IAB UK Submission to the CMA following Google's changed approach to Privacy Sandbox, announced July 2024

[in response to the CMA's call for views]

Background

1. As the CMA's *Online platforms and digital advertising market study* explored, in digital advertising, the open display market uses an intermediated model where a supply chain of third-party intermediaries facilitates the buying and selling of digital advertising space, and related services (such as targeting – both personal and contextual – measurement, anti-fraud, brand safety, etc.).
2. In a web environment, many media owners/service providers with ad-supported business models operate within the open display supply chain. Entities in that supply chain that wish to process personal data or use cookies have compliance obligations that depend on the ability to communicate with individual users to provide information and capture their choices and, where appropriate, to signal those choices to other entities in the supply chain. For example, to provide transparency and/or obtain consent for processing personal data or using cookies.
3. In this context, in a web browser environment, both the media owners/service providers and their advertising partners rely on the necessary user interactions taking place on a site-by-site basis via the media owner/service provider. While some media owners/service providers may have first-party relationships with their users, for example, if they have accounts or logins, third parties in the open display supply chain have no direct relationship with users and cannot interact with them directly in this context.
4. The same requirements apply to sites that are not ad-funded but that may also use cookies or process personal data for advertising-related purposes, for example, retailers or brands who want to serve ads to people who've visited their sites, measure interactions with their ads or measure the outcomes of their ad campaigns (e.g. site visits or purchases). These entities need to be able to communicate directly with their users about the use of personal data and cookies (whether first or third party), both on and off their own media properties, for the commercial and compliance reasons described above.
5. IAB UK and its members have previously identified potential issues or challenges in relation to proposals for user choices/controls to be managed at the browser level, in terms of data/cookies used for advertising purposes. These are shared below. They are not specific to Google's proposal, and they relate to the scenario described above, where media owners/service providers and advertising entities are reliant on user interfaces on individual websites for advertising purposes and to meet their legal obligations for processing personal data and using cookies, for a range of purposes.

Note: extracts are provided below from previous responses that we think are relevant to the CMA's call for views and they should be read in that context.

Data reform consultation

6. In 2021, DCMS launched a consultation on reforms to the UK's data protection regime. This included asking questions about an approach whereby users can express their privacy preferences through browsers, software applications and device settings, although no developed proposals were put forward in the consultation.

Extract from IAB UK's response to the Government's consultation on 'Data: A new direction', November 2021

Q2.4.6. What are the benefits and risks of requiring websites or services to respect preferences with respect to consent set by individuals through their browser, software applications, or device settings?

Our concerns about centralised privacy controls include:

- Potentially obstructing providers of ad-funded content and services in communicating with their users about why and how they use their personal data, and the value exchange. Having the relationship with the consumer intermediated by a browser, operating system or device hinders a service provider from building a trusted relationship with their user base.
- Whether centralised, 'general' choices (e.g. granting or withholding consent) and the insertion of an independent third party can meet the specificity requirements on data controllers to obtain consent under the GDPR. If not, then…users would still face specific consent requests in addition to the general consent of the browser/software layer.
- As a matter of principle, it is important that legislation does not dictate which technologies must or can be used to capture and set users' choices. It would need to be clear that software, browsers etc. would be neutral in the user relationship. For example, they could prevent the processing of personal data or use of cookies. which would hinder a service provider's ability to lawfully collect or display information. Browsers and other software are not able to distinguish between, for example, data processing purposes that (under either the current or a future framework) do or don't require consent; is lawful or unlawful; etc.
- There may be competition implications of centralising controls through software and tools provided by private companies and these need to be fully explored and understood. The CMA is investigating the deprecation of third-party cookies in Chrome and the potential impacts for competition in digital advertising and the ecosystems that rely on it.

- We note that the ICO's response[1] to this consultation strongly supports such an approach to managing data preferences. Its response says:

  The consultation's inclusion of the use of browser and non-browser based solutions is a good one. This is where people can say once how they would like their data to be used and have this respected across the online services they visit. This would allow people to choose to go pop-up free
- In our view, the ICO's narrative vastly over-simplifies the practical, legal, economic and competition implications that would result from a move away from transparency and consent notices, that online services are in effect required to use in order to comply – and demonstrate compliance – with UK GDPR and PECR, to centralised controls via browsers or other means.

  ....

  the ICO has not, to our knowledge, consulted with affected industry sectors nor provided any detailed information about its work or thinking in this space beyond broad public statements.
- The ICO's response also suggests that this approach could address concerns identified in the CMA's Market Study. However, there are obvious overlaps with the CMA's current work to examine the operation of certain browsers and the impact they could have on competition in the digital advertising market. This is a priority project in the DRCF's work programme and this is important context for this proposal, noting government's proposal (in this consultation) to require the ICO to have regard to competition when discharging its functions.

The DPDI Bill

7. One of the proposals in the DPDI Bill, which was in part informed by the consultation referred to above, was to introduce legal provisions to facilitate 'browser-based or similar solutions' for managing cookie consent (but not consent under the UK GDPR) and to set requirements for the automated signalling of user choices.

