DIGITAL REGULATION PROJECT

Yale *Tobin Center for Economic Policy*

Compliant Use of Personal Data for Advertising on Social Networks in Europe by Gatekeepers

Policy Discussion Paper No. 11[1]

September 26, 2025

Compliant Use of Personal Data for Advertising on Social Networks in Europe By Gatekeepers

Introduction

With the passage of the Digital Markets Act (DMA), the European Union has created a new regulatory regime impacting digital markets.[2] One set of the new obligations imposed upon designated digital gatekeepers concerns the use of personal user data for the monetization of online content, particularly relevant for the regulation of social networks. The company at the forefront of current enforcement efforts under these obligations is Meta. This paper examines Meta's compliance efforts under Article 5(2) of the DMA in the context of both economic issues applying to personal data as well as requirements of the General Data Protection Regulation (GDPR).[3]

Meta has been designated as a gatekeeper in two core platform services offering social networks (Facebook and Instagram) that rely on collecting end user personal data as a key element of its business model.[4] Meta was also designated as a gatekeeper in two number-independent interpersonal communication services (WhatsApp and Messenger) and Meta Ads is a designated core platform service in online advertising services. The firm also operates some distinct services that are not designated as gatekeepers (e.g. Dating and Gaming Play).[5] Its business model has been to collect and combine vast amounts of personal data from all across its ecosystem, which allows it to offer targeted advertising for which advertisers are willing to pay a lot of money. This business model harms contestability in digital markets because Meta's data advantage means other digital platforms cannot secure sufficient amounts of advertising revenue, and hence will be precluded from successfully operating even when in principle being able to offer a better service to customers. Article 5(2) of the DMA addresses this harm to contestability by limiting gatekeepers' data collection and combination. This obligation goes 'beyond the conditions that other market players face.'[6] As we detail below, the legislature intended to make it more difficult for Meta to retain its data advantage, which likely at least in part derives from illegal practices under GDPR, and thereby open digital markets to others.[7] These changes benefit compliant rival platforms.

---

[2] Regulation 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L265/1.

[3] Article 5(2)(a) of the DMA specifies that gatekeepers may not process personal data from third parties, for the purpose of providing online advertising services, without the user having a specific choice and giving consent as defined in the GDPR. Article 5(2)(b) likewise requires consent for the combination of data from third parties and also data from the gatekeeper's own services. In this paper we do not discuss compliance with Article 102 TFEU as discussed in Case C-252/12, *Meta v Bundeskartellamt* EU:C:2023:537.

[4] 97.5% of Meta's annual global revenues comes from advertising. Case DMA.100055, Meta – Article 5(2) (23 April 2024), footnote 4.

[5] Cases DMA.100020 Meta - online social networking services, DMA.100024 Meta – number-independent interpersonal communications services, DMA.100035 Meta - online advertising services, DMA.100044 Meta – online intermediation services – marketplace (5 September 2023).

[6] Meta – Article 5(2) (above n 4), para 54

[7] For example, the above-cited *Meta v Bundeskartellamt* case addresses GDPR in part with regard to Meta's data collection and combination practices.

The Article focuses on Meta's compliance but the concepts discussed herein are more widely applicable than Meta's current compliance effort. In particular, we propose principles to help gatekeepers design, and regulators evaluate, choice architecture and service design that protects consumers from exploitation while allowing those consumers to make an affirmative choice to benefit from sharing personal data. We show that careful design of the baseline versions of the services offered by gatekeepers combined with an off-platform benefit that consumers get if they, in a second stage, choose to share more personal data, protects both consumers and the gatekeeper.[8]

Our analysis is in part inspired by the European Commission's ongoing investigation into Meta for noncompliance with Article 5(2) of the DMA. Thus far, the company has made a sequence of changes to its services and the choices it presents consumers in response to the DMA and subsequent noncompliance investigation. On April 23, 2025, the European Commission fined Meta €200 million for failure to comply with the DMA's provisions under this article: in particular those that cover the processing of personal data for advertising and the combination of user data from different sources. The Commission based its decision on a former version of Meta's services, not the company's latest attempt at compliance (from November 2024), for which the investigation remains ongoing. The November 2024 version of Meta's compliance effort is the subject of our analysis throughout this paper.[9]

Meta's menu of versions with its accompanying choice architecture represents substantial progress but still does not give users an effective choice over what personal data to share, and therefore does not seem to bring the gatekeeper into compliance with the DMA. In principle, Meta's decision to offer a menu of options with different levels of data sharing is an excellent method of delivering choice to users. However, by (i) hiding data collection choices behind ad-type choices, (ii) hiding settings for users to opt out of intensive data collection, and (iii) coercing and defaulting users into the most data-intensive options, Meta's menu of options does not provide the user with an appropriate consent environment, nor sufficient protection of users' rights under European Union law.

Although we focus throughout on the specific issues surrounding the Meta case, the standards we propose are equally applicable to any ad-supported social network that must comply with Article 5(2) of the DMA and should be helpful guideposts to companies seeking to understand better their potential obligations under European Union law. Regulators may also find the analysis helpful in providing an economic framework for discussing and evaluating compliance.

We begin by discussing the requirements of Article 5(2) of the DMA, specifically the concept of "free consent" under European Union law, which is a key point of debate (Section 1). We explain the degree to which this notion, which is based on the GDPR, is supplemented when applied to gatekeepers on the basis of Article 5(2) of the DMA. We then assess Meta's approach to

---

[8] Each of this Article's authors may not endorse every element of the proposal we outline below. Nonetheless, all authors agree that each of the concerns and proposals identified herein is supported by sound legal and economic principles; we offer these proposals based on that consensus.

[9] The conduct at issue in this Article could also be a violation of EU competition law or consumer law, but our analysis is limited to DMA enforcement. For a discussion of all legal bases, see A. D'Amico, D. Pelekis, C. Santos, B. Duivenvorde. "Meta's Pay-or-Okay Model – An analysis under EU Data Protection, Consumer and Competition Law" TechReg 2024.001.

compliance, drawing from firsthand user experience (Section 2). Finally, we propose a path to achieving compliance (Section 3). Throughout the paper, we do not discuss the desirability of the DMA constraints on the processing of personal data. We take the text and the spirit of the DMA and other European regulations as given and propose a model for compliance with existing law. Our proposal modifies Meta's design by offering users a baseline configuration with limited data-processing that does not fall within Article 5(2), alongside options for users to choose to increase or decrease the processing of their personal data. Specifically, we propose the following:

1. The baseline should entail users being asked to (i) consent to the processing of on-platform data for on-platform advertisements and (ii) exclude the processing of off-platform data for advertising or other purposes.
2. Users who do not want (1) above, namely their on-platform data processed for advertising would have the option to pay a reasonable price to Meta.
3. If Meta wants users to allow it to process and combine off-platform data (e.g., because doing so would allow it to sell more valuable ads in more places), it can offer users some value in exchange for their consent to allow Meta to process and combine these data, provided that any such incentive does not take the form of an improvement or change in Meta's own services.

In our proposal, users will first be offered a binary choice between the baseline account configuration and a zero data processing option for a reasonable price (1 and 2 above). Subsequent to this initial choice, Meta would be free to ask users to consent to additional use, collection, combination, and other processing of their personal data (all falling under 3 above). Dividing these choices into multiple stages ensures users are always given straightforward, specific choices about the processing of their data.

This structure will result in many users first choosing the baseline option because it does not involve any monetary cost. If the fully private option is very costly, the fact that nearly every user chooses the baseline could be evidence of coercion to share personal data. We explain how the need to avoid coercion guides the price of the choice without data processing. The "no data" option may carry a monetary charge, but only one based on the revenue Meta could generate through contextual advertising without user consent to process data. On the other hand, companies like Meta will likely want users to share far more data than the user-preferred baseline and may be tempted to coerce further sharing. We thus explain how a gatekeeper could legitimately compensate users for sharing more data beyond the baseline by offering incentives that do not affect the gatekeeper's own services (Section 3).

A key advantage of this model is that, in our understanding, Meta *already* allows users worldwide to configure their accounts to fit our proposed baseline *at no cost*. Currently, however, this option is neither easy to find nor straightforward to understand. By making it the baseline setting (while always allowing the user to buy a no-data-usage option), Meta can bring its platforms into compliance. The issue at hand, then, is proper consent, not the fundamental business model of ad-supported social networks, which support the widescale provision of a free service to end users. Such a model can comply with European law with only a few adjustments, as we describe throughout the paper. Therefore, compliance with European law is not a fundamental threat to the company's ability to do business.

We conclude the paper by generalizing our proposal to articulate a basic model for allowing consumers to benefit from online data processing and choose to exempt themselves from such processing if they so desire.

1. Article 5(2) DMA: limiting gatekeeper data accumulation

Large digital companies combine and process personal data for a number of reasons. Our focus in this article is on the data-processing for the purposes of personalized advertising. Meta uses this advertising to monetize its social network offering—a service that has traditionally been provided to end users for a monetary price of zero. In carrying out these processing operations, Meta must demonstrate compliance with the GDPR and the DMA. The DMA supplements the GDPR in two ways. First, it narrows the lawful bases for the processing of off-platform data by gatekeepers for the purposes of advertising to only one: end-user consent. Second, it requires that the consumer is offered a specific choice to agree to share this data, but that the consumer should be able to access the service even if they do not consent.

