The CMA's response to the European Commission's public consultation on the evaluation and review of the ePrivacy Directive

1. The Competition and Markets Authority (CMA) is the United Kingdom's lead competition and consumer enforcement authority which works to promote competition for the benefit of consumers, both within and outside the UK.

2. The CMA welcomes the opportunity to respond to the consultation on the evaluation and review of the ePrivacy directive.

3. We respond only to questions 22 to 24 of the consultation as these relate to issues where we have particular experience as a competition and consumer authority. The consultation raises a number of issues which fall outside our remit and we do not address these in our response.

Question 22

The practice of websites to deny access to those users who refuse to accept cookies (or other technologies) have generated critics that citizens do not have a real choice. To what extent do you agree to put forward the following measures to improve this situation?

	Strongly agree	*Agree*	*Disagree*	*Strongly disagree*	*Do not know*
Information society services should be required to make available a paying service (without behavioural advertising), as an alternative to the services paid by users' personal information			X		
Information service providers should not have the right to prevent access to their non-subscription based services in case users refuse the storing of identifiers in their terminal equipment (ie identifiers not necessary for the functioning of the service)			X		

The CMA's response to question 22

Role of the CMA

4. The CMA is not the UK's privacy or data protection authority (that role belongs to the Information Commissioner's Office) but has the role to promote competition to make markets work well for consumers, businesses and the economy. Nonetheless business practices in this area have the potential to promote or restrict competition and it is in this capacity that we respond to this part of the questionnaire.[1]

Information society services should be required to make available a paying service (without behavioural advertising), as an alternative to the services paid by users' personal information

5. We make the general point that, in practice, there is generally not a binary choice between monetary payment and 'payment' by personal data (as the question may suggest): businesses may collect monetary payment **and** data in the same transaction, and (conversely) consumers may be prepared to money and/or data in exchange for services. The position may be quite complex in practice but different consumers may be prepared to disclose different levels of data to different parties in exchange for different services or benefits, as illustrated below.

Examples of money/data exchange

- Some consumers may be prepared to pay a monetary price for a service and disclose no data (other than that necessary to supply the service). This may appeal to consumers with a strong privacy sensibility (who do not wish to share personal data regardless of any economic benefits).
- Some consumers may be happy to share any data about themselves where they see economic or other benefits to such data exchange (for example where it gives access to 'free' services, better targeted adverts which the consumer wants etc).
- Some consumers may be willing to share certain data only with certain parties for certain purposes only, for example a consumer may be prepared to share data with a first party retailer for future advertising by that retailer but not with third party data brokers.

[1] We also do not therefore here consider the potential impact of the General Data Protection Regulation on, for example, the obligations relating to profiling.

6. As a matter of general principle, additional burdens should only be placed on businesses if justified. On the basis of existing evidence and, taking into account the development of nascent innovative business models and the risks and costs of intervention, it appears to us to be disproportionate to *require* businesses to offer a 'paid for' alterative at this stage. In particular, SMEs may not have the technical ability or resources to establish alternative mechanisms and this may result in them withdrawing services.

7. In our view, the provision of consumer data for services is a form of value exchange the benefits of which should be shared between consumers and businesses. It is, however, very difficult to establish a monetary 'price' since this may be different for different consumers and transactions (even for the same products). Rather than compel suppliers to offer alternative means of payment, we would rather encourage greater transparency and choice over data collection and use/privacy policies to enable consumers to make a genuine choice how much data, if any, to allow the business to collect. This may drive competition by enabling consumers to shop around and reward businesses which best serve their needs.

8. Consumers should be clearly informed what data businesses collect, and what they intend to do with it, so that they can make an informed decision about whether to proceed. Without this, consumers will remain at a disadvantage and be hindered from assessing whether the transaction is one they are prepared to enter into. Requiring a paid for option would not address this issue the consumer will be similarly unable to assess whether the paid for option is better for them than the data collection option, and may be exposed to the risk of misunderstanding what data is being collected even where they opt for the paid for option.

9. Finally, even where a paid for option is offered, it may not follow that the supplier collects no data about the consumer,[2] and there is a real risk that less scrupulous suppliers take the money AND collect data about the consumer. In some circumstances they may do this with the apparent consent of the consumer, which the consumer may give because they do not understand the transaction. Accordingly, the position for consumers may become worse.

[2] We refer to data which is not essential to the immediate service being requested. The supply of certain data may be necessary to supply the service being requested.

Information service providers should not have the right to prevent access to their non-subscription based services in case users refuse the storing of identifiers in their terminal equipment (ie identifiers not necessary for the functioning of the service)

10. On the question whether ISS should not have the right to prevent access to non-paying consumers who refuse to allow the storage of non-essential cookies, we are not aware that this practice is widespread and, as such, in the absence of clear harm, it would appear difficult to justify regulatory change (although the impact on the market should be kept under review).

11. As a matter of principle, businesses should generally be free to decide with whom to contract and under what conditions, subject to applicable law. In the case of a trader whose business model is to provide 'free' services in exchange for data, clearly if consumers were able to access such services without offering a 'counter-performance' of data, the ability of the trader to continue to offering such services may decline. There may therefore be an incentive to refuse access to services (subject to wider commercial and reputational considerations).

12. If businesses wish to prevent access to services to consumers who refuse non-essential cookies and similar technologies, in our view, it is important that consumers should clearly understand the basis of this exchange, and not be misled.

