ICO call for views approach to regulating online advertising
IAB UK response

General comments

- IAB UK and its members welcome the fact that the ICO is looking at how to encourage innovation in the online advertising market and considering how it can modify its stance on PECR to support investment in digital advertising, while safeguarding user privacy.
- We agree that data protection is paramount and that obtaining user consent remains the appropriate standard for many uses of personal data. At the same time, we believe it is important for the ICO to recognise that not all activities related to digital advertising present the same level of risks for the fundamental rights of data subjects and consequently, certain low privacy impact activities should not require consent.
- We want to work meaningfully with the ICO on exploring approaches to PECR that meet the stated objectives, i.e. to support commercially viable advertising models, that work for businesses and safeguard data subjects. However, we do have questions around the approach that the ICO is taking, given its narrow focus.
- Firstly, we find the timing of this call for views confusing as well as its sequencing with related ICO and government workstreams. For example, it comes in the middle of the Government's own work on how it will use its new powers under the Data (Use and Access) Act (DUAA) on PECR Regulation 6 exceptions. While we appreciate that the ICO wants to conduct its own work in this area, we believe it is crucial that these two work streams are carefully sequenced and coordinated. We would welcome more clarity from the ICO on how the output of this consultation will directly inform the government's work on developing exceptions. This would help to ensure regulatory and legislative coherence and provide businesses with some reassurance on how this combined work will affect long-term planning and investment. This would also help to provide more clarity to data subjects on their rights.
- Additionally, the ICO's prior consultation on proposed new storage and access guidance is also linked to the outcomes of this call for views but, similarly, has been separated from it. The ICO has yet to fully assess the significant additional and damaging consequences that would arise from the expanded scope of the guidance or provide businesses with a clear understanding of the next steps in the consultation process, including when the ICO will publish the completed impact assessment. We would welcome clarification as soon as possible on how the outcomes of this call for views will be interpreted alongside the proposed expanded scope of the storage and access guidance. A clear understanding of how these initiatives align will be critical for businesses seeking to innovate responsibly.
- IAB UK respectfully asks that the ICO times and sequences its work to more closely align with the needs of the industry and the commercial environment in which they operate. The preferred sequence of decisions would be:
    - Clarify that technologies which are ephemeral and do not store data on a user's terminal equipment under PECR should not be considered "storage and access".
    - Review the ICO's interpretation of "strictly necessary" so (a) it is not limited to the *technical* provision of the service from the sole perspective of the user, (b) it also factors in the perspective of the service provider and (c) the ICO is no longer categorical that no advertising purpose can ever be considered strictly necessary.
    - Provide time and space for DSIT's consultation on uses which should no longer require consent under the DUAA;

- We also note that in the ICO's letter to the Government in March, which outlined the ways it would support the objective that regulators support the Government's growth agenda, the ICO said it would be "cutting red tape for businesses by paving the way for privacy-friendly online advertising with a regulatory review"[1]. We presume that this call for views is intended as the delivery of this commitment and a key indicator that the ICO will use to demonstrate its delivery of this agenda.
- In this regard, the call for views confidently predicts this new regulatory approach will unlock business growth and innovation. As we note below, this call for views risks conflating the technical possibility of new advertising models with commercial viability and this cannot be presumed by the ICO or businesses. Further work is needed to fully understand what combination of factors are necessary to unlock investment in this market and the extent to which the ICO's proposals would shape investment decisions. We therefore believe it would be highly beneficial for the ICO to conduct and publish an economic impact assessment alongside its final statement for this call for views that would help demonstrate the tangible benefits of its proposed approach to digital competitiveness.

