Information Commissioner's Opinion:

Data protection and privacy expectations for online advertising proposals

25 November 2021

Information Commissioner's Office

Contents

1. Executive summary

Online advertising enables advertisers to reach individuals with their products and brands, while helping organisations to generate income to fund their online services. It supports a large ecosystem of advertising technology (adtech) providers, publishers, and advertisers. It also generates a significant proportion of the revenues of major technology companies.

The concept is simple: advertisers want to show adverts to individuals who are likely to buy their product, and individuals want to see adverts that are relevant to them. Behind it stands a complex web of data processing involving the profiling, tracking, auctioning, and sharing of personal data. The reliance on personal data means data protection law has an important role to play in building trust and confidence, and in protecting the public from personal data misuse.

Technologies used in online advertising, and the way they are deployed, have the potential to be highly privacy intrusive. The Commissioner's 2019 update report into adtech and real-time bidding sets out the concerns about the adtech ecosystem. In particular, it covers the significant role cookies and similar technologies play in enabling the gathering and processing of personal data to target and profile[1].

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

The Commissioner has been collaborating with the Competition and Markets Authority (CMA) in assessing these developments and ensuring they meet the requirements of data protection and competition law. The Information Commissioner's Office (ICO) and CMA joint statement of May 2021 outlined that the interest of consumers is best served when the objectives of both competition and data protection are achieved[2]. The ICO and the CMA will continue to work closely together so that developments in the adtech industry operate in a data protection compliant way that ensures an appropriate level of competition.

The proposals from both Google and other market participants are not yet fully realised. There is a window of opportunity for proposal developers to reflect on genuinely applying a data protection by design approach. The Commissioner

[1] https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf.
[2] https://ico.org.uk/media/about-the-ico/documents/2619797/cma-ico-public-statement-20210518.pdf

therefore encourages Google and other participants to demonstrate how their proposals meet the expectations this Opinion outlines.

New initiatives must address the risks that adtech poses and take account of data protection requirements from the outset. Any proposal that has the effect of maintaining or replicating existing tracking practices (such as those described in the 2019 Report) is not an acceptable response to the significant data protection risks that the Commissioner has already described.

The Commissioner expects any proposal to:

- engineer data protection requirements by default into the design of the initiative;
- offer users the choice of receiving adverts without tracking, profiling or targeting based on personal data;
- be transparent about how and why personal data is processed across the ecosystem and who is responsible for that processing;
- articulate the specific purposes for processing personal data and demonstrate how this is fair, lawful and transparent; and
- address existing privacy risks and mitigate any new privacy risks that their proposal introduces.

The Opinion represents the Commissioner's view at the time of publication. The Commissioner may form a different view based on further findings or engagement with key stakeholders.

2. Introduction

The Commissioner puts forward this Opinion on Data protection and privacy expectations for online advertising proposals to provide guidance to market participants about how they can:

- demonstrate a genuine adherence to the principles of data protection by design and by default; and
- bring forward proposals that effectively address the range of data protection and privacy harms that are characteristic of current approaches to online advertising.

The Commissioner outlines a range of data protection expectations that must be met. The Commissioner advises developers to assess their approaches against these expectations. This will help them demonstrate how their proposals will achieve better outcomes.

The Commissioner makes clear that proposals that seek to continue to intrusively track and profile users are at odds with data protection and privacy requirements.

This Opinion also:

- reinforces the need to address the concerns raised in the 2019 report;
- clarifies the Commissioner's views on the joint work being undertaken with the CMA; and
- addresses common misconceptions about the application of data protection and other relevant legislation.

The Commissioner is leading initiatives[3] to:

- create a more transparent, user-centric approach that empowers individuals; and
- addresses the power imbalance that exists between them and key market participants.

User choice, consent, control and accountability must be meaningful. First and foremost, they must be shaped around compliance with the law and consideration of individuals' interests, rights and freedoms.

[3] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/09/g7-data-protection-and-privacy-authorities-meeting-communiqu%C3%A9/

2.1 The Commissioner's work on adtech

In 2019, the Commissioner published a report on the use of cookies and similar technologies and processing of personal data in online advertising[4]. It focused on real-time bidding (RTB) and industry protocols such as OpenRTB[5] and Google Authorized Buyers[6]. These protocols are attempts to standardise how data is collected and shared, and how adverts are served. The 2019 report detailed several inadequate practices in RTB, including systemic compliance issues with:

- legal requirements on cookie use;
- lawfulness, fairness and transparency;
- security;
- controllership arrangements;
- data retention;
- risk assessments; and
- application of data protection by design principles.

The 2019 report acknowledged that there are many issues associated with adtech. This includes the market position of so-called 'big tech' firms, and the financial vulnerability of some online services (eg publishers). The Cairncross review examined a number of these issues in the context of online journalism, such as the role of large online platforms and their relationship with news organisations[7]. While these issues were outside the core scope of the 2019 report, this did not mean they were free from data protection concerns.

The Commissioner called for industry to make changes, but also recognised the need for a measured and considered approach due to the importance of advertising to participants in a commercially sensitive ecosystem[8]. The Commissioner also undertook significant engagement with key stakeholders to obtain industry views, both before and after publication of the 2019 report[9].

In early 2020, the Commissioner set out a revised regulatory approach for the COVID-19 pandemic. This included a reassessment of priorities and resources to take account of the changed circumstances, including a pause in the adtech work. This was to ensure that the ICO could focus its resources into the

[4] https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf
[5] As stated by the Interactive Advertising Bureau (IAB), OpenRTB's goal is "to create a lingua franca for communicating between buyers and sellers". See https://iabtechlab.com/standards/openrtb/ and https://github.com/InteractiveAdvertisingBureau/openrtb/blob/master/OpenRTB%20v3.0%20FINAL.md.
[6] "Authorized Buyers" refers both to Google's own protocol and the broader Authorized Buyers programme, which also supports the OpenRTB protocol. See https://developers.google.com/authorized-buyers/rtb/start.
[7] https://www.gov.uk/government/publications/the-cairncross-review-a-sustainable-future-for-journalism
[8] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/06/blog-ico-adtech-update-report-published-following-industry-engagement/
[9] https://ico.org.uk/about-the-ico/what-we-do/our-work-on-adtech/

pandemic response, and not place undue pressure on industry during that time[10].

In January 2021, the Commissioner announced a resumption of the adtech work with a series of audits[11]. The ICO served assessment notices under the Data Protection Act 2018 (DPA 2018) on six organisations in the adtech ecosystem[12]. The Commissioner is currently assessing the outcomes of these audits.

The Commissioner has also undertaken a review of how some of the most-visited UK online services use cookies and similar technologies. As a result, the Commissioner has written to a number of these services to further assess their compliance. This includes, where appropriate, requiring that they take further steps to ensure their use of cookies is in line with PECR. We continue to monitor the responses from those organisations.

2.2 Recent market developments

Since the 2019 report was published, industry has developed a number of initiatives that seek to address the risks adtech poses and shift towards less intrusive tracking and profiling practices. These include:

- proposals to phase out or "deprecate" the use of "third party cookies" (TPCs) and other forms of cross-site tracking and replace them with alternatives;
- increases in transparency of online tracking, such as Apple's "App Tracking Transparency" (ATT), which has had a notable impact – both in terms of the number of users exercising control over tracking, as well as the market itself[13];
- mechanisms to enable individuals to indicate their privacy preferences in simple and effective ways; and
- developments by browser developers to include tracking prevention in their software.

One of the most significant is the proposal by Google known as the "Google Privacy Sandbox" (GPS). The GPS intends to replace the use of third-party cookies (TPCs) and other forms of cross-site tracking with alternative technologies for enabling targeted advertising (and the measurement of advertising).

Google's status in the digital economy means that any proposal it puts forward has a significant impact. For example:

[10] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/05/ico-statement-on-adtech-work/
[11] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/01/adtech-investigation-resumes/
[12] One assessment notice has been appealed and two withdrawn.
[13] https://www.theregister.com/2021/11/01/apple_privacy_settings/

- the market share of its Chrome browser;
- the services it makes available to individuals and organisations (eg online search); and
- the role it plays in the digital advertising market.

Both the GPS proposals and counterproposals by other market participants seek to ensure that several key purposes for which TPCs are used can continue in a more privacy-friendly manner. These include:

- targeting advertising to individuals based on information related to them (eg their behaviours, interests and attitudes); and
- measuring the success of the advertising (eg whether an individual took an action after seeing an advert).

TPCs currently enable these use cases but often involve unlawful processing of personal data. The phasing out of TPCs is a welcome development. However, any new proposals need to be designed with data protection by design and default considerations from the beginning. They need to reconcile the objectives of advertising and measurement with an approach that reduces the privacy risks and harms to users.

2.3 Purpose of this Opinion

The Commissioner recognises these developments may have a significant market impact. The Commissioner also considers that it is appropriate to provide further regulatory clarity on the data protection expectations that they should meet, as many are at early stages of development. This can ensure that those developing these initiatives:

- build in compliance with the data protection principles at the design stage; and
- mitigate the risk of data protection non-compliance and harm to the individual over the longer term.

It is important that any proposals can demonstrate their compliance with data protection law, irrespective of the status of the market participant that puts them forward.

There is an opportunity for market participants to move towards developing solutions that incorporate key considerations of data protection compliance. They should also place the interests, rights and freedoms of individuals at the core of their design. The Commissioner's assessment of these developments is from that perspective, regardless of who proposes any solution or their position in the market.

2.4 Scope of this Opinion

Article 58(3)(b) of the UK General Data Protection Regulation (UK GDPR) and Section 115(3) of the Data Protection Act 2018 (DPA 2018) allow the Information Commissioner to issue, on initiative or on request, opinions to Parliament, government, other institutions or bodies, and the public, on any issue related to the protection of personal data.