To understand the impact of the DMA in the context of the collection of personal data, it helps to visualise different sources from which personal data of a user of Facebook.com may be obtained by Meta. One way of doing this is to distinguish between on-platform data (which Meta processes from the user's activities on Facebook.com) and off-platform data (which Meta processes from the user's activities on another Meta platform such as, e.g., Instagram or which, sometimes with the aid of cookies, Meta collects from third-party websites or apps). On-platform data is therefore collected by the platform when the consumer is using a particular Core Platform Service (e.g. Facebook.com), Off-platform data includes data from other services provided by the same company (e.g. Instagram, Dating) as well as data collected from the use of third-party apps or websites.[10] On the basis of the DMA, end-user consent is the sole legal basis upon which a gatekeeper like Meta may combine and process off-platform data for such monetization purposes.[11]

This limitation is found in Article 5(2) of the DMA.[12] Article 5(2)(a) forbids the gatekeeper from processing personal data of end users using services of third parties that make use of the core platform services of gatekeepers (e.g. when a business user has a contract with a gatekeeper providing advertisings services). More widely, Article 5(2)(b) prohibits combining personal data from the core platform service under scrutiny with personal data "from any further core platform services or from any other services provided by the gatekeeper or with personal data from third-party services." This provision is more extensive than Article 5(2)(a) because it includes the

---

[10] This is the distinction drawn by the German Competition Authority in its Facebook case. Budeskartellamt, "Facebook Proceedings Concluded" Press Release 10 October 2024.

[11] A firm that is not designated as a DMA gatekeeper instead may be able to collect data for monetization purposes using two other legal bases in the GDPR: it may claim that processing is necessary for the performance of a contract (Article 6(1)(b) GDPR) or that processing is necessary for the purposes of a legitimate interest (Article 6(1)(f) GDPR. A gatekeeper is not entitled to rely on these two legal bases for the purposes of monetization, see Article 5(2) DMA.

[12] For a more granular account, see G. Monti and A. de Streel, "Data-Related Obligations in the DMA" (CERRE, 2024) https://cerre.eu/wp-content/uploads/2024/01/Data-Related-Obligations-in-the-DMA_FINAL.pdf , Meta – Article 5(2) (above n 4) paras 29-32.

combination of data for all purposes and not only advertising, though we focus primarily on advertising here. Article 5(2)(c) forbids a gatekeeper from cross-using personal data from a core platform service to another service, including other core platform services. Cross-use, however, is allowed if the two services are provided together or support each other.

These three prohibitions are complementary and the Commission explains that the policy behind them is 'to seek to address gatekeepers' enhanced access to personal data of end users, which provides gatekeepers with potential advantages in terms of accumulation of data, thereby raising barriers to entry and hindering contestability in digital markets.'[13]

The effect of this prohibition has both a competition impact and a privacy impact. The DMA allows rivals of the gatekeeper to collect data more easily by affording them the possibility to obtain these data via legal bases other than consent as well as request that users share personal data generated on gatekeeper platforms with rivals. If rivals are better able to use more data to monetize their services, the expectation is that rivals to gatekeeper platforms can emerge. From a privacy perspective, the concerns arising from the combination of third-party data are especially stark. Users may think they are engaged in private activity (e.g. browsing a labour union's website or buying a medication) when a gatekeeper is instead processing that data. (Note that the legal provisions above are not specific to sensitivity and cover all third-party data.)

Nevertheless, a gatekeeper may obtain and use an end user's off-platform data listed in Article 5(2) if "the end user has been presented with the specific choice and has given consent."[14] The concept of consent is the same as under the GDPR, and it is defined thus: "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."[15] The concept of specific choice is new and unique to the DMA.

Specific, Informed, Unambiguous, and Free Consent

The concept of consent adopted from GDPR has four key elements. We explain how certain elements of the concept of consent should be interpreted in light of the economic power that gatekeepers have.[16]

First, the consent must be *specific*. For consent to be specific, the user must consent to the particular use of data for a given purpose. The GDPR specifies that: "[c]onsent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations."[17] In the *Meta* judgment the ECJ explained that this is particularly important when the controller collects a lot of end-user data, especially data that "users cannot reasonably expect . . . to be processed by the operator," such as data gathered outside of users' "conduct within the social network."[18] When the gatekeeper is collecting both data that users

---

[13] Meta – Article 5(2) (above n 4) para 32.
[14] Article 5(2) DMA.
[15] GDPR, Article 4(11).
[16] See also A.S. D'Amico, "The DMA's Consent Moment and its Relationship with the GDPR" (2025) 16 European Journal of Risk Regulation 170.
[17] GDPR, Recital 43.
[18] Meta, para 151.

might expect and not expect (for the latter, i.e., tracking their activities across the entire internet), the ECJ wrote that it would be "appropriate… to have the possibility of giving separate consent."[19] Giving users the ability to consent to each processing of data separately—especially when users will likely find one category much more objectionable than the other—is an application of the *specific* choice requirement.

Second, the consent must be *informed*. This rules out choice architectures that are difficult to navigate and understand. The DMA supplements this for gatekeepers, indicating that "When the gatekeeper requests consent, it should proactively present a user-friendly solution to the end user to provide, modify or withdraw consent in an explicit, clear and straightforward manner."[20]

Third, the consent must be *unambiguous*. This rules out consent given to an option that does not explain what data are collected, and whether they are used for showing ads or other purposes. This interpretation is reinforced by the fact that the DMA adds that gatekeepers cannot make user "choices unduly difficult, including by offering choices to the end-user in a non-neutral manner, or by subverting end users' or business users' autonomy, decision-making, or free choice via the structure, design, function or manner of operation of a user interface or a part thereof."[21]

Fourth, consent must be *free*. As explained in Recital 43 of the GDPR, this requires an absence of coercion. The recital sets out a general presumption against consent when there is a power asymmetry: "consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller." This recital uses as an example a public authority seeking user data, but in the *Meta* judgment the ECJ explained that the existence of a dominant position may also "create a clear imbalance" between the data subject and the controller.[22] In this context, the ECJ states that "users must be free to refuse individually [...] to give their consent to particular data processing operations not necessary for the performance of the contract, without being obliged to refrain entirely from using the service offered."[23] In this context however, the ECJ allows that users wishing to withhold consent can be charged an appropriate fee.[24] It is beyond the scope of this paper to discuss what an appropriate fee is for the purposes of Article 102 TFEU but we consider that our proposal for determining fees for the DMA can offer useful pointers (see Section 3).

Specific Choice

The other requirement under Article 5(2) is that of "specific choice." According to the Commission's *Meta* decision (which is the first and so far only decision interpreting Article 5(2)) the requirement means that if a gatekeeper asks for user consent to data sharing practices listed in

---

[19] Meta, para 151.

[20] DMA, Recital 37.

[21] DMA, Article 13(6)

[22] Meta, above note 9 para 149.

[23] Meta, above note 9 para 150.

[24] Meta above note 9 para 150. "those users are to be offered, if necessary for an appropriate fee, an equivalent alternative not accompanied by such data processing obligations." Note also that this line is what Meta used to design its initial offering, described below.

Article 5(2), the user must have the option to withhold consent and continue to use the offered service.[25] The DMA refers to this as 'a less personalised but equivalent alternative.'[26]

Some guidance is offered to gatekeepers about this alternative. For example, it may be offered on the basis of no or less data processing, where "less" processing includes processing that is not subject to Article 5(2) requirements.[27] This means that other data processing activities that are not forbidden by Article 5(2) may be carried out in the alternative version. Moreover, the service that the user gets from choosing the less personalised alternative cannot be different from the version available if one consents to data processing, nor can it be of degraded quality (except insofar as the lack of data itself changes the service, such as by making advertisements less personalized, which some users may dislike).[28]

In the Commission's 2025 *Meta* noncompliance decision, the Commission in places interprets this requirement to mean that any difference not only in the product but also in its conditions of access (e.g., whether a user compensates the gatekeeper by direct payment or by viewing advertisements) is prohibited.[29] Were this strict interpretation to be adopted, Meta would be prohibited even from charging a reasonable fee to users who withhold consent to process customary, on-site data in a way that is compliant with the above requirements.

We find this prohibition not to be proportionate or aligned with the goals of preventing user exploitation and promoting contestable markets with healthy business models. The relevant question is not mere difference but rather whether users can freely choose whether or not to consent to data processing. For example, suppose in a hypothetical world, a gatekeeper charged users a small fee to consent to data collection but made withholding consent free. We would have no objection to the difference in conditions of access because such a difference clearly imposes no burden on users who want to withhold consent.

The *Meta* decision is replete with evidence that aligns with our reasoning. In particular it explains how Meta used conditions of access to degrade user choice (as in, make withholding consent prohibitively difficult and expensive to users).[30] Such behavior clearly harms users and their ability to choose whether or not to consent to data processing. Because the Commission only evaluates the offerings that lie before it, the decision should be read as a response to the offer it analysed—one that was facially noncompliant. We are confident that our proposal— which does not exploit users, allows more healthy business models, and gives consumers a demonstrable choice in offering or withholding consent—can comply with the "specific choice" requirement even if the conditions of access to different options are not identical.

Consequences for Compliant Consent: Offering a Baseline

These requirements in the GDPR (and DMA) create a tension for all firms (only gatekeepers are covered under the DMA), but especially for firms like Meta that collect a lot of data for many

---

[25] Meta – Article 5(2) (above n 4) para 37.
[26] Recital 36 DMA.
[27] Meta – Article 5(2) (above n 4) para 133
[28] Meta – Article 5(2) (above n 4) para 136. This is consistent with Recitals 36 and 37.
[29] Meta – Article 5(2) (above n 4), para 90-92.
[30] Meta- Article 5(2) (above n 4) para 96.

different purposes. On one hand, end users must be allowed to make informed, specific, unambiguous, and free choices. On the other hand, if a firm does provide such a variety of options, then setting these out in detail risks creating complexity and information overload. This in turn makes it hard to provide the relevant information in a clear and straightforward way that enables compliant consent.[31]

In such an environment in which consent is required to collect and use data, it is in the interest of both firms and users to establish a baseline that satisfies both the legal consent requirements and meets the firms' own needs to conduct their businesses with as few frictions as possible. For both of these aspects, it is important what the baseline option comprises and how it is described. The task of explaining the baseline option is especially demanding when the baseline option is not what users might reasonably expect initially. Thus, we believe that the baseline option must either (i) not require user consent or (ii) be explained sufficiently clearly and be sufficiently simple that it can be fully understood by users. Given existing evidence on how users interact with digital consent forms, however, we suspect a full understanding of users effectively requires the baseline to be in line with reasonable user expectations.[32]

In practice, we expect that Meta would wish to avoid setting the no-consent option as the baseline, because under this option it might be unable to obtain sufficient user data to successfully operate its advertising business. We should thus see a baseline option that is in line with reasonable user expectations as to what their consent would cover. In addition to such a baseline, the company would also have to offer users the choice of a no-consent alternative to the baseline (as specified in the DMA's Recital 37), which could, in our view, include a reasonable fee (see Section 3 for our proposals). After users have made a free choice in this compliant configuration, the platform would be able to ask them to consent to more complex or intrusive data collection, combination, and processing—particularly uses that are beyond their reasonable expectations for the service. We discuss more what such follow-ups may look like below (Section 3).