Section 1: Advertising purposes and capabilities

- Firstly, we welcome the ICO proactively asking what features and capabilities are needed for a "commercially viable" advertising model. It is crucial that the ICO's work is grounded in a solid understanding of the technical and commercial environments stakeholders operate in and the minimum requirements needed for advertisers and advertiser businesses to operate. However, we believe that the ICO should be guided by the practical realities of the market and avoid defining what is and is not "commercially viable" for businesses.
- Advertising funds a variety of online services with different cost bases, and each operates in a very different competitive landscape. The regulatory and commercial features, as well as the different actors of the supply chain, that will be needed for these different providers to thrive will therefore be extremely different. By prioritising certain features over others, the ICO risks incentivising one part of the ecosystem or a particular business model to the commercial detriment of another.
- Below is a brief and illustrative outline of what elements would be deemed as necessary for most of our members. Again, the ICO cannot assume that these features will operate in a homogenous way across the different parts of the advertising ecosystem or indeed make a model commercially viable by default. We also urge that, when assessing these, that the ICO adopts a risk-based and tech neutral approach.
- We would welcome further, more detailed conversations with the ICO and our members on these elements and how they work in practice.

Ad delivery and billing

- Impression tracking provides proof of ad delivery between advertisers and publishers and is therefore fundamental to the commercial relationship between the two. It requires temporary storage of ad delivery confirmations to verify that they have been successfully served to users.
- Session management cookies, which ensure consistent ad delivery during user browsing sessions. This allows advertising campaigns to be delivered coherently across multiple page views, preventing technical failures that would compromise advertiser investment.

[1] https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/03/package-of-measures-unveiled-to-drive-economic-growth/

- Conversion tracking and click tracking, which measures or verifies the performance of advertising services once a user has interacted with an ad (e.g. bought a product or signed up to a service). This type of tracking is essential to performance-based billing models that have become central to digital advertising's commercial viability. It is also essential to ad efficiency measurement.
- Viewability measurement, enables advertisers to know that their advertisements were viewable to users, not merely delivered to pages that users never saw. This again supports billing models commonly used in online advertising by ensuring payment only occurs for advertisements that had genuine opportunity for user engagement.
- Server-side logging, which maintain records of ad delivery, user interactions, and billing events that support transparent commercial relationships between companies operating in the online advertising ecosystem.
- Campaign management, which allows the coordination of advertising delivery across multiple websites and time periods, ensuring that advertiser objectives are met and billing reflects actual campaign performance rather than isolated transactions.

Ad fraud and prevention

- Traffic Validation, which uses IP address analysis to detect suspicious patterns such as multiple requests from single sources, proxy server traffic, and geographically inconsistent access. This helps to distinguish legitimate users from automated systems.
- Behavioural Analysis, which monitors user interaction patterns with ads including mouse movements, and page engagement duration. Machine learning algorithms can process these types of signals to identify sophisticated bots that attempt to mimic human behaviour, so this analysis addresses modern fraud techniques.
- Impression Verification, which ensures ads are viewable rather than hidden through fraudulent techniques. This includes detection of ad stacking and pixel stuffing, where advertisements are layered invisibly or rendered microscopic to generate false impressions whilst appearing legitimate to basic delivery tracking.

These capabilities require supporting technologies to create unique profiles identifying repeated fraudulent attempts, and traffic source verification validating referrer information and campaign parameters to prevent artificially generated traffic.

Brand safety, brand suitability and brand compliance

- Content Classification, which uses natural language processing and semantic analysis to categorise webpage content in real-time. This then identifies potentially harmful content including violence, hate speech, and misinformation, creating safety scores that enable automated placement decisions. Without this, advertisers risk association with damaging content that undermines brand reputation.
- Contextual Matching, which ensures ads appear alongside content that aligns with both advertiser values and target audiences. This includes keyword analysis and topic categorisation that prevents placement next to inappropriate subjects.
- Real-Time Filtering, which prevents ads from appearing on pages that violate brand guidelines, using pre-defined safety criteria to automatically exclude unsuitable inventory before impression delivery occurs.

These capabilities require supporting technologies including image and video recognition to analyse multimedia content beyond text, and domain reputation scoring that assesses publisher credibility and content quality patterns over time. However, it should be kept in

mind that this is analysis of *content*, as opposed to analysis of *users/devices* and is therefore privacy respectful.