2.4.1 The legal framework

The UK GDPR and DPA 2018 apply to any processing activities in online advertising that involve personal data. The Privacy and Electronic Communications Regulations 2003 (as amended) (PECR) also apply to the use of cookies and similar technologies. The Commissioner continues to monitor, assess and investigate privacy issues within adtech from this perspective. The Commissioner has previously issued guidance about the requirements of the law for these processing activities, including:

- detailed guidance on the use of cookies and similar technologies[14]; and
- the general Guide to the UK GDPR[15], as well as specific guidance on topics such as personal data and controllers and processors[16].

Accountability requires organisations to be able to demonstrate how they comply with the data protection principles[17].

2.4.2 The Commissioner's tasks, functions and powers

Part of the Commissioner's role is to monitor the application of the UK data protection framework in order to protect fundamental rights and freedoms and facilitate the free flow of personal data[18]. However, it is important to note that the Commissioner's tasks, functions and powers do not include endorsement or approval of specific approaches or processing operations outside the circumstances specified in the law[19].

The Commissioner's tasks include:

- promoting public awareness and understanding of the risks, rules and safeguards relating to processing;

---

[14] https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/
[15] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/
[16] See the Commissioner's guidance on "What is Personal Data?", controllers and processors, contracts and liabilities, data protection by design and by default, data protection impact assessments, consent, legitimate interests, and the right to be informed.
[17] https://ico.org.uk/for-organisations/accountability-framework/
[18] See Section 115 of the DPA 2018 and Article 51 UK GDPR.
[19] Section 115(2) of the DPA 2018 specifies that general functions are conferred on the Commissioner by Article 57 of the UK GDPR (tasks) and Article 58 (powers). The Commissioner's authorisation and advisory powers are specified in Article 58(3).

- promoting awareness among controllers and processors of their data protection obligations;
- monitoring relevant developments, particularly information and communication technologies and commercial practices, that have an impact on data protection; and
- fulfilling any other task related to the protection of personal data.

The Commissioner's advisory powers are ways to undertake these tasks. This includes publishing Opinions. Market participants should be clear that the Commissioner cannot pre-approve, co-design or provide a binding view on any proposal or solution where doing so does not form part of these tasks, functions or powers. However, the Commissioner continues to work in collaboration with the CMA to ensure that data protection and privacy outcomes can be robustly assessed as proposals develop.

The Commissioner also notes that data protection obligations fall on controllers and processors. How they determine their roles and responsibilities depends on the specific circumstances and the processing activities involved. The requirement to follow a data protection by design approach applies to organisations responsible for the processing[20]. For example, where organisations design and implement their own products, services or applications to process personal data.

In some cases, market developments may originate from those whose actual role in the eventual processing may be unclear. For example, they may be a producer of products, services or applications that process personal data but do not either take specific decisions about such processing (as a controller does) or undertake that processing on behalf of another (as a processor does).

Where this is the case, Recital 78 of the UK GDPR acknowledges that these producers should be encouraged to take the right to data protection into account during design and development. This is to ensure that organisations using the products can meet their obligations by selecting those that are built with a data protection by design approach.

2.4.3 What this Opinion covers

This Opinion addresses developments since the 2019 report, including those from Google and alternatives from other sources. In general, the Commissioner's view is that these developments are not yet sufficiently mature to assess in detail. They have not fully shown how they demonstrate participants' compliance with the law, or how they result in better data protection outcomes compared to the existing ecosystem. Until they reach an appropriate level of development,

[20] See Article 25 of the UK GDPR.

the Commissioner will reserve detailed analysis and responses to specific proposals and detailed consideration of the broader impacts[21] they may have.

Instead, this Opinion outlines the Commissioner's overarching expectations that any development seeking to address the risks posed by adtech should meet. These include expecting market participants to address the issues highlighted in the 2019 report.

This Opinion is therefore intended for:

- industry participants that are developing alternatives to the current ways in which adtech processes personal data; and
- anyone with an interest in the development and regulation of online advertising technologies. This includes government, regulators, public bodies, industry groups, technology developers and civil society groups.

The Opinion represents the Commissioner's view at the time of publication. It may be subject to change or may lead to future guidance. The Commissioner reserves the right to make changes or form a different view based on further findings, changes in circumstances and engagement with stakeholders.

[21] The ICO's Regulatory Policy Methodology Framework includes guidance on how we assess impacts on individuals and the wider economy. See: https://ico.org.uk/media/about-the-ico/policies-and-procedures/2619767/regulatory-policy-methodology-framework-version-1-20210505.pdf

3. Online advertising developments

A number of developments have taken place within online advertising since the Commissioner published the 2019 report, including across the browser and mobile app spaces. They arise from different market participants, including:

- industry bodies and trade associations;
- browser developers;
- technology firms; and
- standards bodies.

Several of these represent a move away from the use of cookies and similar technologies to undertake tracking of individuals online. They are driven in part by the work of the ICO and other data protection authorities in highlighting the non-compliance with data protection law. Others arise due to potential changes to the wider legislative framework[22].

Furthermore, there is a growing appreciation of the risks of excessively processing personal data and disseminating data of a highly personal nature about an individual's online behaviours. This exposes both individuals and groups to a range of harms, and undermining trust in online services.

The Commissioner supports the shift to less intrusive approaches to online advertising. The Commissioner also acknowledges that some developments are creating significant tensions between the wider adtech market and the browser and mobile platform operators. For example, the role of personalised ad targeting and value measurement of that advertising (ie how to reach the user with an advert, and how to measure if the advert generated value).

The Commissioner welcomes efforts that propose to:

- move away from the current methods of online tracking and profiling practices;
- improve transparency for individuals and organisations;
- reduce existing frictions in the online experience;
- provide individuals with meaningful control and choice over the processing of device information and personal data;
- ensure valid consent is obtained where required; and
- ensure there is demonstrable accountability across the supply chain.

[22] For example, legislation in other jurisdictions such as privacy laws in particular states in the US, as well as proposed EU legislation such as the ePrivacy Regulation, Digital Services Act and Digital Markets Act. In the UK context, see also https://www.gov.uk/government/consultations/data-a-new-direction and https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/10/response-to-dcms-consultation-foreword/.

The Commissioner notes that any solutions presented, even those that appear privacy-positive, need to transparently and accountably demonstrate how they comply with the law and uphold individual rights.

In outlining developments, this section:

- addresses the concept of "online tracking" generally;
- summarises the key issues the Commissioner highlighted in the 2019 report;
- outlines the general move to phase out third-party cookies;
- discusses browser developments;
- discusses the Google Privacy Sandbox;
- discusses developments relating to user preferences and identifiers;
- discusses standards body processes; and
- summarises the Commissioner's ongoing work with the CMA.

3.1 The meaning of "online tracking"

Central to the issues discussed in this Opinion is the role that online tracking plays in the digital economy. This also raises questions about whether it is fundamentally necessary, proportionate and fair to undertake targeted advertising of individuals to:

- enable online services to remain free at the point of use; or
- ensure the existence of a vibrant digital economy with a multiplicity of market participants.

"Online tracking" is not a legally defined term in the data protection framework the Commissioner regulates. The Commissioner notes that in the context of web standards, the term "tracking" is defined by the World Wide Web Consortium (W3C)[23] as:

Quote

"The collection of data regarding a particular user's activity across multiple distinct contexts, and the retention, use, or sharing of data derived from that activity outside the context in which it occurred."[24]

[23] W3C develops open standards for the web. Its membership includes representatives from several business ecosystems, including advertising, e-commerce, media and entertainment, network and communications, publishing, smart cities, automotive and transportation, and Web of Things. Major technology companies such as Google, Apple, Facebook, Amazon, and Microsoft are W3C members.
[24] https://www.w3.org/TR/tracking-compliance

The Commissioner also notes that the ordinary meaning of the word may be defined as "the act or process of following something or someone"[25].

From a data protection perspective, online tracking is a term that describes or refers to different processing activities, undertaken by different means, for different purposes. A variety of organisations can undertake it, from single businesses to large corporate entities. For example, a large organisation that operates multiple online services, or many smaller organisations sharing information between them.

It is not a term that is understood by simply looking at key definitions in the law. However, data protection law defines processing as:

Quote

"any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction"

Additionally, Regulation 6(1) of PECR says that:

Quote

"[...] a person shall not store or gain access to information stored, in the terminal equipment of a subscriber or user"

Online tracking may include many of the activities referred to in the above provisions, depending on the circumstances of any implementation and intended purposes. For example, as the W3C definition indicates, the broader concept of tracking at the very least involves **processing operations** such as:

- collection;
- use;
- disclosure by transmission;
- dissemination or otherwise making available; and
- alignment or combination.

In practice, online tracking may involve many of the types of processing operations defined in data protection law, depending on the circumstances.

[25] https://www.collinsdictionary.com/dictionary/english/tracking

It can involve active or passive techniques. It may include not only personal data that individuals actively provide, but also personal data that results from observation, derivation, and inference[26]. Currently, it generally either begins with or involves processing of device information. It can also include data matching, combination, and enrichment within the extensive data supply chain.

In principle, online tracking can therefore be considered as processing activities involving the monitoring of individuals' actions, especially over a period of time (including the behaviour, location or movements of individuals and their devices), in particular to:

- build profiles about them;
- take actions or decisions concerning them;
- offer goods and services to them;
- evaluate the effectiveness of services they use; and
- analyse or predict their personal preferences, behaviours and attitudes[27].

Online tracking, for any purpose, must not be carried out at the expense of individual rights or compliance with the broader provisions of the law.

For example, the Commissioner has provided guidance on situations where PECR's consent requirement applies[28]. This guidance also discusses both the legitimate interests balancing test and whether further processing is compatible with the original purpose(s). It outlines that, PECR aside, neither the balancing test nor a compatibility assessment would enable the processing to be fair and lawful without consent. This is because of the nature, scope, context and purposes of these processing activities, and the risks they pose to rights and freedoms. This is the case where:

- personal data obtained via the use of cookies and similar technologies is used for purposes such as analysing or predicting personal preferences, behaviour and attitudes of individuals, and to inform measures or decisions taken about them; and

[26] The Commissioner notes that passive tracking that involves personal data is still processing of that data, and can in some circumstances raise more significant risks of harm (eg where individuals are entirely unaware that it takes place). Information that relates to an identified or identifiable individual is personal data. This does not change if the data is collected passively, or where the processing involves observed, derived, or inferred personal data.

