ICO report for DSIT: Advice on a viable approach to creating online advertising exception(s) to regulation 6 PECR

1. Summary

The Privacy and Electronic Communications Regulations 2003 (PECR) regulation 6 rules cover the use of storage and access technologies (hereafter 'regulation 6'). We committed to reviewing where these rules were preventing more privacy-preserving developments in online advertising models.[1] To support our commitments to government on economic growth and to deliver our online tracking strategy,[2] we carried out a standalone project. This involved extensive research, engagement and analysis to explore what capabilities were necessary for viable online advertising models.

1.1 Purpose of this report

This report lays out our project findings, including our preferred approach. It is for government to decide if and how the law should change. We recognise that this is a challenging area to get right, requiring detailed assessment of the available options.

In developing this report, we considered a range of approaches that could support opportunities for innovation and economic growth in the UK's online advertising industry, while safeguarding people's rights and freedoms.

We've explained our preferred approach and the alternatives we considered fully in section 5. This report also explains:

[1] Package of measures unveiled to drive economic growth | ICO
[2] Online tracking strategy | ICO

- what purposes may not need consent;
- what storage and access is necessary for those purposes; and
- what safeguards should exist for people's rights and freedoms.

1.2 Preferred approach

If the preferred approach we set out here became law, it would allow some online advertising to be shown to users who have not granted regulation 6 consent, while retaining appropriate safeguards. Providers of online services that wish to display advertising to users of their services ("publishers") could store and access some information on a user's device for specific purposes, based on certain criteria. It would open up opportunities for adtech intermediaries to develop new services that could assist service providers with new ways to deliver online advertising.

Today, online advertising is usually enabled by sharing identifiable and potentially sensitive information with large numbers of third parties in the programmatic supply chain. To minimise risks to users, the approach would require the first-party "publisher" site (the online service the user is visiting) to facilitate most of the functionality. Third-party involvement would still be permitted. However, access to identifiable information would be limited to specific cases within certain criteria, to deliver specific functions and provide independent verification.

This isn't because we consider that first-party information is inherently lower-risk than third-party information. Rather, the approach looks to reduce the risk of information being shared amongst large numbers of third parties. It also recognises the finding from our user research that people often feel more comfortable about their information being shared with the online service they are interacting with than with other third parties (see section 2.2).

Industry participants could use the programmatic system under this approach, with restrictions. Third-party access to identifiable information would be permitted only where the online service provider engages that third party to carry out processing activities to assist them in achieving this purpose. This could include measurement and billing related to the advertising material being displayed to the user (eg counting of aggregated impressions, clicks or views).[3]

[3] See for example the similar provision on third-party involvement in the statistical purposes exception.

To minimise risks, any new legislation would need to specify that information stored or accessed is limited to specific purposes (and only the information necessary to achieve those purposes). For example, for targeting ads, our preferred approach would permit the following information to be stored and accessed from a user's device:

- high level device and platform information (device, OS and browser, but not browser version);
- geolocation information to the city or region level;
- temporal information (date and time of day); and
- contextual information – content the user is viewing, mapped to a broad taxonomy.

1.3 Alternative approaches

We considered an alternative approach that would more closely align with how the programmatic ecosystem currently works. We recognised that this would be faster for industry participants to implement with less need for innovation.

This would permit more personal data sharing with third parties under the legitimate interests lawful basis. But the information shared would be restricted to what is required to deliver specific online advertising purposes. For example, it would include widely sharing the user's IP address and device information (eg for ad fraud prevention and detection purposes).

This is not our preferred approach because, aside from PECR, we don't think it is compatible with data protection law for the reasons listed below.

- We think this misaligns with user expectations and carries greater risks of harm to users.
- We think the risks of information being shared with and potentially misused by large numbers of third parties in the ecosystem mean that organisations would be unlikely to pass the legitimate interests three-part test or comply with the purpose limitation principle.
- It would be challenging for us at the ICO to enforce. For example, it would be difficult to enforce purpose limitation where data points permitted for one purpose (eg ad fraud prevention and detection) may be misused by any party receiving that information for non-permitted purposes (eg targeting).

We also considered minimalist options that would require a more radical shift for publishers and advertisers. They would need to make significant changes to their current processes and use of technologies. We rejected these because we did not think they sufficiently offered the capabilities required by industry, according to what we heard during our engagement. A more restrictive approach could disproportionately impact small and medium-sized publishers and limit the potential for innovation and growth.

1.4 Behavioural advertising

In our view, both storage and access of information and subsequent processing for behavioural advertising should continue to require consent under regulation 6. Even if a future exception(s) permitted storage and access for behavioural advertising to take place without consent under PECR, those processing activities involving personal data are likely to require consent under the UK GDPR anyway.

This is because the nature, scope, context and purposes of this processing and the risks it poses to people's rights and freedoms mean that consent is the only appropriate way to carry it out lawfully and fairly.[4,5]

Our preferred approach, if it became law, wouldn't revolutionise the online advertising ecosystem. However, it could provide a way for service providers to deliver online advertising to users who do not consent to behavioural advertising.

2. Context

2.1 Regulatory context

Online advertising is enabled by using storage and access technologies, such as cookies, scripts, tags and web storage. Regulation 6 prohibits storing and accessing information on people's devices (unless an exception applies). This is the case whether or not the information is

[4] ICO. (2019.) Update report into adtech and real-time bidding, pages 17-19. Available at: Update report into adtech and real time bidding
[5] ICO. (2021.) Commissioner's Opinion on data protection and privacy expectations for online advertising proposals, pages 16-19 and 43-46. Available at: Data protection and privacy expectations for online advertising proposals

personal data. There are six exceptions to this prohibition,[6] but none of them enables the use of storage and access technologies for online advertising purposes without consent. This applies irrespective of the type of advertising, the techniques used, and the level of risks and harms to people's rights and freedoms.

This means regulation 6 applies to all uses of storage and access technologies, even where the processing involved or the type of advertising is relatively basic.

The rules-based approach in regulation 6 means there is limited flexibility in the legislation to explore more privacy-friendly models. This is because the need to obtain consent from the subscriber or user applies in all cases.

We have historically seen compliance issues within consent-based behavioural advertising. We have spent several years assessing these, starting with our 2019 update report on real-time bidding (RTB),[7] and most recently through our online tracking strategy.[8]

Although some industry participants have improved their practices, many of the issues associated with RTB that we identified in 2019 still exist today. These include the following issues:

- Invalid consent: due to design choices and a lack of clear and comprehensive information.
- Collecting special category data: unlawful processing of special category data due to the lack of explicit consent.
- Insufficient transparency: privacy information is complex but doesn't provide transparency about the processing.
- Complex supply chains: unclear who will process personal information, for what purpose and how this complies with data protection requirements.
- Data minimisation issues: no assessment of what information is needed to achieve the purpose due to a perception that all information is required or otherwise useful.