In summary, in order to combine and process personal data lawfully, gatekeepers like Meta must get users' specific, informed, unambiguous, and free consent, and must offer the end-user at least a choice between an offer that is based on not combining the data listed in Article 5(2) and one in

---

[31] Arguably, this points to a regulatory failure in the GDPR's decision to allow user consent as a legal basis for processing data. On the one hand, the EU considers data privacy as a fundamental right that it seeks to protect. On the other hand, the GDPR places responsibility for protecting this fundamental right on the holders of this right who have limited capacities and time to understand how to protect this right effectively. This perspective is in line with the so-called privacy paradox where user's stated privacy preferences are at odds with the choices they make. (*See*, e.g., A. Carignania and V. Gemmo "New Media and Privacy the Privacy Paradox in the Digital World: I Will Not Disclose My Data. Actually, I Will … It Depends" (2017) 27(1) International Journal of Computer 201–212.)

We do not engage with or solve this problem here, but we hope that the choice model we propose goes some way to addressing this weakness in the GDPR.

[32] Competition and Markets Authority, 'Online Choice Architecture: How digital design can harm competition and consumers Discussion Paper CMA 155 (April 2022): https://assets.publishing.service.gov.uk/media/624c27c68fa8f527710aaf58/Online_choice_architecture_discussion_paper.pdf

which the user consents to such data being combined. More specifically, this requires the following:

- Users must be asked to consent to different types of processing separately, with particular care when such processing is likely beyond their reasonable expectations and/or is not required for the provision of the service.
- Because it may be impossible to provide the full variety of choices in a sufficiently clear and straightforward way up front, choices must be offered in steps. Enabling free consent will likely require the provision of a baseline option that can be fully understood by users. This is turn requires that it be in line with their reasonable expectations of what such consent would cover.
- If the baseline itself requires user consent (it need not if it includes zero consent-dependent data processing), users must be given an option that does not require consent and is not degraded in quality. This option may be offered for free or at a reasonable price.
- If more data-intensive options are offered in subsequent choices after the baseline, these must be sufficiently clear and noncoercive for users to give consent.

2. Assessing Meta's Approach to Compliance

Meta currently has several personal data-processing buckets underpinning its online advertising services. On the basis of the DMA, we can distinguish five: (i) data from the use of a single gatekeeper core platform service, for example data from the use of Facebook; (ii) data from Meta's other non-ads core platform services (e.g. Instagram); (iii) data from Meta's other distinct services that are not core platform services (e.g. Dating); (iv) data obtained from third parties; (v) data in Meta's online advertising service (Meta Ads). Colloquially, the first bucket may be referred to as on-platform data while the others as off-platform data.

As far as the first bucket is concerned, Meta needs only comply with the GDPR. This means it may offer contextual advertising, which is based on what the end-user is viewing rather than on personal data, or it should seek consent to process personal data. The DMA forbids the combination of on-platform data with the other four (off-platform data) buckets unless the user is given the choice to consent to this combination. Observe that the business model as such is not regulated, only the data gathering and combining activity.

We now turn to consider Meta's prior and current approaches to compliance with the GDPR and the DMA.

Meta's Prior (2023) Approach

In November 2023, as part of its GDPR and DMA compliance efforts, Meta launched an ad-free subscription available in relevant jurisdictions that allowed users to pay the company in exchange for experiencing their chosen Meta platform (Instagram and/or Facebook) without ads.

The initial monthly prices (€9.99 when purchased on the web or €12.99 when purchased through mobile app stores) translated to annual payments of between €120 and €156. This is referred to as the Subscription for No Ads (SNA) Option.

Users who did not subscribe were deemed by Meta to have consented to the version with full tracking for targeted advertisements (that is, both on-platform and off-platform data processing), in line with Meta's standard offering in previous years. Regulators and observers quickly identified the new system as "pay or consent." While users who "consented" continued to have the ability to opt out of certain data processing (see below), they were by default given the most data-intensive processing settings. In addition, both types of users were by default opted-in for the integration of third-party data into their back-end Meta profiles. The Meta Privacy Policy lists nine other categories of Meta's interests (besides advertising) to justify the collection of these third-party data, even for users who see no advertisements.[33]

In the aftermath of this announcement, and with the DMA obligations having become binding on Meta on 7 March 2024, both the European Data Protection Board[34] and the European Commission[35] took issue with what they viewed as the coercive effects of this "pay or consent" model. The chief issue raised by both the European Commission and the European Data Protection Board was that a binary choice between a free service supported by personalized ads that relied on the processing of on- and off-platform data and a paid subscription service that did not rely on the processing of on- and off-platform data for advertising (and continued to process those data for other purposes) did not represent a choice at all. A too-high price is equivalent to not offering a choice and thus undermines the notion of *free* consent. Indeed, Meta had set a very high price, one that far exceeded the roughly €63 individual European users produce annually in ad revenue for Meta.[36] The disparity between these two figures raised additional concerns that Meta was attempting to leverage its dominant position in personal social networking to secure a price increase for users who did not choose to share personal data. In April of 2025, the European Commission fined Meta €200 million for noncompliance with the DMA's provisions around data processing and consent under this former system.[37]

The principal bases of the Commission's non-compliance decision are that Meta did not offer users a specific choice of a less-personalised or equivalent alternative and that consent was not freely given. On the element of choice, the Commission explained that the paid version of the service was not equivalent to the alternative because the end-user had to pay and it was obvious

---

[33] These categories include personalizing Meta products, improving Meta products (which includes AI training, though that identified usage has been temporarily suspended by Meta, according to the Policy), measurement and analytics, business intelligence, social good research, security and safety, and others. *See* Meta. *Privacy policy*. Facebook. Accessed 18 Mar. 2025. https://www.facebook.com/privacy/policy/

[34] European Data Protection Board. (2024, 17 April). *EDPB: Consent or pay models should offer real choice*. EDPB News. https://www.edpb.europa.eu/news/news/2024/edpb-consent-or-pay-models-should-offer-real-choice_en

[35] European Commission. (2024, 30 June). *Press release: IP/24/3582*. European Commission Press Corner. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3582

[36] noyb. (2023, 28 November). *noyb files GDPR complaint against Meta over pay or okay*. noyb.eu. https://noyb.eu/en/noyb-files-gdpr-complaint-against-meta-over-pay-or-okay

[37] European Commission. (2025, April 23). *Commission finds Apple and Meta in breach of the Digital Markets Act*. European Commission, https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1085. It has also been argued that this model may be contrary to EU competition law, the GDPR, and consumer protection law A. D'Amico, et al., above note 3.

to the gatekeeper that end-users would be unwilling to pay. Internal memos "show that the pricing strategy for the [Subscription for No Ads] SNA option built-in the expectation that end users would not exercise their specific choice."[38] Academic studies in Meta's own submissions reveal "that end users of online services overall have low willingness to pay for privacy, even when they would prefer a less personalised experience."[39] Therefore, the new choice was not a realistic one. As discussed in Section 1 above, the Commission's decision also raised the possibility of a formal ban on any differences between options, not just degrading differences, but even without accepting this claim, the decision provides ample evidence of intentional and substantive degradation sufficient to disqualify the pay or consent system.

The Commission further found that Meta's approach was also defective because users were not in a position to consent freely. Three elements were used to find that consent was not freely given. First, there is an imbalance of power between the firm and its end-users, who feel compelled to opt-in to sharing their data. Designation as gatekeeper is an indication of imbalance of power, user lock-in and network effects contribute to giving Meta power as was the fact that until 2019 Facebook had a slogan: "It's Free and Always Will Be," which may have attracted users who were unwilling to pay.[40] These users are now unable to freely consent between the two options presented. Second, end-users cannot refuse consent without suffering a financial detriment, a point that is based on similar evidence discussed when exploring if there was a specific choice. Third, if the user does not consent or pay then they must leave 'the Facebook and Instagram environment altogether.'[41] This is because the consent covers the processing of data from on- and off-platform services. Other consent criteria (e.g. specific, informed and unambiguous) were not considered.[42] It seems likely that these could also be violated given the complexity of the choice setting and Meta's minimal attempts to inform the user.

Meta's Current (2024) Approach

In response to pressure from European regulators, in November 2024 Meta announced the introduction of a third alternative to the subscription and the fully-personalised ads options.[43] Meta called the new, free alternative "less personalised ads." This announcement created an updated menu of three options that vary along two dimensions: price and ad type.

- There is Meta-as-we-know-it (free services supported by personalized ads), which we call Option A;
- The new option (free services supported by "less personalised" ads), which we refer to as Option B;

---

[38] Meta- Article 5(2) (above n 4) para 96.

[39] Meta – Article 5(2) (above n 4) para 93.

[40] Meta – Article 5(2) (above n 4) paras 183-186.

[41] Meta – Article 5(2) (above n 4) para 194.

[42] Since the Commission found that Meta had not satisfied the specific choice requirement, this portion of the decision is discussed largely for completeness, explaining the truncated treatment. Meta – Article 5(2) (above n 4) para 176.

[43] Meta. (2024, 12 November). *Facebook and Instagram to offer subscription for no ads in Europe*. Facebook. https://about.fb.com/news/2024/11/facebook-and-instagram-to-offer-subscription-for-no-ads-in-europe/

- The subscription offer (a service that carries a fee but no ads), which we denote as Option C.