[27] See also Recital 24 of the UK GDPR, which relates to the targeting criterion at Article 3(2) on territorial scope. While this concerns whether the monitoring limb of the targeting criterion is engaged, the Recital specifically references individuals being "tracked on the internet" and is therefore useful in the context of discussing what "tracking" means from a data protection perspective. Recital 24 also clearly refers to subsequent profiling techniques.

[28] https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/how-do-the-cookie-rules-relate-to-the-gdpr/

- online tracking, including profiling, is undertaken for purposes such as direct marketing, behavioural advertising, data brokering and location-based advertising.

The law intends to strike a balance between protecting individual rights while recognising the function that personal data has for the economy and wider society[29]. This does not mean online tracking cannot take place. The key is that the purposes are legitimate and that, unless exemptions apply, individuals are:

- made aware of the processing;
- given meaningful control over their data; and
- can exercise their rights.

Organisations that adopt internal definitions of online tracking need to be clear about the processing activities involved, and how the law applies where these include personal data and device information. This is particularly important if their own meaning of the term forms part of any proposals they develop for online advertising solutions.

The roles that online tracking and digital advertising play in the digital economy is of interest both to other regulators and to Government. The Commissioner continues to engage on these issues with partner regulators through the Digital Regulation Cooperation Forum[30].

3.2 Key issues highlighted in the 2019 report

One of the Commissioner's most important expectations is that industry addresses the issues highlighted in the 2019 report. The Commissioner continues to see evidence of these issues. In brief, these were:

Area	Issue
PECR	Collection of invalid consent due to design choices and lack of clear and comprehensive information about the purposes for which cookies and similar technologies are used. The use of non-essential cookies was frequently justified as being in the "legitimate interests" of the organisation, with consent not being sought as required by PECR[31].
Lawful basis	Unlawful processing of personal data by the use of cookies and similar technologies due to reliance on legitimate interests (see above). Even if it were possible to rely on

[29] See Recital 4 of the UK GDPR and paragraphs 16 to 19 and 37 to 46 of the ICO and CMA joint statement.
[30] https://www.gov.uk/government/publications/digital-regulation-cooperation-forum-workplan-202122/digital-regulation-cooperation-forum-plan-of-work-for-2021-to-2022
[31] The Commissioner reiterates that legitimate interests cannot be relied upon to set non-essential cookies.

Area	Issue
	legitimate interests, participants are unable to demonstrate how they would properly carry out legitimate interests assessments and implement appropriate safeguards.
Special category data	Unlawful processing of special category data due to the lack of explicit consent, with cookie consent mechanisms not designed to collect such consent[32].
Transparency	Privacy information is overly complex but does not provide sufficient clarity about the processing. Existing industry frameworks and mechanisms are insufficient to ensure transparency or fair processing.
Data supply chain	Complex data supply chain coupled with how RTB works means it is unclear who will process personal data, and how this processing complies with data protection requirements.
Controllership	Supply chain involves multiple parties; there is a lack of clarity over roles and responsibilities.
Contracts	Industry use of contractual controls as sole basis for providing guarantees of data protection compliance is insufficient, particularly without appropriate monitoring.
Security	Individuals have no guarantee about the security of their personal data once it is processed.
Profiling	Extensive use of profiling and enrichment of personal data, which is disproportionate, intrusive and unfair in the context of the intended purposes.
Risk assessment	Lack of understanding about when data protection impact assessments (DPIAs) are required, giving little confidence that the risks associated with the processing are fully assessed and mitigated.
Data minimisation	No assessment of what data is needed to achieve the purpose due to a perception that all data is required or is otherwise useful.
Data retention	Inconsistent retention periods across different industry participants means different periods may apply when data is

[32] The Commissioner acknowledges efforts made since 2019 by industry bodies including IAB UK to reduce, minimise or eliminate the processing of special category data in adtech.

Area	Issue
	disclosed or disseminated between industry participants. The rationale for retention periods that do exist is unclear.

These issues of compliance with data protection have real world consequences, and can lead to harm for individuals and groups. Prevention or mitigation of harm is a fundamental purpose for a regulator. Harm can refer to detriment suffered by individuals, or societal harms with collective consequences. Harm can also arise where individuals or groups are prevented or impeded from exercising their rights. The ICO's non-exhaustive taxonomy of harms[33] focuses on harmful consequences, acknowledging firstly that some types of harm overlap with others, and secondly that some harms can lead to others.

The issues highlighted in the 2019 report relate to several types of harm that organisations needed to consider as part of a risk-based approach to data protection. These included:

Type	Description
Lack of autonomy and loss of control	Where individuals are aware of tracking, they may not wish it to take place but feel powerless to stop it. This reduces their ability to choose freely without external influence and deprives them of meaningful control over the processing of their data.
Power and information asymmetry	The opacity of online tracking and the high level of invisible processing creates both power and information asymmetry. Organisations may process significant amounts of personal data. They may undertake profiling and draw inferences in ways individuals would not reasonably expect. Individuals may have no idea about the organisations that hold their data and therefore cannot exercise their rights.
Manipulation and influence	Extensive processing about people's behaviour, preferences and attitudes may enable manipulation and influence. In particular where the means of processing allow for greater tracking and targeting than offline equivalents.
Misuse	Where data collected for one purpose is re-used or misused (eg by other entities it is disclosed to) for other purposes that are not compatible with the original purposes of collection.

[33] https://ico.org.uk/media/about-the-ico/policies-and-procedures/2619767/regulatory-policy-methodology-framework-version-1-20210505.pdf, page 15 and Annex B.

Type	Description
Lack of confidentiality	Significant security risks may arise due to the volume and extent of personal data processing, the number of different organisations involved, and reliance on contractual controls as control measures. The risk of personal data breaches increases.
Chilling effects	Individuals who believe they are being tracked online may modify their behaviour. The processing may impact other rights and freedoms. For example, freedom to determine identity, how individuals choose to present themselves to the world, and how they engage with others.
Reduce trust and confidence	Individuals may avoid using digital services which may then result in unrealised benefits across the economy. Innovation and new technological developments may suffer due to reduced consumer confidence. The availability of personal data may drop, leading to collection of more of it in covert ways to compensate.

New proposals for enabling online advertising must address the issues and harms highlighted above. Use of TPCs has consistently been shown as a key factor in these issues. The lack of accountability across the ecosystem must not be transferred to any new approach.

3.3 Removal of third-party cookies

Prior to the development of the cookie, online services were incapable of remembering visits made to their sites by individual users. As the first e-commerce platforms were being developed there was a need to enable an online service to remember the user's activities[34]. The goal behind the cookie was "to create a session identifier and general 'memory' mechanism for websites that didn't allow for cross-site tracking"[35].

The Internet Engineering Taskforce (IETF) published the original specification for cookies (RFC 2109) in February 1997. This stated that cookies must match the URL the individual sees in their browser. In other words, cookies were originally intended to be used only to keep track of an individual's activity on the site they

[34] For example, early proposals to develop shopping carts so that an online service could remember what individuals added to their basket and allow them to make purchases.
[35] http://montulli.blogspot.com/2013/05/the-reasoning-behind-web-cookies.html

visited. The specification also said that the user was to have "considerable control" over cookie management for "privacy considerations"[36].

As the web and its role in our lives evolved, so did the approaches to identifying, tracking, profiling and targeting individual users. The use of cookies evolved from their original purpose into a vehicle for gathering and processing significant volumes of both device information and data of a highly personal nature. The evolution of cookies and their use for targeted advertising is a cautionary tale of the risks of repurposing technology without also building in safeguards to protect against misuse and harm. Their deprecation is a positive step. However, this does not mean that their proposed replacements are inevitably better.

The Commissioner is aware of views that caution against the removal of TPCs because online tracking will merely continue by other means (eg fingerprinting techniques). The Commissioner notes that both PECR and data protection law are technology-neutral. Regulation 6 of PECR is sometimes known as the "cookie law". In practice, it applies to **any** technique that stores information (or accesses information stored) on an individual's device – as the ICO's guidance clearly states[37].

Additionally, online targeted advertising generally entails the processing of personal data whether PECR is engaged or not. Significant data protection risks arise where individuals are unaware of processing activities involving their data. Organisations should therefore not assume that there are no compliance requirements with PECR or data protection law merely because TPCs are removed (or that they already do not use them for tracking purposes).

3.4 Browser and software developments

Individuals primarily interact with the internet through software applications, such as browsers. At their most basic level, browsers simply fetch and retrieve information from the web and present that information to the individual user. However, browsers themselves do not determine the content that online services incorporate, even if they can determine elements of how that content might be displayed (or not displayed). Ultimately, providers of online services take decisions about the tracking technologies their websites and mobile apps incorporate.

In recent years, browser manufacturers have moved towards limiting the ways in which their users are tracked by online services. This may be both to protect those individuals but also to provide differentiation in the market. Examples include:

[36] https://datatracker.ietf.org/doc/html/rfc2109, sections 4.3.2 and 4.3.3.
[37] https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/what-are-cookies-and-similar-technologies/#cookies5

- **Apple**, developers of the Safari browser (as well as the Mac OS and iOS operating systems, along with widely-used hardware such as the iPhone). Apple introduced "Intelligent Tracking Prevention" (ITP) into Safari in June 2017[38]. Apple states that ITP now blocks TPCs by default[39].
- **Brave Software**, developers of the Brave browser. Brave automatically blocks online adverts and tracking by default and incorporates protections against fingerprinting[40].
- **Microsoft**, developers of the Edge browser (as well as the Windows operating system). Edge includes a tracking prevention feature based on the Disconnect list[41]. By default, it blocks trackers from sites the user has not visited. This intends to fulfil Microsoft's "browser privacy promise", where Microsoft describes how it wants to keep users safe on the web and allow them to take control of their browsing data[42].
- **Mozilla**, developers of the Firefox browser. Firefox incorporates several tracking protections such as "Enhanced Tracking Protection"[43], "Total Cookie Protection"[44] and "Enhanced Cookie Clearing"[45]. ETP also includes the Disconnect list. It blocks social media trackers and cross-site tracking cookies. It was defaulted to "on" in June 2019[46].