[6] Including obtaining consent. For the other five exceptions, see the "What are the exceptions? | ICO" chapter of our guidance on the use of storage and access technologies.
[7] ICO. (2019.) Update report into adtech and real-time bidding. Available at: Update report into adtech and real time bidding
[8] Online tracking strategy | ICO

- Data retention issues: inconsistent retention periods across industry participants. Unclear rationale for retention periods that do exist.

We have seen innovation in online advertising approaches in recent years to address some of these problems, including a reduced reliance on third-party cookies (TPCs) and developments in the use of privacy-enhancing technologies (PETs) to serve key advertising capabilities.[9] However, users are often still at risk of their personal information being misused even if the display of advertising doesn't involve intrusive tracking and profiling (eg contextual ads). This is because in practice, contextual ads run alongside behavioural ads on services, and personal data is still gathered via the programmatic system to serve both. This means that the same challenges and risks of harm apply, even where ads are targeted differently.

The online advertising industry generally considers that behavioural advertising is more profitable than alternative types of targeting, such as contextual advertising.[10] Because PECR doesn't distinguish between types of advertising with different levels of risk, industry practices don't either. This leaves limited incentives to invest and further develop more privacy-preserving advertising practices, because the same consent requirement must be met for all online advertising.

Changes to the law are a matter for government. We have carried out this review and collated this advice in our capacity as an independent regulator and advisor to government, drawing on our experience of overseeing the existing legislative framework. We will continue to oversee the existing PECR framework and regulate in accordance with it.

2.2 User perspectives

We know that users understand the value of online advertising and sometimes want to receive more personalised services based on information they have chosen to share.[11] However, our 2024 survey found that more than half (56%) of adults would prefer to give

[9] For example, a browser API for ad measurement is progressing through the W3C that uses techniques including multi-party computation and differential privacy to improve privacy outcomes compared to current attribution practices. See: Attribution Level 1
[10] There is some evidence to support this, as described by the European Commission in their 2021 report: Online advertising: the impact of targeted advertising on advertisers, market access and consumer choice (page 19). Available at: Online advertising: the impact of targeted advertising on advertisers, market access and consumer choice
[11] ICO, 2026. Citizens' Juries on New Routes to Viable Online Advertising. Available at: https://ico.org.uk/media2/outapyon/citizens-jury-final-report.pdf

organisations less information about themselves and receive less relevant advertising.[12]

We commissioned citizen juries in England, Scotland and Wales to understand people's expectations of online advertising and consent to inform this work.[13] We gained specific insights into the public's attitude to the use of information for online advertising without consent.

This research included the following key insights:

- People placed importance on the relationship they had with particular service providers. Where they had trust and confidence in a particular service provider, they felt more comfortable with the provider using personal data about their interactions with the service to display advertising to them, including some degree of personalisation. Having this take place solely within a so-called 'first-party boundary' was more aligned with their expectations. In contrast, people firmly viewed the use of their personal data outside this boundary as something they wouldn't reasonably expect and should only happen with their consent.
- Participants felt that their consent should be required for any behavioural advertising. In particular, targeting ads using information about their behaviour, activity, location or movements (potentially across different online services or devices). This includes where data sharing with third parties, large-scale tracking and profiling (or both) take place.
- They were also less comfortable when the information became more granular about their location. They felt that their consent should always be required for this in cases where online advertising starts to relate to the town or full postcode they are in.
- Participants were comfortable with their information being collected to measure the effectiveness of advertising taking place without consent, provided it was only about the particular service they were interacting with, the information was aggregated (ie non-identifiable) and it was only held for a limited period.

Our most recent Data lives research found that participants considered targeted advertising as a fact of life. This aligns with our citizen juries, where people perceived online advertising as increasingly prevalent. The

[12] ICO, 2024. Cookies and online privacy omnibus. Available at: cookies-omnibus-summary-of-findings.pdf
[13] ICO, 2026. Citizens' Juries on New Routes to Viable Online Advertising. Available at: https://ico.org.uk/media2/outapyon/citizens-jury-final-report.pdf

Data lives research also found that people struggled to grasp how advertising reached them. They didn't necessarily know whether ads were targeted to them on the basis of their personal data or not. They considered it may be abusive in situations where organisations:

- collect (or seem to collect) information in ways that the user could not reasonably expect;
- use (or seem to use) customer information to serve content that is offensive, misleading or coercive; or
- premise (or seem to premise) targeted advertising on aspects of the user's profile that indicate they are most at risk of harm or more open to influence.[14]

Our new consent or pay research explored people's attitudes towards the use of their information, and their understanding of how their information is used in the delivery of online advertising.[15] It found many people have a limited understanding of how their information is shared online and what the choices they make mean in practice. It also made the following additional findings:

- People felt negatively towards consent or pay models, with 57% reporting a negative emotion in response to being presented with a consent or pay choice. However, participants also displayed a nuanced understanding that online advertising funds the services that are often free of charge at the point of use. 76% of respondents agreed with the statement that websites "have to make money somehow – through adverts or subscriptions".
- People often did not have a clear understanding of how their personal data was used online and when or how it may be shared with third parties. Around 20% reported not knowing what the 'consent or pay' options meant for their data processing. Less than half of those who granted consent in the online simulation understood that this choice meant their personal data could be shared with third parties.

Later sections of this report go into more detail about how the findings from our citizen juries and other research have informed our options assessment.

[14] ICO Data Lives Year 3, pages 35 – 36.
[15] ICO research on consent or pay (forthcoming).

2.3 Legal context

The UK GDPR applies where using storage and access technologies for online advertising purposes involves processing personal data. In our view, delivering even a basic online ad will almost certainly process some personal data.[16] When drafting any new exceptions to regulation 6, government must take into account that organisations will be required to comply with the UK GDPR where they process personal data. Government will also need to take account of any competition law considerations, including requirements under the Digital Markets, Competition and Consumers Act 2024.

We have identified six primary UK GDPR considerations, which have been central to our analysis. Many of these considerations build on our previous work in this space.[17] We have also considered our ability to regulate the industry under different approaches.

2.3.1 Lawfulness, fairness and transparency

The interplay between regulation 6 and the UK GDPR means that where stored or accessed information involves personal data, an organisation must first determine what they must do to comply with PECR and then what they must do to comply with the UK GDPR.