As in the first launch, users across all three options continue to be automatically opted-in for the integration of third-party data into their back-end Meta profiles, though they continue to have the option to opt out.

In the same November 2024 update, Meta also reduced the ad-free subscription price to €5.99 when purchased on the web or €7.99 when purchased through mobile app stores, an annual fee of €72 or €96. The updated pricing demonstrates that these prices are not the outcome of a careful cost calculation but rather designed to be part of a regulatory dialogue. The European Commission has not yet issued any formal decision on the compliance of this new system.

Assessing Meta's Current Approach

The new menu hews closer to the requirements of compliant choice, but we see three immediate problems.

(i) Ad Type v. Use of Personal Data

First, these options are differentiated by ad type, not by the extent of processing of personal data.[44] This setup creates two problems. First, users are directed to focus on the types of ads they want to see rather than the data they are consenting to share. Option A (Meta-as-we-know-it) continues to rely on both on-platform and off-platform data processing. Option B (the free "less personalized" version) also processes on- and off-platform data (i.e., the integration of third party data into a user's back-end Meta profile continues to be enabled by default), but has ads that "rel[y] on less data." The ads displayed to users selecting this option will be "based only on context—what a person sees in a particular session on Facebook and Instagram—and a minimal set of data points including a person's age, location, gender, and how a person engages with ads."[45] Option C, also appears to process on- and off-platform data, but does not use it to advertise to the user because the user is shown no advertisements.

Meta may argue that focusing on ad-type rather than data processed is easier for users to understand and thus is a good proxy for data processing. Users also may well reasonably infer that a service with fewer or no ads will imply that the data that would be otherwise used for ads are not collected/combined.

The second problem with the setup, however, is that – contrary to likely user expectations – the three different options *do not appear to correspond to different levels of data processing*. Under the Article 5(1)(c) GDPR data minimisation principle, it should be the case that Meta would combine and process less data about users that choose Options B and C, but this is not made

---

[44] Meta. (2024, 12 November). *Facebook and Instagram to offer subscription for no ads in Europe*. Facebook. https://about.fb.com/news/2024/11/facebook-and-instagram-to-offer-subscription-for-no-ads-in-europe/
[45] Meta. (2024, 12 November). *Facebook and Instagram to offer subscription for no ads in Europe*. Facebook. https://about.fb.com/news/2024/11/facebook-and-instagram-to-offer-subscription-for-no-ads-in-europe/

In the Privacy Policy linked above, Meta also appears to suggest that device usage and characteristics will also be taken into account in advertising.

clear. Across all three options, users continue to be automatically opted-in to Meta's processing of third-party data on their activities off Meta technologies. Their data may also continue to be collected for advertising purposes even if not to advertise to them directly (in the cases of users who have chosen less-personalised ads or no ads).

If Meta in fact continues to harvest such data without consent and contrary to user expectations, Meta's offer could even be misleading under consumer law (as well as being in breach of the GDPR data minimization principle). Either way, Meta's difficulties here would be resolved if it asked users about the data it is combining and processing, rather than focusing their attention on the advertising they receive.

The reader may wonder why Meta would want to continue to combine and process extensive personal data if the user has chosen not to see ads based on those data. From an advertising perspective, a key reason is that Meta's algorithms will typically target other users with personalized advertising more effectively the more data they are trained on, making such advertising more valuable. Or Meta may wish to continue combining and processing data in case the user one day switches back to allowing personalised ads. Moreover, there may be additional non-advertising-based reasons for using these data. Whatever the reason, users are giving permission for such wider data uses, without being aware of this fact, when they sign up to options based on the extent of advertising rather than the extent of data combination and processing. This would seem to breach the requirements for unambiguous and informed consent articulated above (Section 1).

(ii) Difficulty of Access

Secondly, while Meta provides menu options that allow users in all three versions to limit data processing (not just ad type), these options are difficult to access. Most of the relevant settings are located in the Meta Accounts Center, which can be accessed from the Facebook homepage in three clicks—if a user knows exactly what to click. Users who select what seem like intuitive menu options, such as completing the Facebook "Privacy Checkup" or navigating to the Privacy Center, will find themselves either not able to link to relevant privacy settings at all, or with an even longer journey to their destination.[12] Finding the relevant settings after arriving at the Accounts Center requires another two or three clicks, and settings are located in different places and sometimes behind vague descriptions (e.g., "Manage info") and hidden tabs.

Assuming a user finds the settings, the primary privacy or advertising configurations of interest to a user are threefold. First, there are settings that limit Meta's use of personal and third-party data in advertising to the user on and off Meta. These settings are available only to users with the personalized ads version of Facebook in the EU (option A above), which is identical to the version deployed in the rest of the world. Then there are settings that allow users to indicate advertisers and advertising topics that they like or dislike, which can be accessed by any user who gets advertisements on Meta (options A and B above). Finally, there is one option (purportedly) allowing users to limit Meta's collection of data about them (other options only limit the use of that data for advertising purposes), which is to opt out of the integration of third-party data into a user's back-end Meta profile. As mentioned above, all users of Meta technologies are by default opted into the integration of these data. Although we do not have access to a significant number of accounts to be able to generalize this finding, in the Facebook

account we created in Germany, the option to opt out of integration of third-party data did not work. Despite repeatedly opting out of data integration over the course of more than a month, the integration remained on.

Besides designing the choice architecture to make choosing privacy difficult, Meta does not prompt a user to adjust any of these settings or alert the user to their existence. Further barriers include warnings to users who choose a lower-data setting that inform them how their experience will be negatively affected if they proceed. Changing a setting back to the default greater data setting, in contrast, rarely requires more than a single click. As a consequence of all of these difficulties of access, it is likely that users are neither informed nor free in their alleged "consent" to give Meta these data.[46] The European Commission faulted Meta for these hidden configurations in its April 2025 decision, and the new system makes no improvements to it.

        (iii) Problematic Consent Process

In addition to the conflation of advertising and privacy as well as the difficulty of accessing privacy settings, under the current design of the menu, users face some coercion in the decisions they are allowed to make and further fail to be given informed, unambiguous, and specific choices.

In assessing coercion, a data processor's market power is highly relevant because that power can be used to make offers that give users no real choice. In the case of Meta, a user wanting to check up on their friends has no other place to go if their friends only post certain content on Facebook or Instagram. This market power means that the platform has the ability to coerce consent by refusing access, by charging a significant monetary fee, or by degrading the service, if users do not consent. In contrast, a brand-new social network would have a more difficult time coercing users because users would always be free to not use the network without major consequence. The DMA gatekeeper platforms have tremendous market power and therefore must be very careful in how they seek consent.

In light of these conditions, the way in which users are presented the three options (the choice architecture) is not designed to facilitate a free and informed choice. After the account creation, a user is asked to make a (potentially) two-step choice. The user is first asked to choose between a paid account without ads or a free account with ads. If the user chooses the paid account, no further choice is requested. If the user chooses the free account, they are next presented with a prompt to "manage your ad experience" or select "not now." If users proceed, they are given a choice between "personalised ads" and "less personalised ads" with brief descriptions of the different options. If users instead select "not now" Meta automatically places them in the "personalized ads" category, despite not receiving their consent to do so. Users are never prompted to return to that choice.

---

[46] In fact, joining Facebook does not even require being confronted with the long text full of legal language. Users are only <u>reminded</u> in small print that "By clicking Sign Up, you agree to our <u>Terms</u>, <u>Privacy Policy</u> and <u>Cookies Policy</u>. You may receive SMS Notifications from us and can opt out any time." The links take users to the pages where they are presumably informed of Meta's numerous, automatically-enable data collection settings, though we have not confirmed that they are.

For users who do not select "not now" and advance to the choice between Option A and Option B, a new potential source of coercion is present: Users are warned that under the "less personalised" option (Option B), some of the ads they are shown will fill the whole screen and be unskippable. In contrast, the regular ads Meta shows will appear in a user's feed and can be scrolled past in the conventional way. As discussed above, consent cannot be considered freely given if the alternative higher privacy option involves a product that is degraded. Requiring Option B users to experience such ads appears to be a case of degradation because the difference in ad display does not necessarily follow from less-data-intensive ads and thus appears to violate the specifications in DMA Recitals 36 and 37 and the requirements of Article 5(2). In this regard, it would be very useful for the Commission to clarify how to interpret the law with regard to what amounts to a degraded service and state explicitly the basis for that clarification so that gatekeepers and users know what constitutes compliance.[47]

In turn, Meta is perfectly able to show the extent to which Option B degrades users' experience by conducting an empirical examination of user behaviour.[48] If users are offered the current Options A and B and choose between them, the proportion who choose each version can be compared to the proportions users choose when the ads in the two versions are delivered in the same format. We expect a greater number of users to select the more private Option B when the ads are in the customary format. The more that users are coerced away from their first choice by the unskippable ads, the more degrading the design change is.[49]

Insofar as the menu of options (1) does not provide users an understandable choice along the critical relevant dimension (the amount of personal data processed by the gatekeeper); (2) does not make readily available the settings required to make such choice(s); and (3) coerces users in their decisions and makes those decisions otherwise difficult, the updated menu falls short of compliance under current law.[50]

3. Achieving Compliance: A Latent Solution

In its March 2025 compliance report to the Commission, Meta describes how its changes comply with Article 5(2) DMA with respect to advertisements and third-party data processing for Facebook and Instagram. In Section III of the report, Meta describes the "pay or consent" model

---

[47] Other forms of degradation of services include making it harder for non-consenting users to communicate with their friends via Messenger, changing how users are shown content, as well as a large variety of other possibilities that change the user experience of Meta's platforms.

[48] The gatekeeper bears the burden of demonstrating that its architecture is not coercive and would have to bear the costs of such testing because it must demonstrate compliance with the DMA.