This is not an exhaustive summary of every browser development that states it intends to improve user privacy.

There are also related developments in operating systems and mobile ecosystems. For example, in the use of advertising identifiers as well as initiatives to provide more transparency to individuals about online tracking. One example is with Apple's "Identifier for Advertising" (IDFA) and the related "App Tracking Transparency" (ATT) framework. ATT requires apps to present individuals with an "authorization request" when they collect data, and share data with other organisations (eg for tracking that individual across different online services or accessing the IDFA)[47].

The use of other advertising identifiers is also changing. For example, Google's recent announcement that the Advertising ID on Android will be replaced by a string of zeros when an individual opts-out of personalised advertising[48].

---

[38] https://webkit.org/blog/7675/intelligent-tracking-prevention/
[39] https://webkit.org/blog/10218/full-third-party-cookie-blocking-and-more/
[40] https://brave.com/privacy-features/
[41] https://disconnect.me/
[42] https://microsoftedgewelcome.microsoft.com/en-gb/privacy?form=MA13E7
[43] https://blog.mozilla.org/futurereleases/2018/08/30/changing-our-approach-to-anti-tracking/
[44] https://blog.mozilla.org/security/2021/02/23/total-cookie-protection/
[45] https://blog.mozilla.org/security/2021/08/10/firefox-91-introduces-enhanced-cookie-clearing/
[46] https://blog.mozilla.org/en/products/firefox/firefox-now-available-with-enhanced-tracking-protection-by-default/
[47] See https://developer.apple.com/app-store/user-privacy-and-data-use/ and https://developer.apple.com/documentation/apptrackingtransparency
[48] https://support.google.com/googleplay/android-developer/answer/6048248?hl=en-GB

It is important for organisations to be clear about the status of these identifiers and how the law applies to them. The Commissioner's guidance on personal data[49] and on cookies[50] provides more information, including about the key data protection requirements of lawfulness, fairness and transparency.

The Commissioner recognises that ATT has prompted a significant increase in individuals declining to be tracked. The resulting market impact arguably reflects the strength of feeling about online tracking[51]. The Commissioner also notes that the CMA is considering the impact of developments in mobile ecosystems (including ATT) from a competition perspective. The ICO's collaboration with the CMA aims to ensure that organisations treat choice and control consistently both for themselves and for others.

The Commissioner will continue to engage on the data protection implications of these developments. However, in principle, the Commissioner notes that any development that empowers individuals and enables them to have meaningful control over the use of their data is a positive one.

The Commissioner may choose to assess the data protection impacts of browser and software developments in more detail in due course, and in collaboration with other relevant authorities.

3.5 The Google Privacy Sandbox

The Commissioner recognises that any proposal from Google has significant attention and impact. This is due to the company's position in the market, the number of online services it provides, and the volume of personal data it processes. For example:

- the Chrome browser has a UK market share of around 60% on desktop[52] and 39% on mobile[53];
- Chromium, principally developed by Google[54], acts as the engine for several other browsers including Edge, Brave, Vivaldi, and Opera;
- the Android operating system has a UK market share of around 45%[55];
- Google Search has a UK market share of around 93%[56];

[49] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-are-identifiers-and-related-factors/#pd3
[50] https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/
[51] https://www.theregister.com/2021/11/01/apple_privacy_settings/
[52] https://gs.statcounter.com/browser-market-share/desktop/united-kingdom
[53] https://gs.statcounter.com/browser-market-share/mobile/united-kingdom
[54] https://blog.chromium.org/2019/11/intent-to-explain-demystifying-blink.html
[55] https://gs.statcounter.com/os-market-share/mobile/united-kingdom
[56] https://gs.statcounter.com/search-engine-market-share/all/united-kingdom

- Google has multiple online services aimed at both individuals and businesses (eg Gmail, Google Docs, Google Cloud, G Suite, Google Analytics); and
- Google offers a significant number of products in the online advertising market, including Google Ad Manager, Google Ads, AdSense, and the Authorized Buyers programme.

In August 2019, Google Chrome engineers introduced the GPS concept, referring to it as an "initiative to develop a set of open standards to fundamentally enhance privacy on the web"[57]. The GPS has three key goals:

- replacing functionality served by cross-site tracking;
- "turning down" TPCs; and
- mitigating workarounds.[58]

Each goal includes several proposals to address existing use cases[59]. The following are examples of these proposals:

- "Attribution Reporting" intends to "measure when user action (such as an ad click or view) leads to a conversion, without using cross-site identifiers"[60].
- "First Party Sets" intends to enable a group of related domains owned by the same entity to function as a single first party for a variety of defined use cases[61].
- "Federated Learning of Cohorts" (FLoC) relates to interest-based ad targeting and intends to "allow sites to guess your interests without being able to uniquely identify you"[62].
- "FLEDGE" relates to remarketing and is designed so that it "cannot be used by third parties to track user browsing behaviour across sites"[63].
- "Trust Tokens" intends to enable websites to convey "a limited amount of information from one browsing context to another to help combat fraud"[64].
- "User-Agent Reduction" intends to "limit browser data shared to remove sensitive information and reduce fingerprinting"[65].

The Commissioner acknowledges that the overall ambition for GPS could lead to a more privacy-focused approach to online advertising. However, there are

[57] https://www.blog.google/products/chrome/building-a-more-private-web/
[58] https://www.chromium.org/Home/chromium-privacy/privacy-sandbox
[59] https://developer.chrome.com/docs/privacy-sandbox/overview/
[60] https://developer.chrome.com/docs/privacy-sandbox/attribution-reporting/
[61] https://developer.chrome.com/docs/privacy-sandbox/first-party-sets/
[62] https://developer.chrome.com/docs/privacy-sandbox/floc/
[63] https://developer.chrome.com/docs/privacy-sandbox/fledge/
[64] https://developer.chrome.com/docs/privacy-sandbox/trust-tokens/
[65] https://developer.chrome.com/docs/privacy-sandbox/user-agent/

several factors that need consideration before any detailed analysis can take place. For example:

- the overall data protection impact of the GPS depends on how each of its proposals interact collectively. For example, many rely on other proposals that are also under parallel development;
- many of these proposals are at different points in the development process, ranging from discussion to testing to origin trials[66];
- some proposals such as FLoC and First Party Sets have been criticised by other market participants, for several reasons[67, 68, 69, 70];
- some proposals such as FLoC and FLEDGE have seen issues arise during development that may effectively introduce additional tracking vectors[71]; and
- regulators, including the CMA in the UK and authorities in other jurisdictions, have expressed concerns about the impact of the GPS.

Proposals like Trust Tokens and User-Agent Reduction are relevant to the privacy and security architecture of the web. Those like Attribution Reporting are built around enabling established patterns and practices in online advertising, such as measurement.

Others like First Party Sets, FLoC and FLEDGE are more novel. For example, First Party Sets involves a different approach to the established security model of the web. FLoC and FLEDGE include techniques such as the use of machine learning and increased on-device processing. These could offer privacy benefits if engineered correctly.

However, some proposals also receiving substantial criticism. For example, some reviews suggest they introduce new or different tracking vectors (eg through fingerprinting). In this respect, the Commissioner reiterates to all market participants that the provisions of PECR and data protection law are technology-neutral. The Commissioner reminds proposal developers that the Commissioner's guidance on the use of cookies and similar technologies applies wherever there is storage of information, or access to information stored, on individual's devices[72]. Organisations must demonstrate that new approaches do not introduce additional privacy threat vectors or lead to increased use of fingerprinting or both.

---

[66] https://privacysandbox.com/timeline/
[67] https://techcrunch.com/2020/11/23/digital-marketing-firms-file-uk-competition-complaint-against-googles-privacy-sandbox/
[68] https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea
[69] https://blog.mozilla.org/en/privacy-security/privacy-analysis-of-floc/
[70] https://github.com/w3ctag/design-reviews/blob/main/reviews/first_party_sets_feedback.md
[71] See footnote 69 above and https://github.com/WICG/turtledove/issues/211
[72] https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/what-are-cookies-and-similar-technologies/#cookies5

Google has not yet fully articulated how the GPS proposals comply with the requirements of data protection law and PECR – both individually or as a whole. This is partly due to individual proposals being at different stages of development, as well as issues raised during those processes. As such, the Commissioner does not intend to provide a detailed critique of specific GPS proposals beyond the content of this Opinion. This may change in future, where appropriate and if they reach a more advanced stage.

As part of the GPS, Google also intends to phase out support for TPCs in the Chrome browser. The Commissioner understands that Google will phase out TPCs in 2023 once the key elements of the GPS are deployed[73]. In the meantime, the CMA and the ICO envisage further dialogue on the development and implementation of the GPS. Our engagement approach with the CMA is described in the ICO and CMA joint statement and Memorandum of Understanding[74].

The changes Google proposes through the GPS will impact Google's own business as well as the publishers, advertisers and adtech organisations that rely on it. It will also impact the browser manufacturers that may choose to incorporate GPS technologies in their products. Additionally, the collective impact on the broader web ecosystem is significant.

3.6 Developments related to user preferences and identifiers

Since the 2019 report there have also been developments relating to the broad intent of enabling individuals to express their preferences about online tracking. Some of these involve browser-based controls, while others are about online consent management. This section summarises several of these developments. It is not an exhaustive list, and the Commissioner may undertake more detailed analysis of specific developments in the future.

It is important to note that user preference developments and identifier-based proposals present different approaches to achieving their outcomes. Some intend to provide individuals with a simple-to-use method of expressing a preference and for that to be respected across the web. Others are specifically intended to manage the reduction and eventual removal of TPCs while continuing to enable targeted advertising.