For example, if a new exception meant that certain types of online advertising processing activities can take place without the subscriber or user's prior consent, the personal data processing must still comply with the data protection principles.

This includes ensuring that the processing is lawful, fair and transparent. Removing the consent requirement 'opens up' the full range of lawful bases in article 6 UK GDPR.

[16] This is because various parties will access information associated with the HTTP request when an ad is delivered, including device information, IP Address, OS and the user agent string. This information is in practice 'freely available' as it's required for networking and communications protocols, while also used for online advertising purposes, including tracking and targeting. The information can't easily be blocked and can single out a person or be processed for wider purposes.

[17] Including the 2019 update report into adtech and real-time bidding. Available at: Update report into adtech and real time bidding and the 2021 Commissioner's Opinion on data protection and privacy expectations for online advertising proposals. Available at: Data protection and privacy expectations for online advertising proposals

In most cases, organisations are likely to choose legitimate interests as their lawful basis. They could also continue to use consent. (Legitimate interests is described further in section 2.3.2.)

For processing to be fair, organisations should use personal data only in ways that people reasonably expect, and not in ways that have unjustified adverse impacts on them. It is likely to be very challenging for organisations to demonstrate that extensive and intrusive profiling is 'fair' within the context of the intended purpose, or is indeed necessary for that purpose. This is particularly the case as people don't expect organisations to use their information in this context.[18,19]

For processing to be transparent, organisations must tell people about what will happen to their information. Transparency and fairness are fundamentally linked. In a consent-based scenario, transparency forms part of the informed nature of consent – the requirement to provide "clear and comprehensive information" about the storage or access that will take place.

In a scenario where organisations don't need to collect upfront consent, these transparency obligations still apply. Otherwise, people won't know how or why organisations are using their personal data.

Any online advertising-related exception(s) should include a requirement that the service provider gives the user "clear and comprehensive information" about the storage or access. This is similar to the construction of other exceptions in regulations 6. Unlike approaches industry has used to implement the opt-in consent requirement, this would not specifically require an informational banner at the point a user visits an online service (unless the service still needs to request consent for other purposes). It would still need to be prominent enough to be sufficiently informative, giving the details required under the right to be informed.

2.3.2 Legitimate interests: the three-part test

Where organisations are able to rely on an exception from the regulation 6 requirements, it is likely that they would then seek to rely on the

[18] As discussed in section 2.2, our Data Lives research found that participants didn't always know how ads were targeted towards them.
[19] We have previously explored this in the 2019 update report into adtech and real-time bidding. Available at: Update report into adtech and real time bidding

legitimate interests lawful basis in article 6(1)(f) of the UK GDPR for any personal data processing.

This requires them to carry out the three-part test, which covers:

- the purpose test – whether there is a legitimate purpose;
- the necessity test - whether the processing is necessary to achieve that purpose; and
- the balancing test – the organisation balances the people's rights, freedoms and interests with those of its own or those of other parties.

A key part of our decision on a possible new approach was whether organisations are likely to be able to satisfy the three-part test.

Firstly, generating income from online advertising is in principle a legitimate purpose, so the purpose test is likely to be met in most circumstances.

It remains challenging for service providers to demonstrate that the processing is necessary to achieve that purpose, and so the necessity test may not always be met. In our legitimate interests guidance,[20] we say that organisations should consider:

- whether the processing actually helps to further that interest;
- whether it is a reasonable way to go about it; and
- if there is another less intrusive way to achieve the same result.

Finally, the balancing test is equally important to consider. Our guidance notes that (assuming consent is not required under PECR) organisations can rely on legitimate interests for marketing activities where they can show that how they use people's information:

- is proportionate;
- has a minimal privacy impact; and
- would not surprise people or make them likely to object.[21]

For this reason, online advertising based on highly personalised or large-scale tracking and profiling is unlikely to satisfy the balancing test. From our research, we know that users consistently expressed concern about this type of processing being undertaken without their knowledge or consent. During our analysis, we considered less clear-cut distinctions on

[20] Legitimate interests | ICO
[21] Legitimate interests | ICO

a case-by-case basis. For example, sharing the full URL to all participants in a programmatic supply chain for brand safety purposes, and the risk of this being misused for targeting or profiling.

2.3.3 Special category data

Special category data is personal data that needs more protection because it is sensitive. It includes personal data revealing racial or ethnic origin, political opinions and data about health, amongst other information. Using any special category data in online advertising requires explicit consent under article 9.[22] As noted in our 2019 report, no other condition is available and none of the other public interest conditions within the DPA 2018 apply.[23]

We acknowledge industry efforts to minimise the likelihood of organisations processing special category data,[24] or ensuring that organisations obtain explicit consent. Our preferred approach excludes special category data, seeking to guard against any processing (direct or by inferred) for targeting and profiling purposes.

We recommend that any exception(s) is drafted in such a way that processing special category data (direct or by inferred) takes the storage and access outside the new exception(s). This means that consent (and explicit consent) would be required.

2.3.4 Qualified right to object

Where legitimate interests is the lawful basis, article 21(1) of the UK GDPR gives people a qualified right to object.[25]

Where a person exercises this right, the organisation must stop processing their personal data – unless the organisation can demonstrate compelling legitimate grounds that override the person's interests, rights and freedoms.

---

[22] Special category data | ICO
[23] ICO (2019). Update report into adtech and real-time bidding. Section 3.2, page 16. Available at: https://ico.org.uk/media2/migrated/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf
[24] See for example IAB UK (2020), Digital advertising guidance: special category data under the GDPR. Available at: https://www.iabuk.com/sites/default/files/public_files/Special-Category-Data-Guidance.pdf
[25]The qualified right to object also applies when the processing is based on either the public task or recognised legitimate interest lawful bases.

As organisations must help people exercise their rights, they must have a mechanism in place to:

- recognise objection requests; and
- assess whether they can demonstrate compelling grounds.

The more intrusive the processing activity is, the less likely it is that the controller will be able to demonstrate that their compelling grounds are sufficient to override people's rights, freedoms and interests.

2.3.5 Direct marketing

People have an absolute right to object to direct marketing under article 21(2) of the UK GDPR, including to profiling for direct marketing purposes. Therefore, people have an absolute right to object when processing for online advertising purposes that is exempt from PECR consent requirements counts as direct marketing.

In circumstances where organisations deliver online advertising without consent that is deemed to be outside the scope of direct marketing, the absolute right to object would not apply. However, the qualified right to object would still apply (as explained in section 2.3.4).

2.3.6 Children

Processing children's information on the basis of legitimate interests for online advertising purposes is likely to be difficult, and only likely to be possible where the processing is very unintrusive and low risk. It would need a more finely balanced assessment than for adults, taking into account the children's developmental stages and the level of awareness about the risks associated with personal data processing.