[49] Meta argues that unskippable full-screen ads are acceptable because they used in other services on the Internet. Clearly, there are many kinds of ads and many business models across the Internet, but what is non-coercive also varies across those business models and cannot simply be imported without justification. In particular, the relevant issue is the comparison within a service across the versions of it with and without personal data processing.

[50] Unless Meta can use a different grounds specified in the GDPR that allows data processing.

as fully compliant with the DMA.[51] It claims that the introduction of what we refer to as "Option B" is "beyond what is written in the law" and not required by the DMA.[52]

Meta also describes the options available to users of the personalised ads version (Option A) to control the data used to show them ads and the types of ads they see. [53] (As noted, all of these settings are on an opt-out basis and are difficult to find.) Meta is careful to note that all of these options made available to users affect the information used to show advertisements to them, not the information that Meta processes about them in total for all of the purposes listed in the Meta Privacy Policy. Meta does not make any mention in its compliance report of the ability of users to opt out of the integration of third-party data into their back-end Meta profiles.

Although Meta's current efforts are for the reasons above not sufficient, we believe that it already offers the foundations of a system that would likely satisfy regulators and courts alike. This solution is based on the legal analysis provided in Section 1. Recall that we concluded that, to meet the consent requirements under GDPR and Article 5(2) of the DMA:

- Users must be asked to consent to different types of processing separately, with particular care when such processing is likely beyond their reasonable expectations and/or is not required for the provision of the service.
- Because it may be impossible to provide the full variety of choices in a sufficiently clear and straightforward way up front, enabling free consent will likely require the provision of a baseline option that can be fully understood by users. This is turn requires that it be in line with their reasonable expectations of what such consent would cover.
- If the baseline itself requires user consent (it need not if it includes zero consent-dependent data processing), users must be given an option that does not require consent and is not degraded in quality. This option may be offered for free or at a reasonable price.
- If more data-intensive options are offered subsequent to the baseline, these must be sufficiently clear and noncoercive for users to give consent.

In this section, we discuss the appropriate baseline option, as well as how a reasonable price could be set for an option without data processing that requires consent, and how users might reasonably be rewarded for consenting to a more data-intensive option.

---

[51] Meta may justify the "pay or consent" model by citing the European Court of Justice ruling on an Article 102 TFEU case against Meta brought by the German competition authority. In this ruling, the Court held that "users must be free to refuse individually, in the context of the contractual process, to give their consent to particular data processing operations not necessary for the performance of the contract, without being obliged to refrain entirely from using the service offered by the online social network operator, which means that those users are to be offered, *if necessary for an appropriate fee*, an equivalent alternative not accompanied by such data processing operations" (emphasis added). However, the DMA imposes additional obligations on gatekeepers beyond those considered in this case, which undermine Meta's claim of compliance. *See* Court of Justice of the European Union. (2023). *Case C-252/21, Meta Platforms and Others v. Bundeskartellamt*. EUR-Lex. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62021CJ0252.

[52] Meta**.** 2025. *Meta's Compliance with the Digital Markets Act: Non-Confidential Public Summary of Meta's Compliance Report.* March 6, 14.

[53] Meta**.** 2025. *Meta's Compliance with the Digital Markets Act: Non-Confidential Public Summary of Meta's Compliance Report.* March 6, 17-22.

The baseline option

As discussed in Section 1, we believe that the requirements of specific, unambiguous, informed and free consent are easiest to meet when consumers are provided with a baseline up front that is easy to understand and in line with reasonable expectations of data processing consistent with the service provided. We are particularly sensitive to the first choice a user makes upon joining the platform because that decision will likely define the user's experience of the platform.

We propose that this baseline option should be exactly the same as Meta's current Option A *except* that it should allow only the combination and use of "on-platform" personal data—and further should be configured by default to opt users out of all of the settings described in the previous section to which they currently are by default opted in (including the combination of third-party data). In such a baseline, personalised advertising on Facebook would be fully allowed, but without employing any "off-platform" personal data.

Conveniently, this configuration is one that Meta already offers to users who navigate Meta's (as explained above, rather complex) settings. Since Meta already offers it to users, this option should be free and should not be degraded (such as by including non-skippable contextual advertising). Moreover, this configuration is implicitly favoured by the Commission in its Meta decision, where it suggests that a compliant alternative 'must be characterized by no, or less, data processing, i.e. by data processing that is not prohibited, pursuant to Article 5(2).'[54]

This baseline would differ from Facebook's existing "less personalised" option in that (i) it would still allow on-platform data to be used for personalised advertising, (ii) there would be no unskippable ads or any other form of product degradation, and (iii) there would be no back-end integration of third-party data into the user's profile. Overall, we expect our proposal to allow Meta to sell significantly more lucrative advertisements than its current "less personalised" option.

Having explained that this baseline complies with the DMA, we now suggest other choices that the end-user may be provided with that ensure that the end-user is given the specific choice to consent to provide more data (which is also required by the DMA) and what other options the end-user may be provided with to guarantee compliance with the GDPR.

Setting a reasonable price for a no-consent-required option

If Meta does choose to offer our proposed baseline, it will also have to offer users a version of the service that does not require any consent for data processing. If user consent to the baseline option is to be freely given, it is further important that the no-consent-required option is priced at a reasonable level so that the end-user has a real choice.

At a minimum level, a reasonable fee should not exceed the monetary value of consent, not be interpreted as the right to maintain monopoly profits, and not charge users for levels of data use previously offered for free. (The final requirement entails that the baseline proposal be free to users, since Meta already offers it for free.) In Meta's case, the regulator could define a reasonable fee as equivalent to the value the company would obtain from advertisement to the

---

[54] Meta – Article 5(2) (above n 4) para 133.

user without requiring their consent for data processing (i.e., the value of contextual ads that could be shown to a user) at the same quantity/format/duration/etc. of the advertising Meta currently conducts. (In other words, Meta could not calculate this figure by assuming it would show many more ads, or longer, more arduous, or otherwise different ads to users who withhold consent than those who grant it, as that would be a form of degradation of the product.) Such a fee would capture the value Meta could lay claim to without requesting any user consent, and which it would forgo in an ad-free service. It thus would be a good benchmark around which to base what "reasonable" fees the company would be entitled to. If Meta chose instead to offer a no-consent option that included some advertising, the revenue those ads generated would subtract from the price Meta could charge on top to users. Meta should provide a single alternative to users alongside the baseline we propose up front. Once it has done so, the company is welcome to offer additional versions to users subject to the same constraints on degradation discussed throughout the paper.

One advantage of this approach is that it minimizes the incorporation of Meta's monopoly profits into the price it is allowed to charge users for consent. The advertiser market for contextual display ads exists across many platforms, creating competition that benefits advertisers.[55] Under our proposal, Meta would have to provide evidence as to the value of contextual ads sold on its platform in order to establish the reasonable price. If it declined to do so, or offered figures based on insufficient or problematic conditions, regulators could use other sites where contextual display ads can be purchased to establish a price. Since Meta's tools are highly developed and advertising on its platform is valuable, the company would have strong incentives to comply rather than risk prices based on perhaps inferior advertising platforms. This approach would certainly generate a lower figure than the annual fee of €72 that Meta is currently proposing for its minimum data-use option.

Finally, observe that unlike Meta's pay or consent model, the fee here is in the context of a wider menu of options. Our baseline option recognises the legitimacy of a business model based on providing services based on advertising. As the Bundeskartellamt explains, the end-user expects the processing of on-platform data.[56] The paid option is likely to be selected by a minority who consider that any type of surveillance is undesirable.

Incentivising More Extensive Data Sharing

Furthermore, a gatekeeper should be free to find means to process additional parameters of user data so as to develop a competitive business model. For this, we think a gatekeeper can provide end-users incentives. Incentivisation is important because the evidence suggests that when users are confronted with a specific and unambiguous choice between higher and lower privacy options, with no incentives either way, they overwhelmingly adopt the higher privacy option. For example, around 85% of American users who were offered Apple's App Tracking Transparency

---

[55] *United States v. Google LLC*, No. 1:23-cv-00108 (E.D. Va. Apr. 17, 2025) (mem.), 58.
[56] Bundeskartellamt, 'Background information on the Bundeskartellamt's Facebook proceeding' (7 February 2019) available at:
https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Diskussions_Hintergrundpapiere/2019/07_02_20219 _Hintergrundpapier_Facebook.html?nn=295782

choice screen opted for the no tracking option.[57] Thus, if Meta wants to maintain its current level of processing, it will need to give users something of value in return for their consent to such processing.

One form of incentive may be for Meta to explain to consumers that with greater data sharing they will see more "relevant" ads whenever they have to view ads. This could work so long as more targeted advertising is perceived by users to contain more useful information. A consumer may hope to see ads for concerts of their favourite band, vacation spots, or other things that cater to their taste.[58] This form of inducement creates an incentive for Meta to ensure that ads stay attractive to users.

Alternatively (or in addition), consumers could be compensated for agreeing to more extensive data sharing. Indeed, the most recent evidence suggests that Meta would likely have an incentive to share profits with users if allowed to do so. Researchers have measured the difference between ads that use personal data generated only from a user's own activity on Meta's platforms and those that use tracked user data from across the internet; these less targeted ads generate fewer clicks and are therefore 37% less effective at the median than those that use full targeting.[59] The implication, should advertisers want to continue to receive similar value for their advertising spend, is that ad prices would need to fall by about 30%. If Meta is allowed to offer users compensation for increased data sharing, both the company and users will benefit.

Such compensation, though, if improperly constituted, poses the risk of coercing users into consenting to share their data. In particular, gatekeepers including Meta must be prevented from offering users any form of compensation that comprises a premium version of their own services. Offering anything akin to such a premium version (unlike cash or a third-party benefit) risks becoming coercive over time. To see this, notice that if Meta is allowed to offer extra features or services to individuals willing to share their data, then sooner or later, due to technological progress, today's premium product will become tomorrow's standard. At that point Meta will in effect be offering a downgraded, below market, service to individuals not willing to share their data. This returns us directly to the problem above. Therefore, it seems prudent to require any benefits the platform offers the user in exchange for data be either monetary compensation or be created by a third-party and consumed off the platform.