3.6.1 The Transparency and Consent Framework (TCF)

The TCF is developed by IAB Europe. It aims to communicate an individual's preferences between online services and other participants within the advertising

[73] https://blog.google/products/chrome/updated-timeline-privacy-sandbox-milestones/
[74] https://ico.org.uk/media/about-the-ico/mou/2619798/ico-cma-mou-20210430.pdf

data supply chain. The first version of the TCF was published in 2018, and it has continued to develop since.

The Commissioner substantively addressed the TCF in the 2019 report, noting that it was insufficient to ensure transparency, fair processing or free and informed consent. There were also concerns stemming from a lack of clarity about how compliance was monitored and a reliance on contractual controls. Subsequent iterations of the TCF and its use by publishers have not significantly addressed these issues[75].

The Commissioner acknowledges the ongoing investigation into IAB Europe and the TCF by the Belgian data protection authority[76]. The Commissioner notes the suggestion from IAB Europe that they expect to be confirmed as a controller for the TCF. The Commissioner will reflect on this at the appropriate time, and recognises that the outcome of this activity is subject to applicable processes at both the national and EU levels.

3.6.2 Global Privacy Control (GPC)

GPC is a proposed specification that will allow individuals to notify online services of their privacy preferences[77]. It can take the form of a setting within a browser or an extension that an individual can install. When enabled, it sends a signal communicating the individual's preferences about the sale or sharing of their data to each site. It shares similarities with the historic Tracking Preference Expression specification ("Do Not Track" or DNT).

GPC's draft specification states that it is intended to convey a "general request" concerning the sale or sharing of personal data, but "is not meant to withdraw a user's consent to local storage as per the ePrivacy Directive […] nor is it intended to object to direct marketing under legitimate interest"[78].

As such, the GPC does not at this time appear to offer a means by which user preferences can be expressed in a way that fully aligns with UK data protection requirements. However, this is in part due to the context in which it has been developed and applied to date.

3.6.3 Advanced Data Protection Control (ADPC)

ADPC is developed by the RESPECTeD Project, formed by the Sustainable Computing Lab at the University of Vienna and the non-profit organisation Nyob.eu. It "aims to empower users to protect their online choices in a human-

[75] For example, the Commissioner notes that current implementations of the TCF appear to contain settings options for both consent and legitimate interests in respect of non-essential cookie use.
[76] https://iabeurope.eu/all-news/update-on-the-belgian-data-protection-authoritys-investigation-of-iab-europe/
[77] https://globalprivacycontrol.org/faq
[78] https://globalprivacycontrol.github.io/gpc-spec/, Section 5, "Legal effects".

centric, easy and enforceable manner". It also intends to support publishers and service providers to comply with applicable law, including data protection[79].

The Commissioner acknowledges the RESPECTeD Project's own description of ADPC being a proof-of-concept and a starting point for a broader discussion. As such, the Commissioner does not intend to address its functionality in this Opinion, or provide a view about whether it achieves its stated goals.

3.6.4 Identifier-based proposals

These proposals originate with industry participants, trade associations and representative groups. Conceptually, they have a similar aim to things like the TCF, GPC and ADPC in that they intend to collect an individual's preference and transmit it to other market participants. However, they are based on the use of some form of identifier. This generally relates to the personal data of an individual using the service (such as an email address). Organisations adopting the solution collect this information, as opposed to general preference settings or controls at the browser or software level[80].

Depending on the specific solution, once an individual provides their data, they can then set their preferences about its use. The identifier may be further processed, and also shared with other organisations.

The Commissioner notes that these solutions generally appear focused on the concept of reducing direct identifiability. Depending on the proposal, this process is sometimes called "anonymisation". However, it is important that developers of these solutions note that:

- if terminal equipment information is processed, Regulation 6 of PECR applies whether the information is personal data or not; and
- the concept of personal data is broader than direct identifiability. Information is personal data when it relates to an identified or identifiable individual. An identifiable individual is one who can be identified, **directly** or **indirectly.** Data protection law also includes "online identifiers" in the definition of personal data[81].

Effective anonymisation requires organisations to demonstrate how they mitigate identifiability risk. If there are means reasonably likely to be used to identify an individual (directly or indirectly), then the data is not anonymised. This means data protection law applies to the information. Organisations need to

[79] https://www.dataprotectioncontrol.org/about/

[80] Examples of identifier-based solutions include concepts such as the Trade Desk's "Unified ID 2.0", LiveRamp's "RampID", and the "Secure Web Addressability Network" (SWAN) proposal. See also the description of the IAB TechLab, "1:1 Linked Audiences", at https://iabtechlab.com/blog/re-architecting-digital-media-for-predictable-user-privacy/.

[81] See Section 3 of the DPA 2018 and Article 4(1) and Recitals 26 and 30 of the UK GDPR, as well as the Commissioner's guidance: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/

consider identifiability risk when they seek to demonstrate that their approach results in the creation and subsequent processing of anonymous information[82].

Identifier-based solutions can require an individual to supply something associated with them such as their email address. They can therefore involve processing of personal data at the outset. The underlying email address may ultimately be "masked", at least in a sense. However, an identifier is created for the purposes of processing information relating to that individual. This is regardless of the extent to which the original email address or other information such as their name can be inferred from it. Depending on the specifics, these approaches may also not result in effective pseudonymisation, particularly if the original email address is also involved[83].

It is also unclear whether these solutions enable individuals to have a general choice about tracking in the first place, and what happens when they make this choice. For example, whether the online service becomes inaccessible to them if they indicate they do not want to be tracked. This does depend on the approach that specific solutions choose to take and may therefore not be identical with each proposal. However, this may essentially replicate the current issues with tracking walls. These approaches also need to ensure that they do not use dark patterns and nudge techniques to get individuals to "agree" to be tracked in order to access those services.

The Commissioner notes that some of these proposals are subject to significant comment and scrutiny, and does not intend to address the specific details of any critique or response in this Opinion[84]. However, looking at these proposals in concept, the Commissioner's view is that these solutions do not address the issues raised in the 2019 report regarding transparency, control, consent or accountability.

They also introduce a more fundamental question about whether it is necessary, proportionate or fair for individuals to have to provide their personal data in the first place. This is particularly the case if identifier-based solutions only offer an opt-out. This replicates many of the existing issues that arise in current opt-out solutions. The proposals also do not seem to recognise the additional risks of harm that they introduce. For example, they involve the creation of a "universal" identifier which may in concept provide for more direct, detailed and systematic tracking than the existing ecosystem. More generally, they do not seem to remove or reduce online tracking activities and may also provide incentives for online services to increase the use of tracking walls.

---

[82] https://ico.org.uk/media/about-the-ico/documents/4018606/chapter-2-anonymisation-draft.pdf.

[83] It should be noted that in at least one proposal the email address itself appears to be processed in its original form by certain participants for the purposes of displaying a user interface and updating network participants. See https://github.com/SWAN-community/swan/blob/main/apis.md.

[84] See for example https://blog.mozilla.org/en/mozilla/swan-uid2-privacy/ and https://swan.community/our-response-to-mozillas-privacy-analysis-of-swan-community/.

Overall, in their current form these approaches do not appear to result in a significantly different outcome for individuals when compared with existing techniques that use cookies and similar technologies.

3.6.5 Summary

This is not an exhaustive list. The Commissioner may, in due course and in collaboration with other relevant authorities, choose to assess the data protection and competition impacts of these developments more specifically.

However, it is already technologically possible to ensure that individuals' preferences are respected, and the use of their personal data is minimised. In this context, the Commissioner has initiated a strategic dialogue among G7 data protection and privacy authorities to work together to ensure that:

- people's privacy is more meaningfully protected;
- businesses can provide a better browsing experience; and
- technology firms and standards organisations are encouraged to develop and roll out privacy-orientated solutions[85].

The Commissioner therefore welcomes the general intent of proposals that seek to provide a means for individuals to express their preferences easily, and for that to be reflected by online services they visit. In concept, these have the potential to reduce some of the risks and harms identified in the 2019 report (eg by giving greater control to individuals). They may also contribute to the work of the G7 authorities.

The Commissioner reiterates that any proposal must offer meaningful choice to users and allow them to decide not to be tracked or profiled. Proposals that essentially repackage the fundamental issues highlighted in the 2019 report do not fit with the Commissioner's expectations.

The ICO will continue to work with other data protection authorities and the CMA to explore and further enhance the ability for users to exercise meaningful choice and control.

3.7 Standards body processes

Proposals that relate to web architecture and infrastructure have led to continuing engagement at internet standards bodies such as W3C. For example, Google has expressed its intent for some of the GPS proposals to become new web standards, enabling their use by other organisations.

[85] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/09/ico-to-call-on-g7-countries-to-tackle-cookie-pop-ups-challenge/. The dialogue involves authorities from Canada, France, Italy, Germany, Japan, and the United States alongside the ICO.

Where proposals are put forward for application in the UK, they should demonstrate how they take account of the legislative requirements set out in the UK GDPR, DPA 2018 and PECR (eg data protection and PECR requirements about the processing of personal data and device information).

Where approaches involve potential web standards or may have significant impact on the broader web, the Commissioner expects any proposal to:

- engage organisations such as the W3C at an appropriate stage in the development lifecycle; and
- have worked through any applicable review process.

For example, the established means at W3C to obtain wider review[86], which includes the "Self-Review Questionnaire: Security and Privacy"[87]. This is intended to address likely questions raised by key W3C groups such as the Technical Architecture Group and Privacy Interest Group.

The Commissioner observes that several elements in the Security and Privacy Questionnaire may have application in the context of controllers who need to undertake DPIAs. While the W3C processes are not a replacement for any legal requirements like DPIAs, they may form part of the relevant considerations. The Commissioner also notes that the questionnaire advises conducting a privacy impact assessment as part of the process. Even where the proposer is not a controller or processor, it is good practice to undertake this activity. It not only enables the proposer to demonstrate how they consider relevant privacy issues, but also may enable controllers to meet their own data protection obligations if or when they decide to adopt the proposal.

The Commissioner's collaboration with the CMA includes exploring the role of the web standards organisations in shaping the technical details of any proposals.

