcement powers into line with the UK GDPR and DPA¹⁴.

In our response to the government's 2021 'Data: a new direction' consultation¹⁵, and through our ongoing dialogue with DCMS, we have provided feedback in relation to a number of data reform proposals, including those to remove requirements for prior consent for some types of cookies, and to facilitate innovate re-use of data for a different purpose, under a different lawful basis, or by a different controller. We recommend that there is coordination between the government's data protection reform work and the OAP to ensure that a

¹⁰ <https://ico.org.uk/media/about-the-ico/documents/2619797/cma-ico-public-statement-20210518.pdf>

¹¹ <https://ico.org.uk/media/about-the-ico/documents/4019050/opinion-on-data-protection-and-privacy-expectations-for-online-advertising-proposals.pdf>

¹² <https://www.gov.uk/government/news/cma-to-keep-close-eye-on-google-as-it-secures-final-privacy-sandbox-commitments>

¹³ Paragraph 204: Data: a new direction (publishing.service.gov.uk)

¹⁴ Paragraphs 216-218: Data: a new direction (publishing.service.gov.uk)

¹⁵ <https://ico.org.uk/media/about-the-ico/consultation-responses/4018588/dcms-consultation-response-20211006.pdf>

consistent approach is adopted to tackling harms within the online advertising industry.

Competition

There is an ongoing need to reconcile pro-competition and pro-privacy regulatory measures in the online advertising ecosystem. The ICO and the CMA continue to work closely together, both bilaterally and through the Digital Regulation Cooperation Forum (DRCF), to ensure that competition and privacy law are respected and complied with as the online advertising industry develops solutions to identified issues within the ecosystem.

This collaboration will continue with the introduction of new competition rules for digital markets and the largest digital firms through the future Digital Markets, Competition and Consumer Bill. Our collaborative approach provides greater clarity for industry stakeholders and ensures coherence as technological and regulatory approaches to compliance issues develop.

As the government proceeds with implementation of the OAP it will be important for any online advertising regulator to work closely with both the ICO and CMA in pursuit of a fair, competitive and transparent ecosystem for users.

Online safety

The OAP consultation highlights the role of the Online Safety Bill's (OSB) provision on fraudulent advertising in protecting consumers online. It should also be noted that there are further interdependencies between the OAP, the OSB and the ICO's remit, particularly in relation to the use of age assurance technologies and the Children's Code.

As with competition law, the ICO is keen to ensure that the interactions between online safety, data protection and regulation of online advertising are managed carefully throughout the OAP, and we are committed to working with government and our regulatory partners to achieve a coherent framework for digital regulation that delivers benefits for users and businesses alike.

Conclusion

The ICO is committed to supporting the government in the development and implementation of reforms to the regulation of online advertising. We look forward to engaging further on the issues highlighted in this response and on any other areas where the ICO's experience and expertise would assist the government.