Question 23

As a consumer, do you want to be asked for your consent for the processing of your personal data and other information stored on your smart devices as regards the following? Select the option for which you want to be asked for your consent (several options possible):

(a) Identifiers placed/collected by a third party information society service (not the one that you are visiting) for online behavioural advertising purposes

(b) Identifiers placed/collected by an information society service you are visiting – when their purpose is website analytics, measuring number of website visitors, where visitors go within the website, etc. (eg. 'first party' cookies or equivalent technologies)

(c) Identifiers placed/collected by an information society service you are visiting whose purpose is to support user experience, such as language preference cookies [1]

(d) Identifiers collected/placed by an information society service to detect fraud

(e) Identifiers collected/placed by an information society service for frequency capping (number of times a user sees a given ad)

(f) Identifiers collected and immediately anonymised in a way that it is impossible to identify the users' device

(g) Other

[1] See Article 29 Working Party Opinion 04/2012 on Cookie Consent Exemption of 07.06.2012

The CMA's response to question 23

13. We considered questions of consent for different types of cookies in our report on the Commercial Use of Consumer Data (CUCD).[3] In our report, we broadly categorised the types of cookies as necessary, functional, performance-related and advertising- related. The descriptions in categories *(a)* to *(f)* above would, in our view, fall broadly within similar categories (*(a)* and *(e)* are advertising-related, *(b)* and *(d)* are performance-related, functional, *(c)* is functional and *(f)* could fall within different categories).

14. While we did not undertake an analysis of consumer preferences in the above report, we considered existing business practices in relation to the application of the existing 'cookie law'. (See, for example, paragraphs 2.32ff. and 4.141ff in the CUCD report). The evidence we considered suggested that consumers have different levels of concern depending on the purpose of the cookie in question. In particular, although each case must be considered separately, broadly there was some evidence that cookies which are necessary, functional, and performance-related were found to be less of a cause of concern than some advertising cookies – particularly when data is anonymised. The evidence also suggested that some consumers were uncomfortable with advertising cookies set by third parties, particularly when the consumer may not clearly be aware of the existence and privacy policy of the third party (again, whether or not the data is anonymous is a factor in levels of concern).

15. We considered the question of how far the existing mechanism to obtain consent through a 'cookie notice' is sufficient to generate trust in the market. In general, we found that cookie notices did not empower consumers to have control over the different types of cookies involved. In particular:

    (a) Cookie notices generally do not differentiate between the different types of cookies and so do not allow consumers to apply different consents to

---

[3] The CMA's report on the Commercial Use of Consumer Data (June 2015).

them (that is, consents are 'bundled' for all types of cookies). In our view, consumer control would be enhanced if the consents were differentiated or graduated so that consumers could choose, for example, to consent to a functional cookie but not consent to a third party cookie (see paragraph 4.149 of the CUCD report).

(b) Cookie notices purport to seek consent although, in practice, the cookie has already been 'dropped' on to the consumer's device. The consumer therefore has to remove the cookie afterwards which is not always straight-forward.

16. We noted, however, that there are examples of practices which enable consumers to exercise greater choice over the setting of cookies (for example of graduated consent). We also noted market developments to improve consumer control, including privacy dashboards and self-regulatory initiatives. See in particular paragraph 4.141ff and 5.44ff of the CUCD report.

17. We would note in addition that, although the e-Privacy Directive (as implemented in the UK by the Privacy and Electronic Communications (EC Directive) Regulations 2003) applies to cookies and similar technologies, there are other means by which traders can identify information about website users (including their route into the website, device used, location), which may be used in principle for targeted pricing, and other analytical activities – not just targeted advertising. Therefore any legislative proposal should take into account the full range of technological means, and be future proofed, and take into account the full range of purposes which website operators may use information collected for.

Question 24

It has been argued that requesting users' consent to the storage/access of information in their devices, in particular tracking cookies, may disrupt Internet experience. To facilitate this process and users' ability to consent, a new e-Privacy instrument should (several options possible):

- Require manufacturers of terminal equipment including operating systems and browsers to place on the market products with privacy by default settings (eg third party cookies off by default)

- Adopt legislation, delegated acts for example, defining mechanisms for expressing user preferences regarding whether they want to be tracked

- Mandate European Standards Organisations to produce standards (eg Do Not Track; Do not Store/Collect)

- Introducing provisions prohibiting specific abusive behaviours, irrespective of user's consent (eg unsolicited recording or filming by smart home devices)
- Support self-co regulation
- Others

The CMA's response to question 24

18. Consumers seek both convenience and privacy protections when dealing with traders. We consider it imperative that traders respect the fundamental rights of consumers under privacy and data protection laws and, as far as possible, recommend that this is achieved in a way that helps consumers make competitive choices.

19. As regards the proposals set out here, we make the following observations:

    (a) **Privacy by default settings** – We would welcome the introduction of flexible mechanisms for consumers to exercise choice and control which could enable them to make decisions according to their individual preferences. This may include appropriate default settings but there needs to be balance to ensure that the protections do not stifle innovation.

    (b) **Legislation defining mechanisms for expressing user preference** – Our concern here would be both future-proofing and also ensuring that any mechanism is sufficiently flexible to ensure a 'seamless' experience.

    (c) **Standard setting** – We would support proposals to set appropriate standards although, as set out above, great care must be taken not to stifle innovation that could benefit consumers.

    (d) **Prohibiting specific abusive behaviours, irrespective of user's consent** – In our view, such legislative measures should only be put in place if they are shown to be necessary to address harm which cannot otherwise be addressed by existing regulations or self-regulation. Such measures should be based on an evidenced assessment of harm.

    (e) **Self-regulation** – As outlined in our CUCD report, self-regulation can play an important part in raising standards for consumers in this area and we would support such initiatives.

5 July 2016