3.8 The Commissioner's work with the CMA

During 2019-20, the CMA conducted a market study into digital advertising. The CMA's report was published in July 2020[88]. Following this publication and in the broader context of its digital work, the CMA is conducting a market study into mobile ecosystems[89] and investigating various market developments (including the GPS[90] as well as Apple's App Store[91]) to assess their compliance with competition law. This is to ensure effective competition outcomes for the benefit of consumers.

[86] https://www.w3.org/Guide/documentreview/
[87] https://w3ctag.github.io/security-questionnaire/
[88] https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study
[89] https://www.gov.uk/cma-cases/mobile-ecosystems-market-study
[90] https://www.gov.uk/cma-cases/investigation-into-googles-privacy-sandbox-browser-changes
[91] https://www.gov.uk/cma-cases/investigation-into-apple-appstore

The CMA recognises strong data protection and privacy as a key measure of a healthy market. The ICO and the CMA intend our regulatory approaches to work together to benefit the UK. We both want to ensure that:

- people have genuine choice over the service or products they prefer, with a clear understanding of how and by whom their data will be used; and
- businesses compete on an equal footing to attract customers, with transparency in the way they operate and the provision of meaningful choice across the market.

In May 2021, the ICO and the CMA published a joint statement[92] setting out our shared views on:

- the interactions between competition and data protection in the digital economy;
- how both regulators are working together to maximise regulatory coherence; and
- the steps we intend to take to understand and promote outcomes which achieve the objectives of the competition and data protection regimes.

The CMA is conducting a formal investigation under the Competition Act 1998 into the GPS[93]. The investigation is considering the impact of these proposals on competition in digital advertising markets. It incorporates consideration of the regulatory requirements set by the ICO.

As part of this process Google has offered a range of commitments to the CMA in relation to the GPS. These include ensuring compliance with data protection and privacy standards. The ICO has been involved alongside the CMA in the assessment of these proposals. The CMA has been reviewing and assessing Google's offer of modified commitments, with that stage of the CMA's investigation currently due to complete by the end of November 2021.

The ICO is supporting the CMA so that they can appropriately factor in the requirements of data protection into any assessment of a market participant's ability to leverage data protection legislation. For example, to either facilitate data access or engage in practices which restrict data flows in an anti-competitive manner.

The Commissioner will continue to work collaboratively with the CMA to assess Google's proposals, and support the CMA's currently ongoing commitments process in respect of data protection and privacy.

[92] https://ico.org.uk/media/about-the-ico/documents/2619797/cma-ico-public-statement-20210518.pdf
[93] https://www.gov.uk/cma-cases/investigation-into-googles-privacy-sandbox-browser-changes

4. Data protection concerns

As the ICO has progressed its work on adtech, alongside developing a close working relationship with the CMA, the Commissioner has noted several issues or misconceptions. These have arisen externally among some market participants. Several were referenced in the joint statement. They include:

- a view that data protection law inherently favours the concept of a "first party" over that of a "third party" (as the terms are used in web standards and in industry)[94];
- a perception that organisations can do what they want with personal data after collecting it;
- an assertion that data protection law favours disclosure of personal data within a group of undertakings over data sharing between independent businesses[95]; and
- a belief that data protection law enables large technology platforms to, in essence, use privacy as a "shield" by interpreting the law in a self-preferencing way.

In addressing these issues and misconceptions, the Commissioner notes that the guiding principles for data protection are to consider individuals' interests, rights and freedoms and in particular to uphold their information rights.

As the ICO and CMA joint statement notes, there are strong synergies between competition and data protection objectives. The interests of individuals and organisations are met when the requirements of both laws are upheld[96]. The links between data protection, competition and consumer law are extremely important given the roles of data in general, and personal data in particular, in the business models of online services. Individuals and organisations benefit from a healthy market where:

- there is genuine choice;
- there is the freedom to exercise that choice; and
- data protection and privacy are built into the design of products, services and applications that process personal data.

The Commissioner is clear that data protection and privacy can work in harmony with the goals of ensuring fair competition. Market participants should note that the ICO and the CMA are committed to supporting each other's goals and have

[94] https://ico.org.uk/media/about-the-ico/documents/2619797/cma-ico-public-statement-20210518.pdf, paragraphs 20 to 22 and Box B.
[95] https://ico.org.uk/media/about-the-ico/documents/2619797/cma-ico-public-statement-20210518.pdf, paragraphs 76 to 83.
[96] https://ico.org.uk/media/about-the-ico/documents/2619797/cma-ico-public-statement-20210518.pdf, paragraphs 50 to 67.

already responded to and addressed perceived tensions between our respective regimes. We have made clear that the objectives of data protection and competition law are not "tradeable". For example, assumptions that enabling access for market participants reduces requirements for data protection to be considered are unacceptable.

4.1 First parties and third parties

As highlighted in the joint statement, a distinction is often drawn between the concepts of "first party" and "third party" when used both in web standards and industry definitions of data use[97]. The Commissioner is aware of a view by market participants about how data protection law regards these concepts. For example, that first party has an inherently lower risk than third party. The Commissioner rejects this view. What is relevant for data protection purposes is:

- whether the data is personal data;
- the organisation(s) responsible for determining the purposes and means of the processing, and for demonstrating compliance; and
- if the processing involves disclosure to other organisations, clarifying who they are, their roles and responsibilities, and how they will process the data in compliance with the law after they receive it.

Similarly, what is relevant for PECR purposes is:

- who is responsible for processing terminal equipment information; and
- the purposes they want to process it for[98].

4.1.1 The different meanings of first and third party

The Commissioner believes that confusion arises partly because the two terms mean different things in different contexts[99]. They do not necessarily reflect the legislation the Commissioner regulates in all cases. This may cause misunderstandings to arise, both in the context of developing a particular proposal as well as how those responsible assess the data protection implications of that proposal.

The Commissioner understands that the main uses of the terms are:

- in web standards and (in particular) cookie use;
- as categorisations of data in the marketing industry; and

[97] https://ico.org.uk/media/about-the-ico/documents/2619797/cma-ico-public-statement-20210518.pdf, paragraph 22 and Box B.
[98] For example, the responsible person may have taken decisions about the means of this processing, including use of tools or code provided by another entity.
[99] This appears to be recognised by W3C contributors, at least in discussion groups. For example, see: https://www.w3.org/2020/10/27-party-time-minutes.html.

- in laws and regulations (eg contract law generally, as well as UK data protection law specifically).

It is therefore crucial that any market participant who adopts these terms in the context of proposals that involve personal data processing is clear about:

- the meaning of the term they use; and
- how it relates to data protection law.

4.1.2 First- and third-party in the context of web standards and cookies

The first type of use generally relates to a first party being the online service an individual visits. Any other service from which content is loaded is a third party. In essence, if the individual visits the website https://example.com, Example.com is the first party.

This is closely but not precisely mirrored in the context of both first- and third-party cookies, as well as how browser tracking policies work at web standards organisations such as W3C[100]. The ICO's guidance on the use of cookies and similar technologies also reflects this[101].

It is correct to note that the use of cookies and similar technologies presents lower privacy risks in some cases than in others. Some uses of first-party cookies may be regarded as carrying a lower privacy risk (eg the concept of "first party analytics"). However, this is not a general rule and does not necessarily apply to first-party cookies alone. The risks ultimately depend on the nature, scope context and purposes of the processing and how it is implemented.

The Commissioner is aware of suggestions by members of W3C groups to adopt an alternative approach to these terms in the context of web standards, precisely due to the differences in meaning[102]. The Commissioner welcomes any effort by industry to align commonly understood terms and practices, particularly where legal requirements apply (eg UK data protection law, or privacy legislation in other jurisdictions). This will not only assist organisations when assessing the data protection compliance of any proposals that involve personal data, but also individuals in understanding what happens to their data.

4.1.3 First- and third-party in the context of data categories

The second type of use relates to categorisations certain industries and sectors apply to data. These include:

---

[100] https://tess.oconnor.cx/2020/10/parties

[101] https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/what-are-cookies-and-similar-technologies/#cookies4. The Commissioner observes that over time, resources historically served by third party cookies are being delivered via a first party cookie, even if the resource itself remains external to the online service, which further complicates use of the terms.

[102] See footnote 100 above.

- "first party data", regarded as data relating to direct interactions between an individual and an organisation;
- "second party data", which is essentially one organisation's first party data that another organisation purchases; and
- "third party data" is data purchased from sources that were not the original collectors of it, such as data brokers or aggregators[103, 104].

For example, in the context of first party data, online services such as publishers have direct relationships with individuals. For example, where they are customers of the service the publisher provides. In situations like these, publishers process the personal data of those individuals. They may wish to leverage the 'customer relationship' for several purposes. For example, to gain insights into their customer base, to personalise services, or to target adverts.

However, from a data protection perspective, these categories can all involve personal data. The only relevance is about the specific aspects of data protection law that apply[105]. It is a matter for the publisher, in its role as a controller, to determine which of these provisions apply in the context of the personal data it processes and any industry-defined terms it follows. When it does, it must consider the specific circumstances and the requirements of data protection law.

For example, when a publisher shares personal data that it classes as first party data available with another organisation (thereby making such data second party data from that organisation's perspective). Then, both the publisher disclosing that data and the organisation receiving that data have obligations under data protection law. These include ensuring that the processing is fair, lawful and transparent. This is so individuals know what will happen to their personal data and are given meaningful control, subject to the requirements of the law.

Data protection law does not prevent organisations sharing personal data. It facilitates fair and proportionate data sharing, as the ICO's data sharing code of practice describes[106]. The important point is that however an organisation categorises personal data, the processing must be done in line with the law. Organisations must ensure they comply with the data protection principles, and consider any risks of harm that may arise from that processing and mitigate them appropriately.