Extract from evidence submitted by IAB UK to the DPDI Bill Public Bill Committee

<u>The policy intention</u>

- The Government's goal is to enable UK consumers to set their cookie choices centrally, e.g. in a browser, software or device. They state that the changes to PECR made by the DPDI Bill are intended to 'pave the way for the removal of irritating banners for...cookies' when there is 'sufficient availability of technology which enables subscribers or users to effectively

[1] https://ico.org.uk/about-the-ico/consultations/department-for-digital-culture-media-sport-consultation-data-a-new-direction/

express their consent preferences'.[2] The Bill empowers the Secretary of State to implement this systemic change in the future via regulations.
- However, our members have significant concerns about this approach, which poses serious legal and commercial risks for the ad-funded internet. While the provisions in regulation Clause 79(3) look innocuous, that is because they contain scant detail.
- The Data Reform consultation that preceded the Bill did not consult on any specific proposals, but asked broad questions about different ways that consent mechanisms might work. The final policy was not discussed with the affected industries before being included in the Bill, and while the consultation asked about the risks of centralised controls, no plan has been put forward for mitigating them. There is no clear explanation of how the policy might work anywhere and there is no transparency about the eventual decision-making by the Secretary of State.

<u>Challenges and risks</u>

- Changes in this area are not straightforward and require a full assessment of the likely practical, legal, economic and competition implications for the digital advertising sector. While annoying to people online, cookie banners will remain a legal requirement and have a legitimate function in enabling data controllers to record valid consent and demonstrate that they have met their transparency and consent obligations under the law – both PECR and UK GDPR – which needs to be taken into account in developing possible alternative approaches and balanced against the desire to improve people's online experience. It is also crucial that any changes do not undermine the provision of ad-funded content and services.
- It is also important to note that there are two 'consent' regimes that typically operate together. PECR requires consent to be sought to access or store information on a device (unless an exemption applies). The UK GDPR requires a legal basis to be established to process personal data which often happens in conjunction with the use of PECR-regulated technologies. One such legal basis is consent. 'Pop ups' or 'banners' on websites support both of these requirements.
- Put simply, making changes to the PECR consent regime in isolation may help to remove 'pop ups' for some websites in simple use cases but in many cases, legal obligations will mean that people will still have to receive information and make choices at the point of access.
- Without a more fully-developed proposal it's not possible to understand if the policy of centralised opt-out controls for cookies will actually improve people's online experience. There is a risk that the pressure for people to

[2] https://questions-statements.parliament.uk/written-statements/detail/2022-07-18/hcws210#:~:text=Reforms%20to%20the,are%20sufficiently%20developed and https://publications.parliament.uk/pa/bills/cbill/58-03/0143/en/220143en.pdf (para 565).

make a single choice to apply everywhere online would be overwhelming and may undermine people's ability to make informed choices or understand the consequences of those choices. They may simply switch off all cookies/similar technologies which would severely inhibit the functioning of online services.

- Additionally, making these mechanisms available via private companies (i.e. the owners of browsers, software, etc.) disrupts the relationship between the individual and the service they're using and creates risks around liability for legal compliance. There needs to be strong safeguards attached to third parties assuming this role, in order to protect consumers and UK businesses and due consideration also needs to be given to national security and data access concerns as well as how cookies are categorised

....

- This creates risks:
    a) Enabling cookie consent to be given via a third party intermediates the important relationship between service providers and their customers. It is possible that consent given via a third party could override valid consent previously given to a service a consumer values and trusts.
    b) The legal obligation to obtain and record valid consent will remain on the data controller(s) and/or the provider of the service and it is not clear which party is liable if that consent is not deemed valid and how it would be remedied.
    c) The legal obligation to obtain consent for each applicable purpose would also remain so there would be limited scope for a third party to improve the user experience.
    d) Other parties in the supply chain may rely on these consents, and the insertion of a third party to collect consent creates legal risk for those other parties.

8. IAB UK (and other advertising trade bodies) raised related concerns in our briefings to Parliamentarians about this aspect of the DPDI Bill during its passage through Parliament, which were:

- No proper assessments were published (or undertaken, to our knowledge) before this policy was announced, of:
    a) the potential competition impacts of a move to centralised consent management controls.
    b) the potential impacts of removing cookie banners on the services provided by ad-funded business models.
    c) the potential impacts of centralised control mechanisms on the user experience, particularly given that GDPR standards of transparency and consent (where applicable) will still need to be met, including where

personal data is being processed via or alongside the user of cookies/similar technologies.

9. The digital advertising industry also raised concerns with DSIT (which took over responsibility for the Bill) about its policy intentions and the potential risks and issues (including those set out above) multiple times, including once the Bill was originally published, when it was withdrawn and reintroduced, and during its passage through Parliament. Officials and Ministers recognised those concerns and DSIT committed to further stakeholder engagement and consultation to inform its policy development. However, to our knowledge, this consultation did not take place. Nor were specific proposals brought forward for how such a system of centralised consent controls and signalling might work in practice. Therefore, stakeholders have not had the opportunity to fully consider or analyse the potential impacts of such controls on their businesses, consumers, the market, the ad-supported internet or the digital economy as a whole.
10. We therefore do not yet have established views on the potential impacts of browser-level controls on users of digital services. However, we have noted (as set out above) that work needs to be done to understand the potential impact on the user experience and the implications for companies involved in the digital advertising market and supply chain. We have provided comments below about the need for further consultation to inform this work.

Regulators' activity and industry engagement

11. The implementation of 'global' browser-based data & privacy controls has potentially significant implications. This is a complex issue that needs to be managed carefully and with appropriate consideration of the many different potential implications. It is therefore critical that the CMA and the ICO:
    - Provide transparency to stakeholders about the process and criteria for considering the merits and implications of browser-based controls both in general, and in relation to specific proposals within Google's Privacy Sandbox implementation. 'Privacy' criteria should be based on existing legal standards set out in the UK GDPR and PECR.
    - Ensure a process is put in place for engaging with and consulting industry from the outset and before new user controls are rolled out.
    - Provide transparency throughout this process about the views/advice the ICO is giving to Google and to the CMA, because this has implications for other service providers and the market in general.

IAB UK
August 2024