Some likely compliant compensation forms include the following: Meta could offer users who choose to share data a discount on their mobile plan cost, access to third party video content, or a subscription to a local news publication. Such compensation reflects the value of the personal data and shares that value with a user who is making a free choice. The forms of compensation we suggest above are also carefully chosen to make them less susceptible to fraud. "Bots" will be attracted to a digital platform that pays cash to users, and this would be a good reason for the platform not to compensate end users with money. The gatekeeper's compensation is more

---

[57] Wetzler, T. (2023, 5 July). *App tracking transparency opt-in rates*. Adjust Blog. https://www.adjust.com/blog/app-tracking-transparency-opt-in-rates/

[58] The sharing of users' personal data with proper consent may generate externalities. See, for example, Bergemann, D., Bonatti, A. and Gan, T. (2022), The economics of social data. The RAND Journal of Economics, 53: 263-296. https://doi.org/10.1111/1756-2171.12407

[59] Wernerfelt, N., Tuchman, A., Shapiro, B., & Moakler, R. (2024). *Estimating the value of offsite tracking data to advertisers: Evidence from Meta*. SSRN. https://doi.org/10.2139/ssrn.4176208

resistant to fraud when it requires that the user subscribe to a newspaper or mobile phone carrier, or watch a film, for example. There are surely many other compliant compensation routes Meta could pursue. Whatever they might be, the burden should be on Meta to prove that any chosen compensation does not entail the degradation of the lower-data alternative(s).

Our discussion of possible forms of compensation in exchange for greater access to user data is implicitly categorizing that benefit as compensation and not as a quality of the service. Therefore, the user who does not get the compensation is not experiencing a degraded service itself. If, as we suggest above, Meta offered Facebook users a discount on a mobile phone plan in exchange for showing them more targeted ads, the users would enjoy no better a version of Facebook than users who did not share their data.

It might be possible to interpret the DMA more narrowly by holding that the entirety of what Meta might offer to its users—Facebook, Instagram, a free car wash every month, a discounted phone plan, etc.—constitutes the "service" the company provides. The consequence of this view is that any user who does not receive any part of that service (even if it is as remote to Facebook as a discount on a bill from Vodafone) because she has not allowed Meta to process her personal data is thus receiving a "degraded" service. This extreme interpretation results in concluding that any benefit to the users who share data would be illegal under the DMA.[60]

Such a position harms competition, consumers, and business users. Effectively forbidding a gatekeeper from offering compensation for sharing personal data will limit choices in the marketplace that would benefit consumers directly through the value of discounts and benefits. Secondly, the ability to offer creatively those choices in new business models provides business opportunities for gatekeepers and entrants alike, and likely helps advertisers who will have more choice in where and how to advertise. More entry and variety in business models in turn helps end consumers in the longer run. Leaving Meta without any legal ability to incentivise consumers to share data would protect Meta's profits, rather than creating conditions that encourage sharing some of that surplus with consumers.

Choice Architecture Requirements

Provided that our proposal is adopted, users would be first asked to choose between the baseline and the no-consent subscription and subsequently Meta would be able to ask about further data sharing. We offer a technical appendix that further explores choice architecture details, but here we offer the most important elements to ensure compliance with the law:

- In any subsequent prompt to request user consent for additional data processing, Meta should always give the user the option to "decide later" or select "not now" and remain the low-sharing option she selected at the original consent moment. (Users often like this option, a preference Meta currently uses to keep users in the high-tracking configuration, as discussed above.)

---

[60] The UK ICO also declines to adopt this stance, noting that "you can incentivise people to give consent in some circumstances, as long as this does not amount to an unfair penalty for those who do not consent." Information Commissioner's Office, 'Consent or Pay' (21 January 2025) pp.37-8. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/online-tracking/consent-or-pay/

- There must be limits on the frequency Meta can ask users to consent, as frequent consent requests would degrade the quality of the service to non-consenting users. There could also be required time delays between consent moments if Meta attempted to overwhelm users in order to obtain consent. (The inclusion of the "not now" option would also help to mitigate against such a strategy.)
- There should also be symmetry in any repeat asks to users. If Meta repeatedly asks users to consent (subject to the limitations imposed in the previous point), it should also ask users to review any consent they have already given and allow them to withdraw such consent with no greater difficulty than the process by which they consented to it.

These requirements together will help to ensure that users are given compliant consent options and could form part of a specification decision from the Commission.

An Alternative Proposal: A Free, No-Consent Option?

We note that the EDPB has adopted an Opinion that for large online platforms, the only way a user can make a free choice is if the user can select a *free* alternative that does not require any consent and is also not degraded.[61] In Meta's case, the EDPB's Opinion would require the company to offer a free service without any personalised advertising (or any other consent-required data use). We disagree that this setup is the only way to ask for user consent and think our proposal throughout is consistent with the Commission's and the DMA's demands.[62]

Our proposed solution also has a number of advantages over the more extreme alternative. First, it avoids bizarre legal conclusions, such as that gatekeepers are prohibited from making granting consent more difficult for users than withholding it. In addition, though, our proposed solution will likely result in better outcomes for consumers who want to continue to use involved digital platforms by safeguarding their right to free consent without eliminating healthy business models.

The use of activity on Facebook to advertise to users (all that is allowed under our proposed baseline) is similar to many forms of advertising users encounter daily on- and offline. People are accustomed to having enterprises use their activities on-site to advertise to them (whether that be a physical place, a publication, or a website). As illustration, a person who booked a cruise with a travel agent would likely not be surprised to receive a flyer from the cruise line advertising activities available on the upcoming journey. Analogously, a user who engaged in a Facebook discussion with friends about their cruise and "liked" their photos would not be surprised to see an ad for cruises the next time they return to Facebook. Obtaining consent, then, for this kind of targeted advertisement, should not be confusing or exploitative for users.

---

[61] European Data Protection Board. (2024, 17 April). *EDPB: 'Consent or Pay' models should offer real choice*. https://www.edpb.europa.eu/news/news/2024/edpb-consent-or-pay-models-should-offer-real-choice_en
[62] Meta (above n 4) para 156 adheres more to the EDPB view, but other passages suggest more flexibility, see e.g. para 133. It would be a mistake to read the decision as compelling one route to compliance because this is not the function of non-compliance decisions: it is for the gatekeeper to propose fresh compliance offers, such as our proposal. See DMA, Art 29(5) and (6)

At the same time, requiring large online platforms to offer their products for free without any personalized advertising could have significant negative implications for firms' ongoing businesses including for future innovation. It also risks undermining advertising-funded services by DMA gatekeepers and other companies more generally.[63] Given that the value to firms of preserving some personalised advertising is great and consumers experience this limited form of personalisation in many markets, we consider that our approach strikes a more proportionate balance, while significantly benefiting consumers relative to Meta's current proposals.

Conclusion: Procompetitive Control of Personal Data

The European Union's data protections in the GDPR and the DMA serve both procompetitive and privacy protection ends. Through a close examination of Meta's compliance efforts to date, we offer a model for bringing the company in line with European Union law while preserving the model of ad-supported social networks. Among the most important features of the model is a path towards procompetitive control of personal data.

To recap, the model includes three options with these key features:

1. Users should be offered a baseline setting that aligns with their reasonable expectations for the use of their personal data on the product. For Meta's case, we propose a baseline setting that asks users to consent to the processing of *on-platform* data to advertise to them *on-platform,* but that prohibits the combination of user data with any *off-platform* service or the collection of user data *off-platform*.
2. Users who want to restrict the use of all personal data should be offered the product in exchange for a reasonable fee. For Meta's case, this offering could be a no-consent-required ad model or a no-ad model, as long as no user data is collected, combined, or used in ways that require user consent. For the "no ads" fee to be noncoercive, it should be based on the value of the contextual ads Meta could sell but does not.
3. Designated gatekeepers providing core platform services that would like users to share greater amounts of personal data can develop compliant ways to share the proceeds of access to those data with users to incentivise such sharing. We propose that incentives to share data are compliant whenever they do not affect the service offered to users. This rule prevents the platform from degrading the service to users who do not consent to greater data sharing. Incentives that take the form of third-party services or benefits consumed off the platform will comply with this rule.

Looking forward, if consumers gain benefits (negative prices) from sharing data collected through tracking as a consequence of the regime created by European Union law, the future might deliver functional, non-exploitative markets for access to personal data, even when

---

[63] Such a position also has the downside of potentially constraining innovation in ad-supported technologies by mandating that covered platforms offer a specific configuration of advertising that, while perhaps potentially appropriate in this specific case, may not properly anticipate future developments in the ad-supported internet. The EDPB's reference to "large online platforms" is a potentially wider category than the DMA's "gatekeepers," for which there is a formal designation process, meaning the application of such a ruling could be much broader than those under the DMA.

dominant firms are involved. Furthermore, because there are many places and ways to advertise and otherwise use personal data, companies in this space would likely innovate in ways to compensate users for their valuable consent, and inventive mechanisms could grow out of this competitive dynamic. As of now, Meta and other gatekeepers who reap large monopoly profits from complete data control have enormous financial incentives to prevent such a regime from taking hold. Indeed, the resistance to a neutral choice architecture in and of itself suggests that gatekeepers anticipate the emergence of such procompetitive conditions if the law is so enforced.

Technical Appendix

The following appendix has four parts and is meant to expand on technical details touched upon above. The first continues the discussion of choice architecture under our proposed system to flesh out more of its details and user experience. The second expands on empirical testing that could be required or undertaken to examine whether certain designs are coercive and whether users are in fact informed in their consent to have their data processed. The third broadens the focused discussion in the paper to fashion a basic data-price frontier and illustrate how a functioning data market might work to the benefit of users and firms under European Union law. Finally, the fourth includes images of the user experience of Meta's choice architecture as it currently exists.