[103] https://dma.org.uk/uploads/misc/third-party-data-guide-1.0.pdf
[104] https://www.lotame.com/1st-party-2nd-party-3rd-party-data-what-does-it-all-mean/
[105] For example, in the context of transparency requirements, Article 13 of the UK GDPR applies to personal data obtained from an individual. Article 14 applies to personal data not obtained from an individual. This applies irrespective of any industry terminology or categorisations the publisher uses.
[106] https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-code/

4.1.4 First- and third-party in the context of law and regulations

The third use relates to laws and regulations. It is most obvious in contract law. For example, a contract is an agreement binding two or more parties (ie the parties to the agreement). A third party is a party not bound to the contract.

The term also exists in data protection law. For example, Article 4(10) of the UK GDPR says:

Quote

"'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data."

In data protection terms, persons who are authorised to process personal data generally refers to persons that form part of the legal entity of the controller or processor (ie an employee or comparable role), insofar as they are authorised to process personal data. In general, a third party is anyone who, in the circumstances, is not a data subject, controller, processor or employee. The term essentially describes a relation to a controller or processor from a specific perspective.

It is also relevant to observe that a third party who receives personal data would in principle be a controller in its own right for the processing it carries out for its own purposes.

The Commissioner cannot comment directly on the inclusion of the term in the laws of other jurisdictions, other than to note that these definitions are not necessarily identical to each other[107].

4.1.5 Summary

Data protection law does not inherently favour the concept of a first party over that of a third party within the meanings web standards bodies or data categorisations give to those terms. The distinctions are relevant insofar as they may relate to:

- the processing activities being undertaken;
- identifying the role of an organisation involved in that processing (eg who is responsible for determining the purposes and means of that processing); and

[107] The definition of a third party in the Colorado Privacy Act has similarities with that in the UK GDPR, while the definition in the CCPA is different.

- the risks the processing poses to the rights and freedoms of individuals, and how these are considered.

The Commissioner reiterates that data protection law places obligations on the entity or entities that determine the purposes and means of the processing of personal data. The entity responsible for such decisions is the controller for that processing. It is that entity which is responsible for demonstrating how it complies with the requirements of the law. This is the case regardless of:

- where the controller sources the personal data (ie, direct from an individual, or from elsewhere); and
- whether the controller is a large technology platform with multiple services, or a single organisation that seeks to share personal data with other organisations.

In any scenario the key data protection considerations are:

- whether the information is personal data;
- who is responsible for determining the purposes and means of the processing;
- whether the processing is fair, lawful and transparent (ie, what were individuals told when their data was collected); and
- the purpose(s) for which the data is intended to be processed.

The focus should be on the nature of the risks involved, and their likelihood and severity. In practice this depends on the circumstances of the processing activities. For example, risks to the rights and freedoms of individuals arise whether personal data is processed in a "first-party" context or in a "third-party" context, however organisations seek to apply those terms. The specifics of these risks may differ (eg because the circumstances of the processing may also differ) but it is not necessarily the case that one has a lower risk than the other.

It is for the organisations responsible for the processing to assess and mitigate these risks in either scenario. This applies in any context, including proposals such as the GPS or those from other market participants.

4.2 Purpose limitation

The purpose limitation principle in the UK GDPR provides that personal data shall be:

Quote

"collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes"

This means organisations must:

- be clear from the outset about why they are collecting personal data;
- inform individuals about these purposes (whether the data is obtained directly from them or not); and
- ensure that if they plan to process personal data for purposes other than those originally specified, the new use is fair, lawful and transparent.

Purpose limitation means that an organisation cannot do what it likes with personal data once it has collected it. Any organisation that collects personal data must implement this principle effectively, irrespective of the corporate structure it operates within. It must ask not just "Can we do this?" but "Should we do this?". This is the case whether what is being referred to is sharing data with another organisation or disclosing it to other business units to use for new or different purposes. DPIAs are an effective way to consider these questions.

The principle specifically intends to guard against "function creep" as well as harms arising from misuse or risks of invisible processing.

PECR also sets out purpose specification requirements in the context of the use of cookies and similar technologies. For example, an organisation must tell individuals about the purposes for which it wants to store (or gain access to information stored) in their devices. The purposes also determine whether an exemption applies (eg where the storage or access is strictly necessary to provide the online service[108]).

More generally, data protection law does not prevent organisations using data collected for one purpose for a different purpose. However, there are restrictions. If the purposes change over time, or if the organisation wants to use data for a new purpose, then it can only go ahead if:

- the new purpose is compatible with the original purpose;
- it gets specific consent for the new purpose; or
- it can point to a specific and clear legal provision requiring or allowing the new processing in the public interest[109].

There are some purposes that are always considered compatible with the initial purpose[110]. However, purpose compatibility will not always permit reuse of personal data in the context of online advertising, particularly where consent is required under PECR (as described in Section 3.1 above).

[108] See Regulation 6 of PECR and the Commissioner's guidance on the use of cookies and similar technologies.
[109] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/
[110] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/#compatible_purpose

If an organisation is trying to decide whether a new purpose is compatible with the original purpose, it must consider several factors. These include:

- the context in which the data was originally collected;
- the relationship it has with the individual;
- the individual's reasonable expectations;
- the consequences of the new processing; and
- the available and appropriate safeguards, whose impact the controller must fully assess (eg by a DPIA).

In general, if the new purpose is unexpected or would have an unjustified adverse impact on the individual, it is likely to be incompatible unless the organisation gets specific consent. "Repurposing" in this context would be unlawful.

4.3 Internal disclosure and external data sharing

The Commissioner is aware of a related perception from some market participants that data protection law enables large corporate entities to consolidate their access and ability to use personal data. For example, that the law allows these entities to have an unfettered ability to process this data once they obtain it (eg by relying on legitimate interests as a lawful basis). In the context of online tracking this can sometimes be characterised as enabling platforms to track individuals across multiple services, or otherwise use personal data in ways that smaller market participants may not be able to.

As noted in the ICO and CMA joint statement, this perception is a key concern from a competition law perspective but can also raise data protection concerns[111]. For example, the risks of harm arising from power and information asymmetry between individuals and large platforms.

However, data protection law does not automatically enable this notion of unfettered processing. While legitimate interests is the most flexible lawful basis for processing, organisations cannot assume it is the most appropriate one[112]. If they do rely on legitimate interests, they take on extra responsibility for considering and protecting people's rights and interests.

There are three elements to legitimate interests, and it can help organisations to think of this as a three-part test. They need to identify a legitimate interest ("purpose test"), show the processing is necessary to achieve it ("necessity

[111] https://ico.org.uk/media/about-the-ico/documents/2619797/cma-ico-public-statement-20210518.pdf, paragraphs 77 to 83.
[112] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/

test") and balance it against individuals' interests, rights and freedoms ("balancing test").

The specifics of the three-part test require organisations to undertake a case-by-case assessment of the relevant facts. A legitimate interests assessment is one way they can do this[113].

The Commissioner also observes that any legitimate interests assessment should include considerations of other laws that apply. For example:

- one of the questions in the Commissioner's guidance about the purpose test is "Are you complying with other relevant laws?"[114];
- when describing what counts as a legitimate interest, the Commissioner's guidance states that "anything illegitimate, unethical or unlawful is not a legitimate interest"[115]; and
- the Commissioner's guidance on the principle of lawfulness, fairness and transparency also notes that "Lawfulness also means that you don't do anything with the personal data which is unlawful in a more general sense. This includes statute and common law obligations, whether criminal or civil".[116]

Organisations may be able to process data in the context of intra-group transmission or sharing with other organisations if the disclosure is fair and compatible with the original purpose. As noted in Section 4.2, the disclosing entity needs to justify the disclosure. The receiving entity needs to justify its own processing, taking into account how it received the data. However, data cannot be passed on for a new purpose – internally or externally – if doing so would be incompatible with the original purpose, considering the circumstances.

Additionally, interpretive guidance in the recitals of the UK GDPR about intra-group transmission for internal administrative purposes[117] does not mean an organisation can always rely on legitimate interests for this type of processing. The term "internal administrative purposes" does not have broad application, as indicated by the ordinary meaning of the words. Transmission for other purposes is outside this situation (eg for new commercial purposes).

---

[113] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/

[114] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/#LIA_process, "1. How do we do the purpose test?"

[115] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/#what_counts

[116] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/

[117] See Recital 48 of the UK GDPR. Recitals do not have the status of legal rules. They provide interpretation about the purpose of the legislation. See https://www.legislation.gov.uk/ukpga/2018/16/notes/division/14/index.htm.

The Commissioner notes that:

- an organisation that is part of a group may seek to rely on legitimate interests in the context of intra-group transmission of personal data, provided it undertakes the three-part test appropriately;
- when doing a legitimate interests assessment, the organisation needs to take into account any relevant legal frameworks that may apply to its circumstances; and
- if the intra-group transmission has the effect of infringing any applicable law which applies to the organisation, then the purpose it has identified does not count as a legitimate interest.

Organisations may still be able to rely on legitimate interests, just not for these purposes. They must identify the specific purpose, and consider the necessity and balancing tests in that context.

In any event, organisations must also consider the role of PECR. For example, PECR may require them to have consent (eg because processing activities involve the use of cookies and similar technologies).

The ICO continues to work with the CMA to ensure that data protection law informs market assessments about these issues.

4.4 "Privacy as a shield"

The Commissioner is also aware that the above perceptions may lead to a risk that data protection law is viewed as enabling large, integrated technology platforms to, in essence, use privacy as a "shield". For example, to prohibit data sharing with other organisations on the basis that doing so conflicts with data protection legislation.

As described above, data protection law:

- enables fair and proportionate data sharing (eg as a way of increasing trust and as a driver of greater choice for individuals, innovation, competition and economic growth); and
- requires that personal data is collected for specific purposes, and not further processed in a manner incompatible with those purposes.

In this regard, the ICO's data sharing code of practice guides organisations through the steps they need to take to share data while protecting privacy and upholding individual rights. It provides a practical framework to help

organisations make decisions about sharing data, and clears up misconceptions[118].

The Commissioner also notes that there are examples of data sharing in the digital economy that are undertaken in line with the data protection principles. For example, Open Banking involves sharing individuals' financial data with other organisations[119]. Individuals have control over this sharing, and it only happens with permission.

