epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

UNITED KINGDOM INFORMATION COMMISSIONER'S OFFICE

Regarding the

ICO Call for Views on "Consent or Pay" Business Models

April 17, 2024

By notice published March 6, 2024, the United Kingdom's Information Commissioner's Office ("UK ICO" or "the ICO") has called for views regarding "consent or pay" business models (hereinafter "the Consultation") to close on April 17, 2024.[1] This Consultation is intended to address an emerging business model where individuals are blocked from accessing a website unless they consent to their personal information being processed for the purpose of targeted advertising, or, as the ICO puts it, "pay a fee and not be tracked." [2] Pursuant to this call for views, the Electronic Information Privacy Center ("EPIC") submits the following comments.

EPIC is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to secure the fundamental right to privacy in

[1] Information Commissioner's Office, *Call for views on "consent or pay" business models*, (Mar. 06, 2024), https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/call-for-views-on-consent-or-pay-business-models/ .
[2] *Id.*

the digital age for all people through advocacy, research, and litigation.[3] EPIC has long advocated for robust safeguards to protect consumers from exploitative data collection, use, distribution, and retention practices both in the United States and abroad. EPIC has filed amicus briefs,[4] regulatory comments,[5] and supported legislation with comprehensive data minimization provisions[6] to protect consumers from commercial surveillance regimes.

EPIC supports the ICO's efforts to address the harms stemming from "consent or pay" business models. However, conditioning provision of a service on consent to processing data (including sensitive categories of data) when the processing of that data is not strictly necessary to the provision of the service facially violates the United Kingdom General Data Protection Regulation ("UK GDPR") and infringes UK citizens' fundamental right to privacy and data protection. The ICO should prohibit the use of "consent or pay" business models.

I. Consent is a facially invalid basis for processing data under "consent or pay" business models.

a. Consent is valid when it is freely given, unambiguous, specific, and informed.

[3] EPIC, *About Us* (2024), https://epic.org/about/.
[4] Brief of Amicus Curiae EPIC Supporting Plaintiffs-Appellants and Reversal, Calhoun et al., v. Google, LLC., Case No. 20-cv-5146-YGR (2022), https://epic.org/documents/calhoun-et-al-v-google/ ; Brief of Amicus Curiae EPIC Supporting Plaintiffs-Appellants, Smith v. Facebook, Inc., 745 F. App'x 8 (9th Cir. 2018), https://epic.org/wp-content/uploads/amicus/facebook/smith/EPIC-Amicus-Brief-Smith-v-Facebook.pdf.
[5] Comments of EPIC, *Regarding the ICO Consultation on the Draft Biometric Data Guidance,* Identity and Trust Team (Technical Policy) of the UK ICO (Oct. 20, 2023), https://epic.org/documents/epic-comments-to-the-uk-icos-office-for-the-consultation-on-the-draft-biometric-data-guidance/; Comments of EPIC, *Regarding the Request for Information Regarding Data Brokers and Other Business Practices Involved in the Collection and Sale of Consumer Information*, Consumer Financial Protection Bureau (Jul. 14, 2023), https://epic.org/documents/comments-of-epic-on-cfpb-request-for-information-regarding-data-brokers-and-other-business-practices-involving-the-collection-and-sale-of-consumer-information/ ; Comments of EPIC, *Disrupting Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystem*, Federal Trade Commission (Nov. 2022), https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf (hereinafter "Disrupting Data Abuse Report").
[6] EPIC, *Maryland General Assembly Passes Maryland Online Data Privacy Act* (Apr. 6, 2024), https://epic.org/maryland-general-assembly-passes-maryland-online-data-privacy-act/; *see also* EPIC, *A Proposed Compromise: the State Data Privacy and Protection Act* (Feb. 22, 2023), https://epic.org/a-proposed-compromise-the-state-data-privacy-and-protection-act/ .

Under the UK GDPR, it is illegal to process personal data unless one of the six lawful bases for processing data is met.[7] Consent is one such lawful basis for processing. For consent to be valid, though, it must be "freely given, specific, informed, and unambiguous."[8] Special categories of data, such as political opinions and health data, require both a lawful processing basis under Article 6 of the UK GDPR as well compliance with additional processing conditions under Article 9.[9] One of the additional condition options is explicit consent, which carries the same high standards as consent under Article 6.[10] Lastly, there are "no global rules on children's consent" under the UK GDPR, but generally, an entity must acquire parental consent to process the personal data of children under 13.[11]