Frequency capping

- Delivery control, which makes automated decisions to serve or suppress advertisements based on current frequency counts against predetermined limits. When users reach specified exposure thresholds, the system automatically excludes them from further campaign targeting for the remainder of the frequency period.
- Impression counting, which maintains accurate records of how many times each identified user has seen specific advertisements within defined time periods. This includes real-time tracking that updates exposure counts immediately upon ad delivery, ensuring current frequency data informs subsequent placement decisions.
- User identification, which uses cookies, device IDs, or other persistent identifiers to recognise the same user across multiple website visits. This technology enables the system to associate individual users with their advertising history, creating the basis for frequency management. Without reliable user identification, frequency limits cannot be enforced consistently.

These capabilities require supporting technologies including cross-site tracking in order to maintain frequency counts as users navigate between different websites within advertising networks, and campaign coordination systems that manage frequency limits in an open programmatic context across multiple creative variants and related advertisements.

Measurement and attribution

- Attribution Linking, which maintains the connection between ad exposure and subsequent user actions across time. This means tracking user journeys from initial ad contact through to final conversion, even when there are gaps or delays between seeing ads and taking action. The system needs to store and process this journey data to assign credit properly.
- Performance Reporting, which aggregates conversion data to present clear metrics that show campaign effectiveness. This includes calculating key performance indicators like cost per acquisition and return on ad spend, giving advertisers the information they need to make informed budget decisions and optimise their strategies.

These core functions need supporting technology including cross-site tracking that follows users across phones, tablets, and computers, and multi-touch attribution that handles complex customer journeys involving multiple ad exposures before conversion.

Targeting

- Audience segmentation, which utilises demographic data, browsing behaviour, or contextual signals to group users into meaningful categories that align with advertiser objectives. This allows campaigns to focus on people most likely to be interested in specific products or services, rather than showing ads randomly to everyone. Whilst we acknowledge that user profiling and behavioural advertising always requires user consent, without basic audience segmentation, advertisers cannot justify paying more than the cheapest possible rates for untargeted exposure. As such, the ICO should give consideration to what targeting (beyond contextual) should be permissible without user consent, for example the use of

data and signals shared by users directly, like the sports teams they support and their hobbies.

- Contextual matching, which places advertisements alongside content that naturally relates to the advertised products or services. This means analysing webpage topics, keywords, and themes to ensure ads appear in relevant environments where users are already thinking about related subjects. Contextual targeting works without personal data while still providing the relevance that makes advertising valuable.
- Delivery optimisation, which automatically directs ads toward audience segments or contexts that show better performance over time. This includes basic learning algorithms that identify which targeting approaches generate more clicks, conversions, or engagement, then shifting budget toward those more effective placements.

These core functions need supporting technology including real-time content analysis that can quickly categorise webpage topics and match them with appropriate advertisements, and campaign management systems that can coordinate targeting across multiple websites and platforms.

Section 2: Impacts of our approach

- The ICO's proposal to deprioritise its enforcement of PECR Reg 6 to "certain advertising purposes [that] can pose a low risk to user's privacy" assumes that this – and possibly this *alone* - would create sufficient commercial incentives for businesses to invest in untargeted advertising models to address the funding gap arising when consumers 'reject all'. We have concerns about this for several reasons:
    - The ICO risks overstating the degree to which the additional clarity around its approach to enforcement alone is beneficial to a company. Absent a change to PECR exceptions itself, it provides limited legal protection for companies and none from complaints from data subjects or litigation. This is why it is so fundamental that the government's work on PECR exceptions is prioritised ahead of this work and the ICO actively supports this work.
    - The proposal also risks assuming that this is the only certainty needed by businesses to have the confidence to invest in different advertising models. As noted above, a more nuanced interpretation of the underlying law as to what constitutes "strictly necessary", which weighs up both user privacy concerns and business operational needs, would be of greater value. Nowhere in PECR does it stipulate that 'strictly necessary' should be considered solely from the perspective of the consumer, so the ICO does have scope to interpret this in a slightly more expansive way. Without this, even if the ICO moves towards a relaxed enforcement approach for certain low-risk advertising activity, these will often not provide enough legal certainty for many businesses to take full advantage if no activity associated with digital advertising is seen as 'strictly necessary'.
    - Finally, the proposal also risks conflating the legal and technical *possibility* of developing a new ad model with commercial *viability,* where a model cannot operate where users 'reject all' cookies. This does not consider the full range of factors required to support the financial investment needed to develop and launch a new advertising model at scale. These factors include sustained and predictable demand from advertisers, and a price high enough to cover costs and a reasonable profit margin - plus the technical costs of changing how technology works, and the contract work needed to facilitate this with partners. Even with proposed change to the ICO's regulatory posture, we hear from members that the investment case for untargeted advertising remains weak.