The ICO and CMA joint statement referenced potential data access interventions, which would aim to promote competition outcomes by requiring access to types of data so that smaller businesses or new entrants could compete. Both regulators also described the importance of designing any such interventions in a way that aligns with data protection law[120].

Ultimately, the adtech ecosystem must address the significant accountability weaknesses in the way data is made available to market participants, as outlined in the 2019 report.

It is also the case that the organisations should consider whether the requirements of competition and data protection law can be met without sharing personal data.

[118] https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/about-this-code/?q=upheld#misconceptions
[119] https://www.openbanking.org.uk/.
[120] https://ico.org.uk/media/about-the-ico/documents/2619797/cma-ico-public-statement-20210518.pdf, paragraphs 70 to 75.

5. The Commissioner's expectations

As organisations continue to evolve their proposals, the Commissioner believes that market participants should develop solutions that are focused on the interests, rights and freedoms of the individual. These should move away from intrusive tracking technologies that may continue to pose risks and struggle to comply with the law.

Solutions should aim to achieve privacy-respectful and pro-competition outcomes for both individuals and businesses. They should embody the core concepts of data protection by design and by default, and not reinforce or replicate intrusive practices.

Market participants developing solutions should consider how they will apply these principles and recommendations. This includes not just at the design stage, but where they or other organisations may deploy those solutions.

5.1 Principles

The Commissioner expects any solution, proposal or initiative to meet the following expectations. They link to the core principles and provisions of data protection law. They help to support key considerations for design, documentation, accountability and auditability.

A. **Data protection by design:** Individuals' interests, rights and freedoms should sit behind any design proposal. Market participants should consider how they will evidence their assessment of this during the design of their products, services and applications (eg in how they implement the data protection principles effectively).

B. **User choice:** Individuals must be offered the ability to receive adverts without tracking, profiling or targeting based on personal data, eg contextual advertising that does not require any tracking of user interaction with content. Where individuals choose to share their data, they must have meaningful control and the ability to fully exercise their information rights. Market participants should evidence a high privacy, no tracking by default option, and demonstrate how user choice can be exercised throughout the data lifecycle.

C. **Accountability:** There must be accountability across the full lifecycle of the processing and supply chain, with transparency about how and why personal data is processed across the ecosystem and who is responsible for that processing. This must be transparent to the user. Market participants should evidence how accountability will work across the supply chain.

D. **Purpose:** The design of the proposals must clearly articulate the specific purposes for processing personal data and demonstrate how this is fair, lawful and transparent. Market participants should assess the necessity and proportionality of this processing in the context of those purposes, and demonstrate how their proposals uphold the integrity of the purpose limitation principle.

E. **Reducing harm.** The proposals must address existing privacy risks. As far as is practicable, they must also consider any new risks they introduce, and how they will mitigate them before any processing takes place. Market participants should evidence how they identify privacy risks in their proposals and how they mitigate them (eg by DPIAs).

5.2 Recommendations

The principles above should be considered holistically. Any proposals should explicitly demonstrate how they are being applied. The following recommendations provide further specific guidance for consideration. They can also form key considerations for DPIAs. Developers of products, services and applications should ensure their proposals enable any controller that adopts them to implement the data protection principles effectively and integrate necessary safeguards into the processing.

5.2.1 Demonstrate and explain the design choices

- Clearly describe the solution's architectural design decisions, how these were made, and the data flows concerned.
- Objectively detail the risks posed to individual rights and how these are mitigated.
- Use the least privacy intrusive approach possible to achieve the purpose. Justify all design choices made.
- Consider how different components or technologies will interact and the aggregate impact on data protection and privacy.
- Make any service requirements and objectives available to all parties, including regulators.
- Ensure the solution enables organisations that use it to implement the data protection principles effectively and integrate necessary safeguards into its processing.

5.2.2 Be fair and transparent about the benefits

- Explain the benefits and outcomes the solution seeks to achieve, including the use cases it seeks to address.
- Articulate the benefits from the user's perspective as well, considering their reasonable expectations.

- Be fair, accessible and transparent both to individuals using the web, as well as organisations on the web. Demonstrate how the design process ensures the user experience delivers in practice, and avoids dark patterns and nudge techniques.
- Where benefits for one group of stakeholders may give rise to tensions with another, be clear on how the solution's design manages these in ways that comply with data protection outcomes.
- Ensure the solution enables organisations that use it to provide clear and comprehensive information about the processing activities, how they work, and their purposes.

5.2.3 Minimise data collection and further processing

- Ensure the solution processes the minimum amount of data necessary to achieve its purposes. As a general rule, contextual-based advertising allows most readily for compliance with the data protection principles.
- Consider whether the outcomes can be achieved without using personal data at all. If the solution requires personal data, it must explain why, as well as the steps taken to identify and mitigate risks, and ensure that new risks are not introduced.
- The solution must be designed so that an organisation using it can identify a specific, explicit and legitimate purpose for the processing activities.

5.2.4 Protect users and give them meaningful control

- The solution should demonstrate how it reduces tracking vectors and addresses re-identification risks.
- Ensure the solution is engineered so that confidentiality, integrity and availability are built-in. Apply appropriate security techniques to secure the data both on-device, in-transit and server-side.
- Ensure the solution allows individuals to exercise their rights, whether by browsers, software settings or applications. Demonstrate how it considers the user journey at all aspects of design and development.
- Process data for the minimum amount of time necessary.
- Ensure the solution avoids augmenting, matching or combining personal data without strong justification, transparency and control.
- Ensure the solution allows organisations that use it to obtain freely given, specific, informed and unambiguous consent from individuals, and that consent is as easy to withdraw as it is to give.
- Where possible, design the solution to promote approaches that strengthen user control over the processing.

5.2.5 Necessity and proportionality

- The solution must enable organisations that use it to demonstrate that it is a targeted and effective way to achieve their purpose, and the benefits to the organisations are not disproportionate to any risk to privacy rights.
- It must also assist those organisations in demonstrating they cannot reasonably achieve the purpose using a less intrusive method, and that they are able to justify any impact on individuals.

5.2.6 Lawfulness, risk assessments and information rights

- The solution must allow organisations that use it to identify the appropriate lawful basis and meet its requirements.
- The solution should help those organisations recognise where PECR requires consent and ensure that this consent meets the UK GDPR standard.
- Consider how the solution enables organisations that use it to undertake a DPIA, and allows them to assess the impacts of the processing on the rights, interests and freedoms of individuals.

5.2.7 Special category data

- The solution must address the potential for processing of special category data. It should mitigate any risks of creating or inferring this data unless strictly necessary for the purposes.
- If special category data is processed, the solution must allow the organisation using it to identify the appropriate condition from Article 9 (in addition to a lawful basis under Article 6). Any approach must recognise that consent required under PECR is not explicit consent under Article 9 of the UK GDPR, and the public interest conditions do not apply.
- Where the solution processes personal data to put individuals into groups (eg cohorting or segmentation), the risk of those individuals being placed into protected or vulnerable groups must be clearly identified and safeguarded against.

Ultimately, new online advertising proposals should improve trust and confidence in the digital economy, instead of weakening it. Solutions should be privacy-respectful while ensuring they give due consideration to other relevant laws. They should not replicate or seek to maintain practices that do not comply with the law. They also should not introduce additional privacy and security risks for users, with these being addressed and mitigated prior to the solution's deployment.

6. Conclusions and next steps

The Commissioner welcomes proposals to remove the use of technologies that lead to intrusive and unaccountable processing of personal data and device information, which increases the risks of harm to individuals.

The Commissioner acknowledges that a variety of proposals are under development to address privacy and data protection issues arising from cookies and similar technologies. In many cases, these proposals are under active development and are subject to frequent change. The Commissioner reserves the right to address specific proposals in more detail as appropriate. For example, when they become more stable and once a greater level of consensus is achieved among stakeholders.

However, the Commissioner reiterates that participants within the online advertising industry should not wait until proposals like the GPS reach a more stable point. The principles of data protection by design and by default already apply. Market participants should build these into any solution or technology they currently use to achieve their objectives. Those responsible for the processing activities must demonstrate accountability with the requirements of the law.

Participants should note that continued use of intrusive online tracking practices is not the right way to develop solutions. Anything that essentially results in a continuation of existing practices will not meaningfully change the status quo.

Industry must recognise the need for change. It should understand that the Commissioner does not advocate for alternatives that use the same fundamentally flawed approaches. Solutions that seek to continue "business as usual", through which existing practices are essentially maintained by revised or new frameworks, technologies or contractual arrangements will not:

- satisfy this expectation;
- meet the requirements detailed in the 2019 report; or
- result in fair outcomes for both individuals and businesses on the web, (eg due to non-compliance with data protection and PECR requirements).

The Commissioner acknowledges the importance of ensuring effective competition across the digital economy. However, privacy-positive developments should be sustained and amplified in this context, not eroded in the interests of creating "better" market dynamics. The Commissioner will continue to work closely with the CMA on this. For example, by:

- the continuing assessment of the GPS proposals put forward by Google; and

- by ensuring the data protection and privacy assessment of developments in the web and mobile ecosystems are considered in partnership with the CMA's assessment of competition impacts.

A healthy market is one built on data protection by design, enabling privacy-respectful innovations focused on the individual's interests, rights and freedoms. Meaningful choices benefit individuals and underpin effective competition between businesses. Proposals looking to replace the use of cookies and similar technologies need to ensure that they raise the standards of data protection and privacy, and not dilute them.

The Commissioner requires those developing new proposals to:

- be able to demonstrate that they meet the key expectations in this Opinion;
- understand the broader data protection impacts; and
- build data protection by design and by default into their solutions.

The Commissioner reserves the right to make changes or form a different view based on further findings, changes in circumstances and engagement with stakeholders. The Commissioner will keep these expectations under review, as proposals continue to develop.

The Commissioner is therefore open to receiving further input, in particular to:

- assist understanding of these developments from a data protection perspective;
- help market participants developing technical solutions to better understand how to build data protection by design and default into their services; and
- help those participants understand the broader data protection impacts of their proposals.