The age of the child will also impact the assessment. For example, many organisations set age limits for use of their site within their terms and conditions. For many sites, this is set at 13 years of age. Where an organisation states such age limits, the processing of under 13's information under legitimate interests is unlikely to be lawful.
The organisations have no interest in processing the information of under 13's because they explicitly state in their terms that they don't want these children on their site. As this processing goes against their own terms and conditions, it would be hard for them to argue that legitimate interests could apply.

PECR doesn't have specific provisions for children. However, the UK GDPR applies where children's personal data is processed. As our guidance on the use of storage and access technologies explains,[26] if an online service is likely to be accessed by a child, the organisation should comply with the Children's code.[27] We recognise that many industry participants are aware of the additional considerations for serving online ads to children, and that some actors have already developed solutions which aim to meet these requirements.

2.4 Industry context

Digital advertising is estimated to contribute £129bn in gross value added (GVA) each year to the UK economy.[28] It enables businesses to reach new customers and markets and helps fund the digital economy. We know that some people value personalised advertising, while others accept that ads can enable them to access online services free of charge.

Our online tracking strategy has focused on giving people control over how organisations use their information online. As a result of our work, 99% of the UK's top 1000 websites now give people an equal choice to 'accept' or 'reject' the use of storage and access technologies for online advertising purposes.[29]

An increased proportion of people are choosing to withhold their consent (ie by selecting 'reject all' or similar).[30] When people choose to reject, service providers can face challenges in monetising that traffic in compliance with the law. This also has implications for brands and advertisers who want relevant audiences to see their ads, and intermediaries providing services to facilitate online advertising.

Service providers are continuing to explore other ways to generate revenue. One example is the emergence of 'consent or pay' models.[31] But these aren't viable for every service provider, and people have negative views towards these models (as described in section 2.2).[32]

---

[26] What are the PECR rules? | ICO
[27] The Children's Code: what is it? | ICO
[28] https://www.iabuk.com/digitaldividend
[29] Online tracking strategy update – April 2026 | ICO
[30] The ICO's 2024 cookies omnibus survey indicated that 21% of people choose to "reject" cookies: cookies-omnibus-summary-of-findings.pdf. Anecdotally, some news media publishers have told us their opt-out rates are higher than this.
[31] We have produced guidance on how organisations can use 'consent or pay' models: Consent or pay | ICO
[32] ICO Data Lives Year 3, pages 37 – 40, ICO research on consent or pay (forthcoming).

Outside our activity, we are aware of several other significant factors which are challenging publishers, or more broadly impacting industry decisions on spending budgets and investment. The following are the most notable factors:

- The decreasing availability of TPCs, commonly used for cross-site tracking, targeting and attribution, has forced industry to change their practices. This has been driven by moves from browsers including Safari and Firefox to block them by default[33,34] combined with increasing numbers of users choosing to reject the use of TPCs. The low availability of TPCs means match rates (how often adtech companies can recognise the same user across sites or platforms using TPCs) continue to decline. This is leading to an increasing reliance on IDs such as email addresses or other first-party information available to the publisher to help adtech companies identify users.[35] There has also been a growth in adopting probabilistic identifiers based on other indicators (eg device fingerprinting techniques).[36]
- The evolution of large language models and agentic AI is changing the way users interact with online services, leading to decreasing search traffic and associated page views for publishers.[37]
- The changing formats for advertising. For example, video advertising is rising (eg for connected TV applications),[38] as are voice-activated ads (where users interact with ads verbally, such as through their smart speaker).[39]
- The availability of ad blockers and script removal makes some audiences invisible to publishers. Estimates of ad blocker usage vary, but a recent study carried out by GWI estimated that 21% of adults use ad-blocking software.[40]

[33] Mozilla heralds death of TPC (2023): Saying goodbye to third-party cookies in 2024
[34] Google decided to maintain TPCs in Chrome, see: Next steps for Privacy Sandbox and tracking protections in Chrome
[35] For example, see: As Cookieless Audiences Grow, Here's Why Alternative IDs Matter Heading Into 2025 – Advertising Week
[36] Device fingerprinting, such as browser fingerprinting techniques, involves collecting pieces of information about a device's software or hardware. These can be combined to uniquely identify a particular device.
[37] For example, see: Exclusive: Google's AI Overviews hit by EU antitrust complaint from independent publishers | Reuters
[38] IAB UK Digital Adspend 2025 shows video growth is outpacing the market. Available at: Digital Adspend 2025: UK's digital ad market reaches £40.5bn | IAB UK
[39] For example, see: The growing potential of emerging media platforms: how effective are digital audio ads
[40] Ad-blocking: Consumer Behaviors and Motivations Behind the Trend - GWI

- The imbalance between small to medium-sized publishers and large platforms (eg walled gardens and ecommerce sites) who hold significant amounts of first-party information and are able to more easily adapt to changing requirements or make use of new opportunities.

Regulation 6 requirements are only one component of this complex landscape. This makes it difficult to predict the likely adoption of a new approach to online advertising if the rules change. We have conducted extensive industry engagement as part of this work, including a public call for views, a technical workshop and one-to-one meetings. This has assured us that industry participants could make use of a consent-less approach to online advertising, if it were to become law.

3. Project requirements

We have developed our advice in accordance with our policy methodology.[41] The methodology draws closely from best practice principles and aligns with government guidance, including the HM Treasury Green Book.[42] The process has included:

- understanding the project rationale and objectives;
- carrying out research and analysis;
- running a public call for views; and
- developing and appraising a series of policy options.

As part of this process, we defined several underpinning requirements which set limits on the viability of different options.[43] These are that options must include the following requirements:

1. **Retain safeguards while removing impediments**

   Our primary duties are to secure an adequate level of protection for personal information and to promote public trust and confidence in its processing. In carrying out our functions, we must also consider

[41] The ICO's policy methodology
[42] The Green Book and accompanying guidance - GOV.UK
[43] These requirements are 'constraints' in accordance with the HMT Green Book (paragraph 5.6): Constraints are external considerations that set limits on the viability of different options. Examples of constraints might include legal requirements, ethical standards, social acceptability and timing. See The Green Book and accompanying guidance - GOV.UK.

the desirability of promoting economic growth, and the fact that children's personal data merits specific protection.[44]

Any solution will therefore need to remove any unnecessary impediments to innovation and support economic growth whilst safeguarding people's rights, compared to the current information rights legislation.