Consent is freely given when people are given "genuine choice and control over how [the controller uses] their data."[12] People must be able to "refuse consent without detriment" and "withdraw consent easily at any time." Detriment is not defined in the UK GDPR.[13] Consent is explicitly presumed to not be freely given if "the performance of a contract, including the provision of a service, is conditional on [that] consent despite such consent not being necessary for such performance."[14] The UK ICO guidance further specifies that the entity desiring to process the personal data is responsible for rebutting the presumption of invalidity when the requested consent is made a precondition to providing a service and processing is not "strictly necessary[.]"[15] Controllers can do so by providing a "very clear justification" based on its specific circumstances.[16] Therefore,

[7] United Kingdom General Data Protection Regulation (hereinafter "UK GDPR") Article 6(1).
[8] UK GDPR Article 4.
[9] UK GDPR Article 9.
[10] *What is valid consent?,* United Kingdom Information Commissioner's Office, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/what-is-valid-consent/ (stating that explicit consent has the same requirements as Article 6 consent).
[11] *Id.*
[12] *Supra* note 10*; see also* UK GDPR Recital 42.
[13] *Supra* note 10.
[14] UK GDPR Recital 43; Article 7(4).
[15] *Supra* note 10.
[16] *Id.*

conditioning performance on consent to process personal data is facially invalid unless the purpose for processing the personal data is strictly necessary to provide the service.

Consent is specific and informed when the information given to the data subject at the time of requesting consent includes the data controller's identity, the purpose of the processing, the processing activities, and fact that users have the right to withdraw consent at any time.[17] This includes listing any third party data controllers who will rely on the consent.[18] When a website engages in targeted advertising, it needs to inform the data subject of all the parties it is selling or otherwise disclosing the data subject's personal data to. The request for consent must be "prominent, concise, separate from other terms and conditions, and in plain language."[19] Language that is "likely to confuse . . . will invalidate consent."[20] If the purpose for processing the data "evolve beyond what [is] originally specified[,]" then the controller must refresh the request for consent.[21]

Unambiguous consent must be a "clear signal that [the data subject] agree[s]."[22] Silence, inactivity, and failure to opt-out do not constitute valid consent.[23] The individual must "deliberately and actively [choose] to consent."[24] Consent is also "likely to degrade over time," but the UK GDPR does not set a time limit for when that might occur.[25] The scope of the original consent and the individual's expectations should be guiding factors for when consent needs to be reviewed and refreshed.[26]

[17] *Supra* note 10; UK GDPR Recital 42.
[18] *Id.*
[19] *Supra* note 10.
[20] *Id.*
[21] *Id.*
[22] *Id.*
[23] UK GDPR Recital 32.
[24] *Id.*
[25] *Supra* note 10.
[26] *Id.*

The UK ICO guidelines on consent explicitly state that consent is presumed to be invalid when, among other reasons, "there was no genuine free choice over whether to opt in[;]" when "the individual would be penalized for refusing consent[;]"when "consent was a precondition of a service, but the processing is not necessary for that service[;]" and when "people cannot easily withdraw consent[.]"[27] "Consent or pay" business models are invalid on each of the above bases.

b. Consent is not freely given in "consent or pay" business models because users who refuse consent or withdraw consent face a detriment.

The loss of access to a website and the requirement for the user to pay a fee to restore access violates Article 7 and Recital 42 of the UK GDPR by creating a detriment for users who refuse to consent to the processing of personal data. In order to access a website that uses the "consent or pay" business model, a user would need to allow the website to process the user's data for the purpose of targeted advertising. If the user does not consent to the website processing their data for the purpose of targeted advertising, then the user is blocked from using the website. In order to access the website without consenting to the processing of their data, a user would need to pay a fee. This applies whether the user refuses consent from the start or whether the user consents and then later withdraws that consent. This "consent or pay" system is detrimental to users in three ways:

- **Statutory harm:** a violation of a data subject's Article 7 rights;
- **Financial harm:** the fee a user would pay to use the website without personal data being processed for targeted advertising;
- **Autonomy harm**: blocking the user from using the website unless consent is given to process the user's personal data.

Some may argue that individuals are free to use other websites or services if they do not wish to consent to use of their personal data or pay a fee. However, this argument fails due to a lack of reasonable options for users. Targeted advertising is not reasonably avoidable online.[28] Even the UK

[27] *Supra* note 10.
[28] *Supra* note 5, *Disrupting Data Abuse Report* at 19-20; 55-60; 157-160; 170-174; 187-88.

ICO's own website includes tracking cookies used for targeted advertising.[29] If the UK ICO allows "consent or pay" business models, more and more of the internet will become paywalled to UK citizens.