Choice Architecture Expanded

One obvious choice architecture for our proposal would map on very closely to what the company currently offers, just with the options slightly changed. Where Meta currently asks users to decide between a no-ads subscription and an ad-supported experience, Meta would instead ask users to decide between (1) a no-tracking subscription (with no personalised ads and a reasonable fee or contextual-ads for free) or (2) a free ad-supported service that uses only on-platform user data.

In a second choice screen, perhaps offered at a second visit, Meta could present users in the low data free option with a second choice to opt into the high-tracking, high-personalisation experience. This would likely need to involve an offer of some compensation to incentivise uptake (though of course the company would not *have* to offer compensation as long as it presented users with a compliant choice). Notably, this second option would differ from Meta's current second option both in that it would map on to tracking levels, not just ad experience, and that users would be defaulted to the low tracking (on-platform only), not the high one.

If Meta wished to make other consent requests of users after the initial choice, it would also be entitled to do so, as long as each additional consent moment was compliant (the addition of more and more consent moments will quickly become burdensome to a user, decreasing product quality and also risking user exhaustion). The most important aspect of any additional consent moment would be that users remain defaulted throughout future decisions to the initially compliant choice they made between subscribing and low-data advertising unless and until they give compliant affirmative consent to a different option.

Throughout the development of both the initial consent moment and any additional ones the company would like to offer (such as the high-tracking, high-personalisation experience), the burden will be on Meta to prove that its design is compliant, potentially including empirical testing, which we discuss below.

Alternatively, Meta could argue that users should be presented with all choices at once, though it would have to be careful that users could still make a specific, informed, and unambiguous decision, which could become more difficult as the volume and complexity of information presented to the users increased. This option may potentially be acceptable if Meta only wants to offer users three configurations (i.e., subscription, on-platform-tracking for free, off-platform-

tracking for free), but the burden would be on Meta to show compliance. However, the various types of collection Meta currently might use for advertising (location services, Bluetooth, cross-site tracking, cross-account tracking, etc.) would pose problems for single-choice compliance. While we have mainly focused on cross-site tracking here, as that is the type of collection to which Meta's current architecture draws attention, all of this collection and combination of data across many consent moments deserves appropriate scrutiny under the law.

Empirical Testing

Empirical data will be crucial for understanding not only user preferences, but also to determine whether companies are offering users compliant choices for data sharing. In many cases, it will make sense to place testing requirements on firms to justify their choice architectures and understand user preferences.

For example, in order to determine whether a choice architecture is soliciting compliant consent from users, Meta could be required to test whether users actually understand the decisions they are making, perhaps by holding interviews with users some weeks after their initial decisions to see how well they understand the data Meta is collecting on them and how their choices affected the level of processing.[64]

In another example, our position throughout this paper is that users should not be offered different versions of Meta's services based on whether or not they consent to share personal data because permitting differences in the versions allows for the strategic degradation of the no-consent version to coerce users into sharing personal data. Differences in the design of ads shown in the personalised and less personalised version of Facebook (as in whether they are embedded in a user's feed or displayed as unskippable timed windows) are in our view not compliant with the law, which prohibits offering a better service in exchange for data. If courts or regulators disagree with our general position and allow *in principle* differences in service depending on the level of data users consent to share, at the very least the burden is on Meta to prove that those differences do not degrade the service available to users who do not consent to share personal data relative to those who do (in effect coercing users to share their data, which is prohibited under the DMA).

Meeting this burden would require that Meta provide data to the Commission and the public illuminating the effects of its design choices. This proof should be available in the public version of the compliance report Meta must submit under the DMA. Evaluating the presence of coercion may require experimentation. For example, determining whether choice architecture is clear and neutral can be determined with A/B testing. Meta is capable of evaluating possible choice architectures and measuring user responses under the supervision of the regulator.

The Data-Price Frontier

---

[64] For a more detailed discussion of incorporating consumer responses to choice architectures into regulatory obligations, *see* Lauren E. Willis, *Performance-Based Consumer Law*, 82 U. Chi. L. Rev. 1309 (2015).

Taking a broader view of the choices Meta must make, the analysis here reflects the negative relationship between data processing and price exhibited by users. As noted above, when users are offered a simple and free chance to opt out of data processing, they do. Services charge users when they request a level of data processing even lower than the broad requirements of European law or an experience otherwise beyond it (e.g., not seeing any advertisements and not processing data, even for purposes allowed without consent). On the other end, users are compensated when they consent to offer high amounts of personal data that exceed that which they reasonably expect to share in a service.

Figure 1: The negative relationship between level of consumer data shared and consumer price

Data-Price Frontier

No personal data shared (or less than permitted)
Price > €0 (Subscription)

User consents to baseline
Price = €0

Current Facebook default

User consents to share additional personal data
Price < €0 (Benefit)

Price

Level of Consumer Data Sharing
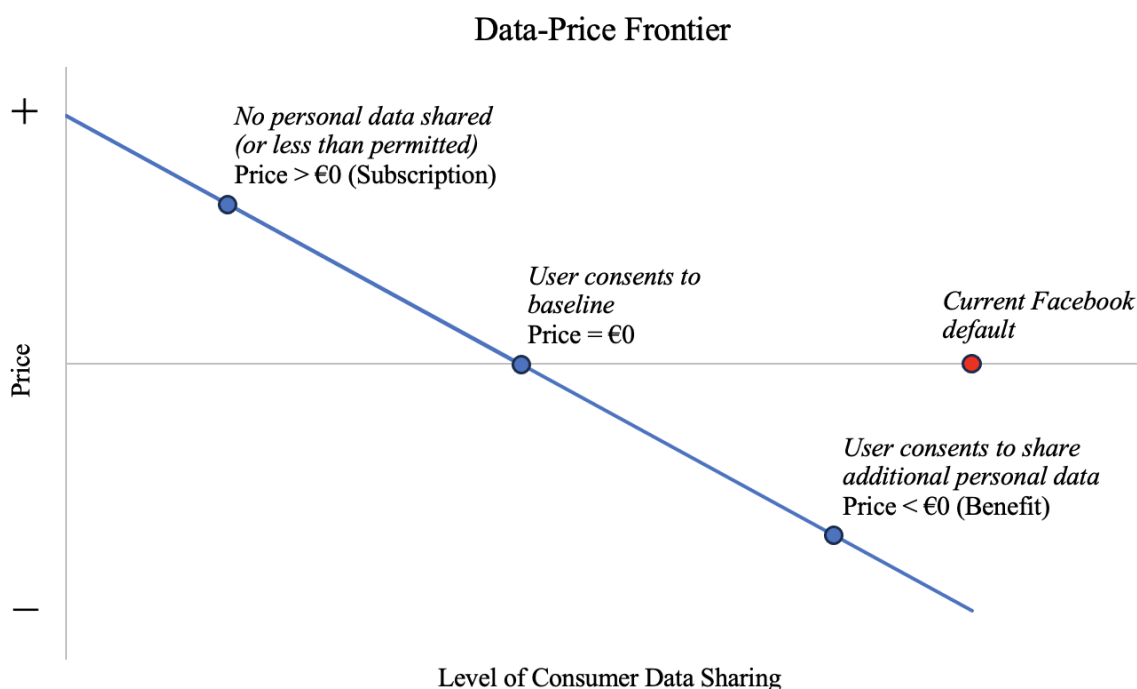
Today, the data-price frontier is still in its infancy, as individuals' data rights are still developing in Europe and beyond. Part of this development is apparent in the question of where the 0 mark lies on the x-axis—that is what level of data sharing should be consistent with a price of zero (rather than a negative or positive price). The analysis above tries to provide an answer to that question. The more conservative option we describe is when the divide is the level of data processing allowed by the law without requiring user consent, as consent indicates that users are being asked to share something of value, for which they should be compensated in a competitive market, whereas price indicates users are getting something of value in exchange for money. In practice, however, two challenges remain. The first is political (in the sense that it is subject to the political process and public debate), which is that the newness of robust privacy and data protections entails some uncertainty about the ideal and actual bounds of the law. The second is more endogenous, because different users derive different levels of value from different platforms, meaning the point of equal tradeoff shifts. Instead of a fixed line, then, regulatory practice should probably recognize something more like zones of prices along the frontier. The discussion of user expectations in courts is likely to be a fruitful way of establishing dividing

lines, as we have tried to do here, on which kinds of data processing belong in which categories. In addition, empirical evidence will also be invaluable in discerning user preferences and company strategies.

Current User Experience of Privacy Settings

We provide below some examples of the text and settings that users must navigate in order to enable privacy-protecting features on their accounts and decide what versions of Meta products they would like to use. The selection is not exhaustive. Interested readers are encouraged to explore Meta's settings themselves, whatever version of Meta products they use.

Image 1: Text Explaining the Different Versions of Meta Products (Facebook and Instagram)

Image 2: Text explaining the difference between personalised and non-personalised ads[65]

Image 3: Describing the types of information Meta collects based on activity (note that it makes no mention of 3rd party data, presumably because those data are not from "activity")

Your activity and information you provide

On our **Products**, you can send messages, take photos and videos, buy or sell things and much more. We call all of the things you can do on our Products "activity." We collect your activity across our Products and **information you provide**, such as:

- Content you create, like posts, comments or audio

- Content you provide through our camera feature or your camera roll settings, or through our voice-enabled features. **Learn more** about what we collect from these features, and how we use information from the camera for masks, filters, avatars and effects.

- Messages you send and receive, including their content, subject to **applicable law** . On some Products, you can use end-to-end encrypted messages. **Learn more** about how end-to-end encryption works.

- **Metadata** about content and messages, subject to applicable law

- Types of content, including ads, you view or interact with, and how you interact with it

- Apps and features you use, and what actions you take in them. **See examples**.

- Purchases or other transactions you make, such as through Meta checkout experiences, including credit card information. **Learn more**.