This means it must deliver on our duty to support innovation, competition and economic growth beyond what is possible within the current legislation. However, we can't go so far with this that it risks people's information rights. This is closely linked to requirement 2.

2. Align with the legal framework

Regardless of any changes made to regulation 6, the UK GDPR applies where the use of storage and access technologies for online advertising purposes involves processing personal data. Therefore, options must align with and work alongside the rest of the data protection legal framework.

Section 2.3 covers the legal considerations which were central in our assessment of potential solutions that would work within the rest of the data protection framework.

We also considered alignment of possible solutions with other parts of PECR, including the rules about electronic mail marketing in regulation 22.

Where requirement 2 is met, we will have confidence that we are safeguarding individual rights as necessitated by requirement 1.

3. Maintain consent where it is needed

Any approach should not undermine our existing policy and guidance on where consent is required under the UK GDPR. We've provided significant interpretive guidance about the nature and role of consent in the data protection framework.[45] We've also seen the

[44] This is because children may be less aware of the risks and consequences associated with processing of personal data and of their rights in relation to such processing.
[45] Consent | ICO

development of domestic case law underlining that consent has a high bar.[46]

In exploring these options, we sought to ensure that any proposed solution maintains consistency with this case law that binds us alongside existing policy and guidance on consent. For example, our guidance that outlines when consent is important and what constitutes valid consent will still apply. Organisations should be able to apply updated PECR rules and existing guidance together.

4. **Be feasible, usable and effective**

   Our approach should be possible to implement in the immediate and longer term with a tolerable level of risk. We did not rule out solutions that require some innovation for medium-term implementation, as this could be positive for industry, the economy and users.

4. Evidence base

In preparing this advice, we built the following evidence base:

- **Qualitative user research** – We commissioned citizen juries in England, Scotland and Wales to understand people's expectations on online advertising and consent. These provided clear boundaries from users specific to the context we are looking at, as described in section 2.2. We've used these to inform our work. The research is available on our website.[47]
- **Public call for views** – We invited views on our approach to regulating consent requirements, and specific considerations for capabilities required to deliver online advertising. We received 76 submissions from industry participants and representative groups, public sector organisations and academics, indicating a wide-ranging interest in this work. The summary of our call for views is available on our website.[48]
- **In-depth engagement** – We ran a technical workshop with industry participants (including DSIT representatives) in July 2025

[46] See, for example, Leave.EU v Information Commissioner [2021] UKUT 26 (AAC) and the assimilated case law it references.
[47] ICO, 2026. Citizens' Juries on New Routes to Viable Online Advertising. Available at: https://ico.org.uk/media2/outapyon/citizens-jury-final-report.pdf
[48] ICO, 2026. ICO advice to government on online advertising exception(s) to regulation 6 consent requirements – Summary of responses to call for views. Available at: https://ico.org.uk/media2/e3qanbyx/20260505-summary-of-call-for-views.pdf

to understand their specific requirements and identify nuances in different approaches. We also participated in stakeholder meetings, including several roundtable events with industry bodies, associations and other stakeholder groups to consider their perspectives.

- **Engagement with other regulators** - We have discussed our preferred approach with other regulators and bodies. None of these bodies raised concerns with us about impacts on their remits. We liaised with the following regulators:
    - The CMA - as part of our duty to consider the desirability of promoting competition, under section 120B of the DPA 2018.
    - Ofcom - to discuss where there may be specific considerations for public service broadcasters delivering online advertising.
    - The ASA - to understand requirements of the UK Code of Non-broadcast Advertising and Direct and Promotional Marketing (CAP Code) for advertisers.[49]

5. Preferred approach

If government decides to amend the regulation 6 requirements, we propose permitting some online advertising purposes without consent within a 'first-party framework'. This would allow the online service or the 'publisher' (the first party that the user is directly engaging with) serving online advertising to store and access information on the user's device for specific purposes. Under this approach, third-party data sharing would be only permitted for controlled use cases and restricted compared to typical data sharing in programmatic advertising.

For information processed by both the online service and supporting third parties, safeguards (including the use of PETs) would be required to reduce the risks of identifiability and tracking.

The purposes that we propose could be permitted without consent in certain circumstances would be:

- ad delivery;
- targeting;
- measurement and billing;
- attribution;
- frequency capping;

[49] Advertising codes - ASA | CAP

- brand safety; and
- ad fraud prevention and detection.

We suggest that an exception(s) to the regulation 6 consent requirements for storage and access to information on the user's device, and subsequent processing, should permit these purposes as far as possible. This should be within the boundaries of the rest of the data protection framework and user expectations.

Our preferred approach allows the greatest functionality and certainty within the requirements outlined in section 3. Section 5.2 provides more details on what our preferred approach involves, and some of the alternatives we considered.

5.1 Alternative options considered

We considered alternative approaches that would more closely align with how the programmatic ecosystem currently works, recognising that this would be faster for industry participants to implement with less need for innovation. Specifically, we explored aligning more closely with existing RTB data sharing practices. This would allow specific information to be shared with third parties to fulfil their key purposes.

At a high level, an alternative approach would permit more data sharing with third parties under the legitimate interests lawful basis (assuming a legitimate interests assessment could be passed). But the information shared would be restricted to what is required to deliver online advertising. For example, it would include widely sharing the user's IP address and device information (eg for ad fraud prevention and detection purposes).

This is not our preferred approach because, aside from PECR, we don't think it is compatible with data protection law. This is because:

- we think it misaligns with user expectations and carries greater risks of harm to users;
- there are risks of personal data being shared with and potentially misused by large numbers of third parties in the ecosystem. This means that organisations would be unlikely to pass the legitimate interests three-part test or comply with the purpose limitation principle. In particular, this would be difficult for the service provider, which is responsible for the initial collection and processing of users' personal data; and

- it poses challenges to our ability at the ICO to regulate the industry. For example, it would be difficult to enforce purpose limitation where data points permitted for one purpose (eg ad fraud prevention and detection) may be misused by any party receiving that information for non-permitted purposes (eg targeting).

We acknowledge that this high-level alternative approach, if it became law, may be preferable to some parts of the industry. This is because it would more closely align with how the programmatic ecosystem currently works and require fewer upfront changes for them to make use of. The 'first party approach' will allow more capability to the publisher and advertiser, while still upholding people's rights and freedoms. This is because the online service can make use of more information than would be possible if it were all shared with numerous third parties, where the risks would be higher.

We also considered minimalist options that would require a more radical shift for publishers and advertisers, who would need to make significant changes to their current processes and use of technologies. These are explained in section 5.2. We rejected these because we did not think they sufficiently offered the capabilities required by industry, based on what we heard during our engagement. A more restrictive approach could disproportionately impact small and medium-sized publishers and limit potential for innovation and growth.