Because of these detriments, the consent itself cannot be freely given and is therefore invalid. To process the user's data for targeted advertising, the website would need a different lawful basis under Article 6 of the UK GDPR.[30]

c. *Consent is not freely given in "consent or pay" business models because the business model conditions the provision of a service on consent to process data when the consent is not strictly necessary for the provision of the service.*

Using a "consent or pay" business model to force users to agree to the processing of personal data for targeted advertising further invalidates the requested consent because targeted advertising is not strictly necessary to the provision of the service. Websites do not need to process personal data for the purpose of targeted advertising to provide the service to the user. The UK ICO's guidance on cookies, a data collection tool used for targeted advertising as well as routine operational use, makes this distinction clear: cookies used to remember what goods a user wishes to buy when they go to checkout, cookies used for load balance or reverse proxying, and cookies used to comply with the UK GDPR's security principle for an activity the user has requested ***may*** be strictly necessary to the functioning of a service—that is, without the use of these cookies, a user would "be unable to undertake certain activities."[31] On the other hand, cookies used for analytics purposes, first and third-party advertising cookies (including those used for operation purposes like click fraud detection),

[29] *Use of cookies by the ICO,* United Kingdom Information Commissioner's Office, https://ico.org.uk/global/cookies/ (if a user views a YouTube or Vimeo link on the UK ICO website and they are logged in to their Google or Vimeo account, that service may set cookies for advertising purposes).
[30] UK GDPR Article 6.
[31] *What are the rules on cookies and similar technologies?,* United Kingdom Information Commissioner's Office, https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/what-are-the-rules-on-cookies-and-similar-technologies/#rules1.

and cookies used to recognize a user when they return to a website for a unique greeting are ***not*** strictly necessary to the functioning of a service.[32] The cookie guidance applies to traditional cookies as well as "similar technologies" such as tracking pixels, plug ins, fingerprinting techniques, Local Shared Objects, and "any technology that stores or accesses information on the user's device."[33] Because processing data for the purpose of targeted advertising is not strictly necessary, it is illegal for websites to condition provision of the service (in this case, access to the website) on consenting to personal data processing for targeted advertising purposes.

Even if the personal data processing for targeted advertising was strictly necessary to providing access to the website, consent would still be an inappropriate basis for processing. The UK ICO explicitly states that consent is an inappropriate basis for processing data when a controller "ask[s] for consent to the processing as a precondition of accessing a controller's services."[34] Instead, the UK ICO recommends using the "necessary for contract" lawful basis for processing data. In that case, instead of offering the illusion of a "free" version of the website, the website could contract with the user to process the user's data for targeted advertising.

II. Conclusion

EPIC urges the UK ICO to center the rights of its citizens over commercial interests by prohibiting the use of "consent or pay" business models. "Consent or pay" business models are diametrically opposed to the UK GDPR's definition of consent as well as the UK ICO's extensive guidance on consent, cookies, and the UK GDPR writ large. The four-factor framework provided by this call for views does not address the fundamental problem with the business model: the fact that consent under this business model is not freely given and, therefore, cannot meet the legal standards

[32] *Id.*
[33] *Id.*
[34] *When is consent appropriate?,* United Kingdom Information Commissioner's Office, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/when-is-consent-appropriate/.

for acceptable consent. Beyond the UK, the European Data Protection Board is set to publish its decision on "consent or pay" business models after the Dutch, Norwegian, and Hamburg data protection authorities submitted a complaint about Meta's rollout of its "consent or pay" business model.[35] In February, 28 NGOs, including EPIC, signed onto a letter requesting the EDPB to firmly oppose "consent or pay" business models in its opinion because of the substantial danger to privacy and data protection.[36] The EDPB is set to publish its decision regarding Meta's "consent or pay" business model soon.[37] No fee will ever be appropriate to sell UK citizens' fundamental right to privacy and data protection, so the UK ICO must firmly oppose the use of "consent or pay" business models.

Respectfully submitted,

Calli Schroeder
Calli Schroeder
EPIC Senior Counsel
Global Privacy Counsel

Maria Villegas Bravo
Maria Villegas Bravo
EPIC Law Fellow

[35] *Request for an EDPB opinion on "consent or pay,"* Datatilsynet (Jan. 26, 2024), https://www.datatilsynet.no/en/news/aktuelle-nyheter-2024/request-for-an-edpb-opinion-on-consent-or-pay/
[36] NOYB et al. letter to EDPB, 'Pay or okay' – the end of a 'genuine and free choice' (Feb. 16, 2024), https://noyb.eu/sites/default/files/2024-02/Pay-or-okay_edpb-letter_v2.pdf .
[37] NOYB, *EDPB Opinion: Meta cannot rely on "Pay or Okay"* (Apr. 17, 2024), https://noyb.eu/en/statement-edpb-pay-or-okay-opinion .