- Hashtags you use

- The time, frequency and duration of your activities on our Products

- Views of and interactions with a Facebook Page and its content, to provide the Page admin with aggregated information about how people use their Page and its content. Meta is jointly responsible with Page admins. **Learn more** about the joint processing for Page Insights.

- Your photo or video selfie if you provide it when you contact us for account support

Information with special protections

You might choose to provide information about your religious views, your sexual orientation, political views, health, racial or ethnic origin, philosophical beliefs or trade union membership. These types of information have special protections under the laws of your country.

Image 4: The location users can disable the integration of third-party data into their back-end profiles
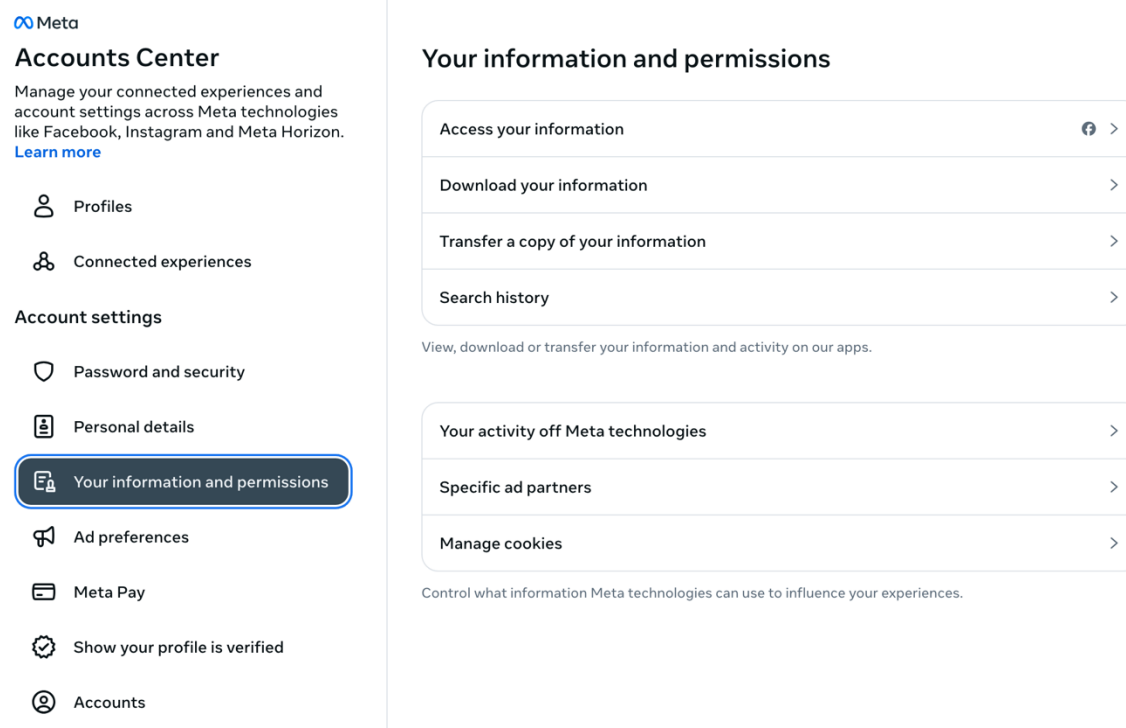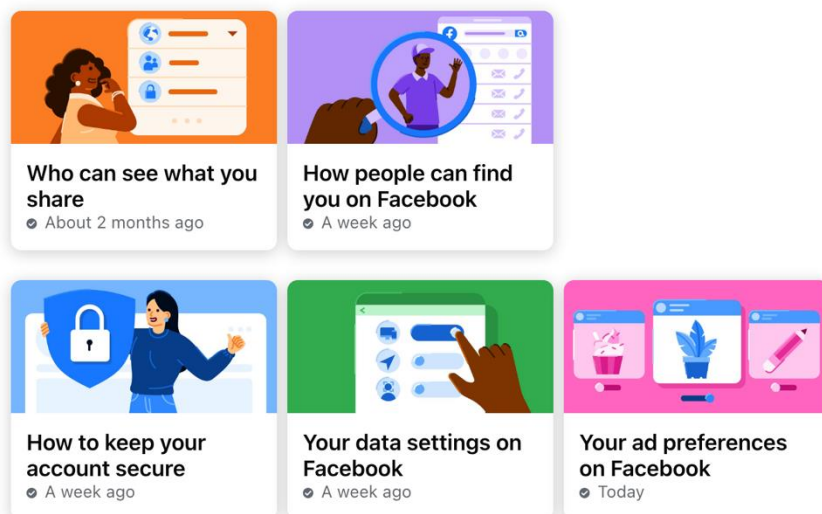

Image 5: A view of the Meta "Privacy Checkup" (note that the checkup does not allow users to change their advertisement settings or disable the integration of 3rd party data into their accounts)
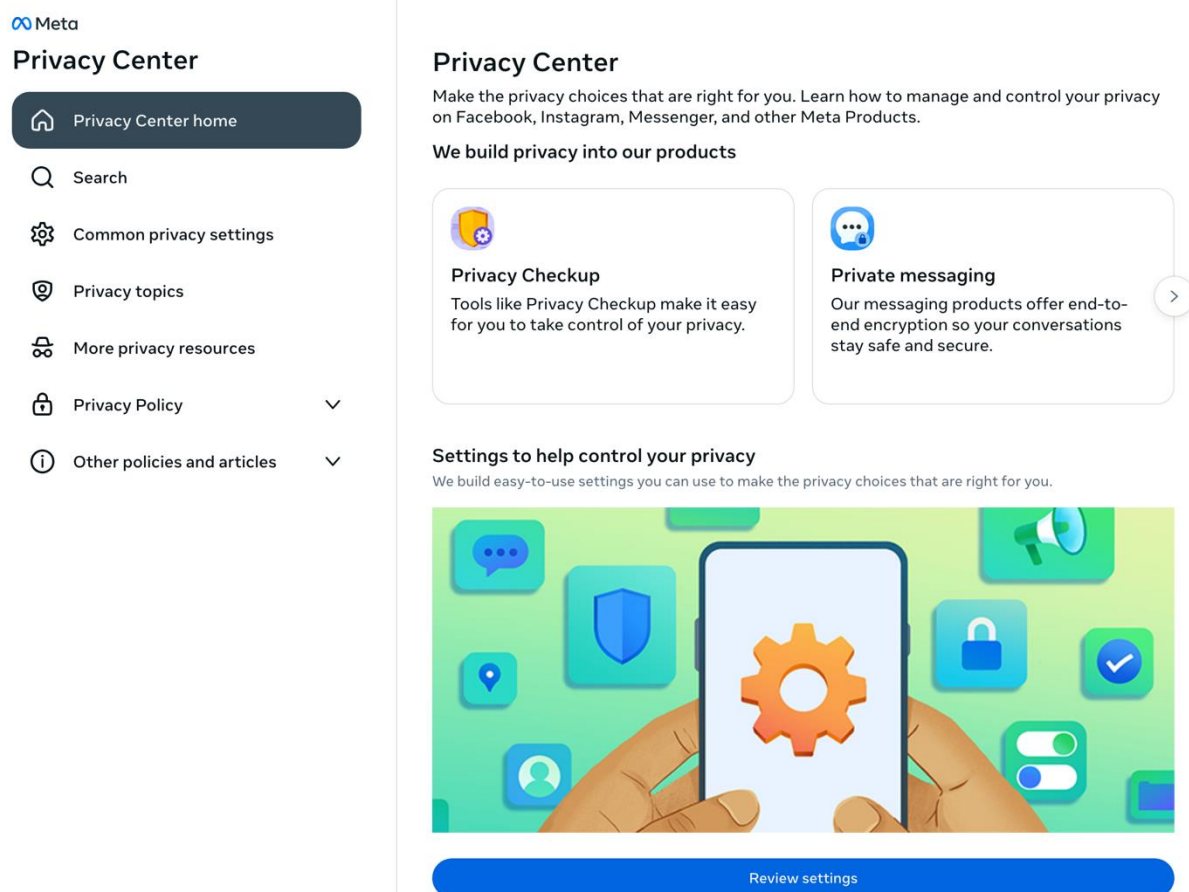
Image 6: The Homepage of the Meta Privacy Center

Author Disclosures for

Meta's Path to Compliant Processing of Personal Data in Europe

Giorgio Monti: Professor of Competition Law at Tilburg Law School and the Tilburg Law and Economics Center and research fellow at CERRE. Pursuant to the Ascola declaration of Ethics, he has co-authored several papers on the DMA with CERRE.

Jacques Crémer: Professor of Economics, Toulouse School of Economics. He has no engagements or affiliations to disclose pursuant to the disclosure policy of the American Economic Association.

Amelia Fletcher: Amelia Fletcher is a professor of competition policy at Norwich Business School, a deputy director at the Centre for Competition Policy, and a research fellow at the Centre on Regulation in Europe (CERRE). She is acting as an expert on two antitrust cases in the tech sector, but these are not closely linked to the issues covered in this paper.

Paul Heidhues: Professor of Behavioral and Competition Economics, Düsseldorf Institute for Competition Economics (DICE), Heinrich-Heine University of Düsseldorf. Within the last three years—in collaboration with E.CA Economics—he has been consulting for E.CA Economics on work done by E.CA for Apple in the context of a competition case unrelated to the policies discussed in this article, as well as engaged in competition consulting in the context of trucking and timber industries.

Nick Jacobson: Associate Program Manager, Tobin Center for Economic Policy at Yale University. He has no other engagements or affiliations to disclose.

Gene Kimmelman: Senior Policy Fellow, Tobin Center for Economic Policy at Yale University and Research Fellow, Mossavar-Rahmani Center for Business & Government at the John F. Kennedy School of Government at Harvard University. Within the last 3 years he has engaged in antitrust and competition policy training for communications professionals, not involving tech sector companies.

Monika Schnitzer: Professor of Economics, Ludwig-Maximilians-University Munich. She has no engagements or affiliations to disclose pursuant to the disclosure policy of the American Economic Association.