5.2. Preferred approach by capability

Each sub-section below provides an outline of our preferred approach for each of the purposes that could be permitted without consent within the project requirements. We also explain where we have drawn a boundary and why.

For brevity and clarity, each advertising capability outlined below is described in a web context. However, the principles about storage and access to information and purposes of processing would apply whenever information is stored and accessed on a user's device, including on mobile apps and IoT devices.

5.2.1 Ad delivery

Ad delivery is the process of delivering ads to users on a webpage. The process starts after the auction is completed (and typically, the highest value ad is chosen). The publisher ad server makes a final decision on the

ad to show and returns the corresponding ad tag back to the user's browser.

Storage and access technologies are needed to technically deliver ads, including sending and responding to ad requests and delivering ad files. Information emitted in the HTTP request for ad delivery when an ad is delivered is likely to involve processing personal data, including device information, OS and the user agent string. This information may be shared and used for other purposes, including targeting.

Currently, if a user chooses to 'reject' the use of storage and access technologies for online advertising purposes, it is unlikely that a service provider will be able to deliver any online advertising. Therefore, including an exception to regulation 6 consent requirements for ad delivery purposes will be central. This would be acceptable if the information used and processes undertaken are limited to only what is required for this purpose.

In line with our user expectations and legal requirements, we suggest that scalable and viable ad delivery could be permitted without consent, when limited to the following processes:

- The use of tools like Google Publisher Tag and Prebid (a client-side auction product), to help define the ad space on a web page and coordinate bids received from advertisers. Prebid and other JavaScript required for bid construction will run and call libraries containing the core wrapper code and involve storing and accessing information on the browser to achieve this.
- The publisher using an ad server (most typically, Google Ad Manager) to coordinate and decide on the 'winning' ad. This requires code that stores and accesses information on the user's device to communicate with the ad server and orchestrate the definition and delivery of ads onto the web page.
- The ad tag requesting the advertiser's ad server – this involves accessing and sharing details like the user's device and the page they're on.
- The advertiser ad server may return additional code that involves storing and accessing information on the user's device to facilitate the final creative delivery from the content delivery network, and for limited ad verification purposes.

The necessary processes described above could be permitted without consent in accordance with user expectations and our legal requirements.

In general, people accept ads on their service, and this purpose could meet the legitimate interests' three-part test.

This is based on the condition that information used and shared is limited to what is necessary for ad delivery, and is only used for those purposes. Information shared with the publisher ad server and third-party advertiser ad server can only be used to assist the publisher.

We considered a more limiting approach that would restrict the use of a third-party ad server and require publishers to self-host ad creatives. However, we don't think this is feasible, as it would not be accessible to all publishers.

5.2.2 Frequency capping

Frequency capping is a way to limit the number of times an ad is shown to a particular user within a specified timeframe. It generally involves storage and access technologies that identify the user (such as cookies or mobile IDs) which store how many times a user has been shown a particular ad. This is compared to the specified cap. If the stored amount is below the cap, the ad can be shown to that user again.

Frequency capping can also be carried out at different points within the overall online advertising process (eg by service providers themselves, or at the ad server level).

The online advertising industry values frequency capping to prevent excessive repetition of ads, which can worsen user experience, harm brand reputation, and waste budgets. This is because money is spent on ads that are unlikely to lead to sales. However, it often carries the risk that identifiable information will be misused to track and profile users.

In line with user expectations and our legal requirements, we suggest that frequency capping within the context of the user's interaction with the service provider (ie the first party) could be permitted without consent, provided that the information stored or accessed is:

- solely used for limiting ad exposure on that service; and
- limited only to what's necessary to achieve that purpose.

Separately, cross-site frequency capping may be permitted, only if enabled by PETs to avoid users being identified and linked across sites. We understand that these market solutions may not yet be available. However, if developed, they could add value for the industry without increasing risk to users.

More minimalist options that don't involve storage or access, such as modelling approaches, can't alone offer the capabilities that many advertisers require.

5.2.3 Ad fraud prevention and detection

Ad fraud is the deliberate manipulation of digital advertising systems. This includes generating fake clicks, impressions or traffic using bots or deceptive tactics to extract money from advertising budgets. Without the ability to detect and prevent ad fraud, advertisers lose confidence that their ads are reaching real users, publisher's credibility is affected, and ad spend is wasted as it is diverted to illegitimate sources.

Ad fraud prevention generally involves sharing identifiable information (eg the user IP address and user agent string) with large numbers of third parties in the bid request. The online advertising industry relies on ad verification partners who do extensive analysis about individual user devices and user behaviour to prevent and detect ad fraud. This does not meet users' expectations or our legal requirements because identifiable information is being collected and shared with third parties and potentially used for multiple purposes.

Instead, we suggest that ad fraud prevention and detection could be permitted at both the pre-bid and post-bid stage, providing that the following are taking place:

- The service provider (publisher), or the publisher ad server on their behalf, is using device information (eg IP address and user agent string) to conduct pre-bid filtering for invalid traffic.
- They are not sharing that information with third parties, including buyers. Instead, the service provider could reassure buyers that their user is human. They would need to do this by passing on a signal that confirms they are satisfied that the visitor is a valid user (eg by using a secure method like the Private State Token API).[50] This would allow the first party to issue a cryptographic token for the buyer to redeem that conveys trust in the user. Alternatively, the service provider could use a tool like those provided by Cloudflare.
- The service provider, or a trusted third party on their behalf, is conducting only limited post-bid analysis to verify that their visitors were human. This could include collecting statistical information for

[50] Private State Token API

basic behavioural analytics (eg information on which page users are visiting, scroll depth, exit pages) to inform analysis.

While less of a direct concern about storage or access, publishers and advertisers could also employ the use of IAB Tech lab tools (specifically ads.txt, sellers.json, buyers.txt and ads.cert) to prevent domain spoofing. This is where bad actors pretend to be legitimate publishers and sell fake ad space.

The methods to reassure buyers that site visitors are valid users will require industry participants to do things differently. The tools listed above are intended as indicative suggestions of how this could be achieved if an exception followed this approach, rather than prescriptive requirements.

A more restrictive option would be to exclude any post-bid analysis. This is due to the volume of behavioural information we understand third-party verification tools currently collect for this purpose, and because this information may be used for secondary purposes beyond ad fraud detection. However, the above proposal aligns with the types of information permitted to be stored and accessed from a device without consent under the current regulation 6 statistical purposes exception.[51] It could add additional value with a low risk to users.