- More fundamentally, any proposal must also recognise that the use of any storage and access technologies in a digital advertising context will almost always also involve some processing of low-risk personal data. A cookie is a non-persistent unique identifier that in most advertising instances will be considered pseudonymous personal data. But even assuming a cookie does not constitute personal data, it will be accompanied in many circumstances by an IP address (which again may constitute personal data) and likely other data that means personal data is involved. The ICO should recognise this so that it can be joined up in its proposal and to provide increased legal certainty across UK GDPR and PECR. For example, when outlining the activities that may be acceptable under PECR without consent, it should state that this will also be indicative that the activity may also be lawful under GDPR relying on legitimate interests – and importantly, without the need to offer an opt out.

- If a relaxed enforcement approach to low-risk activity where the consumer 'rejects all' is the only change the ICO were to make, and it continues to move ahead with its proposed storage and access guidance as drafted, we anticipate many more publishers and providers of ad-supported services will move to a 'pay or consent' model rather than explore the alternative models available. Given the challenging commercial situation many advertising or ad-funded businesses face today and the urgent need to explore new sources of revenue, this model would currently provide far greater legal certainty and immediate access to higher yield targeted ad revenues. It also benefits consumers as services could remain ad-funded and free to use and providers would have greater financial certainty to support product development and sustain these services over the long term.
- Providers unable to transition to a 'pay or consent' model may be able to access some incremental non-targeted ad revenue but over the longer term would likely experience a further decline in revenue, and some may reduce their offerings to UK consumers accordingly or exit the market.
- It is vital that the ICO is mindful of the potential for wider, unforeseen impacts on different business models as a result of its preferred approach and that the wider regulatory framework continues to support a diverse, competitive and innovative digital advertising system.

Section 3: Technical safeguards

- PETs cover a wide range of different techniques within online advertising and are not a single solution. Rather they are a toolkit of techniques that can be used alone or in combination for online advertising purposes. For example, technologies that add isolation protection (like Trusted Execution Environments and clean rooms) can allow for collaborative data analysis without exposing or transmitting the raw data, while technologies that anonymise data (such as those using differential privacy) can make data safer for processing and measurement.
- Although some of these technologies are promising, they face significant hurdles. Many PETs are still maturing, and their widespread implementation can be costly, complex and require specialist technical knowledge which is often in short supply.
- The ICO can play an important role in removing some of the barriers to adoption for those advertising businesses that PETs would work for. This could include:
    - Providing clear, practical and technology-neutral guidance on how PETs can be used to meet data protection obligations for online advertising purposes. This should include real-world examples of how specific PETs can mitigate risks associated with activities like ad measurement, fraud prevention and frequency capping.
    - Ensure the regulatory frameworks provide clarity and incentives (where possible) for the use of PETs. For instance, guidance could clarify that data processed within a TEE or sufficiently anonymised using techniques like differential privacy may benefit from a presumption of compliance for certain low-risk purposes.

- To the extent that the ICO is referring to centralised management of cookie consent e.g.: via a browser, IAB UK set out its position on this matter as part of our response to the proposals that were in the Data Protection and Digital Information Bill in the last Parliament[2]. Our members' view on this has not changed.

[2] https://www.iabuk.com/news-article/what-do-data-protection-changes-mean-digital-advertising