5.2.4 Brand safety, suitability and compliance

Brand safety, suitability and compliance covers practices and tools to ensure that a digital ad will not appear alongside content that could damage an advertiser's reputation. It is an important function for brands to protect their identity and reputation by ensuring their ads are seen in an appropriate place. Similarly, publishers also want to control what types of ads appear on their site.

Brand safety functionality can be delivered when the service provider shares information about where an ad will be shown (such as the URL and content categories) in a bid request. Buyers can use blocklists and allowlists to restrict the delivery of ads to approved sites. Brand safety often involves third-party tools scanning pages to classify content as safe or unsafe, before an ad is chosen for a page. Advertisers can use these classifications to target or avoid specific content.

[51] See Schedule A1: The Privacy and Electronic Communications (EC Directive) Regulations 2003

There are risks associated with sharing the URL of their page or content categories openly in the bid request. When combined with other data points, this information could inform individual targeting. Similarly, third-party brand safety analysis is done using JavaScript tags on the publisher site. These tags may serve multiple purposes, which are unclear to users. For these reasons, neither approach is likely to align with user expectations or meet our legal requirements.

In line with our user expectations and legal requirements, we suggest that the following brand safety functionality could be permitted without consent:

- The first-party website (publisher), or a trusted third party on their behalf conducts page scanning for brand safety purposes.
- The publisher (or trusted third party) conveys the information about the content of their page to buyers, via an abstracted signal.

This approach would enable organisations required to meet the CAP code to do so (eg brands serving gambling or alcohol ads). In these cases, advertisers could use the signal received by the publisher to determine whether more than 25% of visitors to the publisher's site would be children. They could then exclude these sites from serving their ads where this is the case.[52] Alternatively, consent could be sought if advertisers wish to additionally target these ads towards adult visitors and away from children on a site where they are not confident about the proportion of that site's visitors who are children.

A more restrictive option would be to exclude any storage or access technologies for brand safety purposes. This could still enable ads to be delivered in contexts where there is trust and confidence between the advertiser and publisher about where an ad would be served, such as in direct deals. However, this may be limiting for some industry participants.

5.2.5 Targeting

Targeting covers the techniques that advertisers use to direct online ads to a desired audience for their product or service. Targeting helps advertisers spend their budget efficiently and is seen by the industry as central to online advertising. Common techniques include:

- device and platform targeting, based on the device or platform the user is visiting the online service with;

[52] Guidance on age-restricted ads online - ASA | CAP

- contextual targeting, based on the content of the page the user is currently viewing;
- geo targeting, to serve ads to users in particular locations;
- demographic and interest-based targeting of audiences by traits such as age, gender, income, or education, using actual or inferred information; and
- ID-based targeting, which relies on reaching the same user across multiple interactions across a site, a range of sites or devices.[53]

ID-based targeting involves identifying users and sharing their information with third parties (including demand-side platforms). This can include cross-environment identifiers (such as a TPC or mobile advertising ID - MAID) to re-identify people in an open auction environment.

Demographic and interest-based targeting can also involve identifying users. Even where it may not (eg where it involves creating audience cohorts based on specific traits), neither approach would meet user expectations or our legal requirements without consent.

In line with our user expectations and legal requirements, we suggest that using storage and access technologies for targeting could be permitted without consent, when limited to:

- device and platform information from the user's device abstracted to high-level categories (eg device, OS, browser but not browser version);
- geolocation data (derived from IP address or mobile GPS data) - abstracted to the city or region level;
- temporal information – date and time of day; and
- contextual – content the user is immediately viewing mapped to a broad taxonomy, such as 'sports' or 'cycling'.

This approach would enable the service provider (publisher) to provide non-personalised signals for inventory they are currently unable to sell into the programmatic marketplace, where consent is not granted. It would allow them to continue to use the programmatic advertising architecture. However, rather than raw information or a user ID, they could use abstracted signals (eg a deal ID) to represent the inventory in the most appealing way to buyers.

[53] Note that this is a non-exhaustive list of targeting techniques, and some industry participants may define some of these terms differently.

More minimalist options are unlikely to be accessible to all publishers, like further reducing targeting signals (eg abstracting geo targeting to the country level) and limiting targeting decisions to the publisher ad server (ie restricting to direct deals without the use of the programmatic architecture).

5.2.6 Billing and measurement

Billing is the process of calculating and charging advertisers based on agreed metrics. Measurement enables advertisers to understand the reach and impact of their advertising. It usually involves collecting user-level metrics (including impressions, views and clicks) and can capture activity across sites or domains. It often involves granular, user-level metrics being captured by TPCs in a web context, or a MAID in a mobile context.

This report aligns billing and measurement purposes. This is for consistency because both functions often rely on the same information, based on similar uses of storage and access technologies.

As with other purposes using TPCs or a MAID, there are risks of users being identified and tracked across sites by large numbers of third parties. This is misaligned with user expectations and legal requirements. It could lead to high-risk processing.

In line with our user expectations and legal requirements, we suggest that the use of storage and access technologies for billing and measurement could be permitted without consent, when limited to:

- the service provider counting impressions, clicks and views for billing and measurement purposes, and sharing this with the advertiser. This information must be aggregated, non-identifiable and only stored for as long as it is needed for these purposes;
- this information can be collected or verified by a trusted third-party on the service provider and advertiser's behalf, or both.

A more restrictive approach would be to allow reporting only of impressions. However, clicks and views are valuable to the online advertising industry, as well as impressions. This added information can still meet the expectations of users from our citizen juries, provided it is aggregated, non-identifiable and stored for a limited time period.

5.2.7 Attribution

Attribution covers techniques to understand who or what should receive credit for advertisers achieving goals (eg a sale or sign-up). This usually involves following a user's journey from initial ad exposure through to a final action. It may involve tracking users across devices and over multiple sessions, where a conversion action isn't taken immediately, or is taken on a different device. Attribution helps brands and advertisers to measure the effectiveness of their campaigns and make decisions about marketing budgets.

Attribution typically links users between sites, often using TPCs or other storage and access technologies. This does not meet user expectations. It also does not meet our legal requirements, as organisations would be unlikely to be able to rely on legitimate interests as their lawful basis for this processing.

In line with user expectations and our legal requirements, we suggest that using storage and access technologies for attribution could be permitted without consent. However, this would only apply when limited to anonymised, cross-site attribution, with technical and organisational measures to prevent cross-site tracking. For example, this could be achieved by some proposed browser-based PET-enabled attribution solutions.

This is based on the conditions that the information and personal data accessed by the publisher and advertiser is low risk, limited to only the necessary amount, and used only for these purposes. In particular, the risk of individual users being targeted following attribution must be sufficiently remote.

Some attribution use cases are traditionally highly reliant on linking cross-site events to a single user. For these use cases, recording attribution events without consent would potentially require adaptation and innovation.

A more minimalist option would be to exclude any cross-site storage and access capabilities for attribution purposes, leaving organisations to rely on modelling approaches. However, this would be restrictive, as the ability to link a conversion event to a preceding ad exposure is considered a key requirement by the online advertising industry. Further, the innovation taking place with PETs for this purpose sufficiently mitigates risks of cross-site identification. Encouraging the adoption of PET-enabled attribution can also have a wider benefit, including for consented

audiences. This is due to the decreasing availability of TPCs for attribution, explained in section 2.4.

6. Costs and benefits

Our proposed approach would offer a new way to deliver online advertising without consent. It wouldn't revolutionise the ecosystem, but it would provide a way to provide publishers with new revenue opportunities for users who they currently can't legally deliver any online advertising to, because they don't grant consent.

Industry can also continue to deliver behavioural advertising to users who have provided valid consent.

If government decides to make an exception(s) to regulation 6 that is aligned with our preferred approach, the economic growth impact of with this proposal would depend on the proportion of the online advertising industry, including publishers, advertisers and intermediaries, who adapt and innovate to make use of new an exception(s). These decisions will undoubtedly be influenced by other external factors (eg those described in section 2.4) as well as this change in the law.

Due to gaps in available evidence and the need to keep the analysis proportionate (as discussed in the cost-benefit analysis),[54] we have not been able to reliably monetise all impacts. However, our analysis of the available evidence indicates a net positive overall impact relative to the current system. In our view, the expected benefits outweigh the expected costs, particularly in the medium to longer-term.

This analysis would not apply if government introduced an exception(s) that did not align with our preferred approach.

6.1 Costs

There are a number of direct and indirect costs to our preferred approach. However, these are largely short-term costs that would enable future growth and innovation and are expected to be time-limited and concentrated among a subset of organisations that choose to make use of the proposed exception(s). In contrast, the potential benefits are broader

[54] ICO, 2026. Advice on a viable approach to creating online advertising exception(s) to regulation 6 PECR: Cost-benefit analysis. Available at: https://ico.org.uk/media2/icslg2mm/20260421-cba-for-dsit-on-changes-to-regulation-6-pecr-for-online-advertising.pdf

in scope, longer lasting, and can benefit a wider range of market players, particularly when the proposed exception supports the development and adoption of new online advertising models.

We identified the following key costs:

- one-off familiarisation costs associated with understanding and implementing any revised regulatory requirements;
- upfront system and process changes for those organisations that choose to make use of the exception(s); and
- modest ongoing increases in operational and maintenance costs due to handling increased data inventory.

These costs are expected to fall primarily on online service providers. This includes those that may have a significant audience reach but a lower market share and those characterised by infrequent visitors and high-bounce rates where consent banners are in place (described in our cost-benefit analysis as 'mid-tier' and 'base-tier' respectively).[55] Costs may also fall on a smaller number of adtech intermediaries.

Importantly, uptake of the exception(s) would not be mandatory, meaning that organisations would incur these costs only where they judge the commercial and operational case is favourable. Where costs arise, we expect they would be manageable and proportionate and largely incurred once rather than on an ongoing basis.

6.2 Benefits

We have also identified the following benefits:

- Increased ability for some organisations to monetise currently inaccessible inventory about non-consenting users for clearly defined low-risk advertising purposes.
- Improved incentives to invest in privacy-preserving technologies and alternative advertising models.
- Improved confidence and certainty for businesses operating in a complex regulatory landscape.

[55] Top-tier OSPs: key market players within search and display market segments, with significant audience reach and market share. Mid-tier OSPs: have a significant audience reach but a much lower market share than top-tier OSPs, such as affiliate and commission-based metasearch platforms, and subscription publishers. Base tier OSPs: all other OSPs, characterised by infrequent visitors and high-bounce rates where consent banners are in place.

- Downstream benefits for advertisers, intermediaries and users arising from better measurement, reduced friction, and improved trust.

We expect benefits to be:

- strongest for mid- and base-tier publishers most constrained by consent rejection; and
- neutral to modest for top-tier platforms with a large market share of extensive consented information.

In the short term, we anticipate benefits would most easily be felt by organisations using 'direct deals' to deliver online advertising. This is because adaptation would be needed to use real-time bidding while meeting the requirements of our proposed approach. In the medium term, organisations could take advantage of opportunities to innovate to make use of the proposed exception(s).

Revenue impacts are commercially sensitive and difficult to quantify. However, evidence from our stakeholder engagement suggests that even modest uplifts in monetisation for a limited proportion of mid- and base-tier providers could be material when combined. This is particularly the case when viewed against the scale of the UK digital advertising market. Given the size of the market, relatively small percentage gains in accessible user inventory or efficiency could translate into meaningful economic value, alongside wider dynamic benefits not captured in static estimates.

The evidence available to us is not sufficient to allow reliable quantification of the benefits, but we consider that the preferred approach could reduce avoidable frictions for compliant publishers while maintaining consent for higher risk behaviours (eg tracking and profiling). It would create a credible compliance route for activities that underpin delivery, measurement and assurance, making low-risk advertising models commercially viable rather than merely permissible.

We conclude that this approach would assist the government's growth agenda and deliver a positive net value, while maintaining people's rights and freedoms.

In our view, an exception(s) in the law, with further ICO guidance, can provide the certainty needed to encourage innovation for the online advertising industry.

We have published our full cost-benefit analysis alongside this report.[56]

7. Conclusion

As outlined in our letter, it is for government to decide whether it will create new exceptions to regulation 6 for online advertising, and how our advice will inform those decisions.

In the meantime, our work in this area is ongoing as we've outlined in our online tracking strategy update.[57]

We are available to discuss this further and to provide advice on any draft regulations, as part of the statutory consultation process required under regulation 6A(3) of PECR.

Following any changes to regulation 6, we would update our guidance on using storage and access technologies to clarify how organisations could make use of a new exception(s). We would also explore how we can support innovation in this space through our Regulatory Sandbox and Innovation Advice services. Finally, we would supervise the industry's use of any exception(s) and take action where we observe harmful practices.

May 2026

[56] ICO, 2026. Advice on a viable approach to creating online advertising exception(s) to regulation 6 PECR: Cost-benefit analysis. Available at: https://ico.org.uk/media2/icslg2mm/20260421-cba-for-dsit-on-changes-to-regulation-6-pecr-for-online-advertising.pdf

[57] Online tracking strategy update – April 2026 | ICO