

DIGITAL REGULATION PROJECT

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

Policy Discussion Paper No. 11¹
March 18, 2025 (Working Draft)

¹ The Tobin Center for Economic Policy at Yale hosts the papers of the Digital Regulation Project as a way for some of the world's leading economists and regulatory experts to present policy recommendations, based on their relevant research and expertise. The Tobin Center does not take policy positions and therefore the content does not represent the positions of the Tobin Center or Yale University; nor does it represent the positions of any other institution with which any of the coauthors are affiliated

Introduction

Since the passage of the Digital Markets Act (DMA) in the European Union and the subsequent designation of Meta as a gatekeeper, the European Commission and the company have been working to bring Meta into compliance with European law. 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).¹ Article 5(2) of the DMA specifies that gatekeepers may not process or combine certain data (especially third-party data) without specific user consent, as defined in the Regulation. The Commission is currently investigating Meta for noncompliance with this article, and the company has made a sequence of changes to its services and user choices in response to the regulation and subsequent noncompliance investigation. The most recent proposal from Meta is from November 2024 and is the subject of our analysis throughout this paper.²

Meta’s November 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 is unlikely to be compliant with the DMA. We explain why, in principle, Meta’s choice to offer a menu of options with different levels of data sharing is an excellent method of delivering privacy choice to users. However, by omitting or obscuring choices about data processing and steering users into the most data-intensive option on the menu, while making it difficult or unpleasant for users to select a more private choice, Meta’s current menu of options does not provide the user with an appropriate consent environment, nor sufficient protection of users’ fundamental rights.

We begin by discussing the requirement of “free choice” under European law, which is the standard for compliance. We then assess Meta’s approach to compliance, using Meta’s most recent compliance report and explaining what the user experience looks like. Building on the current user experience and Meta’s progress, we then describe a path forward for regulators and the company. Throughout the paper, we articulate three policy findings with regard to bringing Meta into compliance with European law: (1) Meta’s current menu, though a step in the right direction, is not compliant, (2) giving consumers value in exchange for data can be compliant, but not if the value relates to owned services, and (3) Meta already allows users to construct a more private, and free, version of its services that may well be complaint, but only if the company makes that version the default user experience.

The Legal Requirement of “Free Choice”

Under both the GDPR and the DMA, consent (for the processing of protected data) is only valid if users offer it when confronted with a *free* choice. This raises the question of what free choice requires. It has to satisfy at least two criteria.

¹ 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.

² The conduct at issue in this Article may also be a violation of EU competition law, but our analysis is limited to DMA enforcement.

First, for a choice to be considered free, the choice needs to be informed and easy to make, which follows from the GDPR requirement that consent, as defined by Article 4(11) and clarified by Recital 32, must be “freely given, specific, informed and unambiguous.” The GDPR thus rules out choice architectures in which users need to go through a lengthy privacy policy to find out what the various choice options obtain; inasmuch as users do not do so, their choice simply is not informed. And the fact that the choice be unambiguous rules out the use of a service that does not explain what data is collected, and whether it is used for showing ads or other purposes. This interpretation is reinforced by the fact that the DMA adds, in Article 13(6), that gatekeepers cannot make user “choices unduly difficult.”

Second, a free *choice* requires the lack of coercion. As a legal matter this means that a service that had historically been offered by relying on extensive data collection from end users must now, after the DMA, be offered without the data collection activity. The Digital Markets Act is specific about the right a user has to access a similar quality service if they do not want to share their personal data. Recital 37 says:

“The less personalised alternative should not be different or of degraded quality compared to the service provided to the end users who provide consent, unless a degradation of quality is a direct consequence of the gatekeeper not being able to process such personal data or signing in end users to a service. Not giving consent should not be more difficult than giving consent. 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. In particular, consent should be given by a clear affirmative action or statement establishing a freely given, specific, informed and unambiguous indication of agreement by the end user, as defined in Regulation (EU) 2016/679. At the time of giving consent, and only where applicable, the end user should be informed that not giving consent can lead to a less personalised offer, but that otherwise the core platform service will remain unchanged and that no functionalities will be suppressed.”

We see that Article 5(2) and Recitals 36 and 37 of the DMA require the provision of an option that does not involve the processing of off-platform personal data and which provides the users who choose it with a service equivalent to the one provided to users who share personal data. While the recitals are clear about the core platform service being “unchanged,” they do not say anything about cost.

Giving users the choice not to share personal data could result in Meta earning a lower profit than it did when the legal regime allowed it simply to take the data and use them to target advertising; this is because some users will choose *not* to give Meta access to their data. The lack of rules governing personal data that characterized the environment in which Meta’s business model was invented has changed. Users formerly had no control over a gatekeeper’s ability to collect and process their personal data, while today they do. Naturally, a business profiting from using a free input will become less profitable when that input is no longer available. Though the law could limit the profits available to a gatekeeper, it balances the individual's right to protection of their personal data (Article 8, Charter of Fundamental Rights) with firms’ freedom to conduct a business (Article 16 Charter of Fundamental Rights). Importantly, a firm is still free

to conduct its business by using personal data; but it must secure consent from the user because the input it wants to use is sensitive.

It is also relevant to recall that the DMA was introduced because conditions in the digital sector allow gatekeepers to benefit excessively from their market power. Therefore, a rule that requires users to compensate the gatekeeper for profit losses from collecting data would not fix this economic imbalance (in addition to failing to be a free choice under the DMA). This explains why Meta's choice to charge users a fee for accessing the service without handing over their data fails to comply with the DMA.

Before moving on to examine Meta's actual offerings, and acknowledging that there are many compliant versions Meta could make available, we note that Meta already provides one free and (possibly) compliant option, which we recommend as a default in the arguments below. The basic features of this already existing option are that (1) Meta does not process or collect data on users from outside the relevant Meta platform (e.g., Facebook) for advertising or other purposes, and appears not to process any (or very little) data that requires explicit user consent, (2) users are given access to the full user experience available to other users, and (3) users can freely select this option (though, as we note below, it requires considerable effort to find it).

A user who has turned off all the personal data options offered by Meta will experience a version of the service which intersperses ads in a user's feed that rely on legally-acquired personal data and contextual data, all without processing data from off the relevant Meta platform. These types of ads are in the format Meta customarily uses, and are similar in targeting to those Meta showed in the years before it developed the technology to track users around the open web. Meta's long usage of these ads demonstrates that they are technically and commercially feasible. The existing availability of this option without a monetary charge strongly implies that a compliant version of the service cannot contain more ads, or ads that interfere more with the user experience, than the one for which personalized ads are shown.

Assessing Meta's Approach to Compliance

In light of the general structure of "free choice" above and its application to Meta's platforms, we now turn to assessing Meta's offerings and defences to comply with the GDPR and the DMA.

Meta's Past Approach

In October 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. Users who did not subscribe were deemed to have consented to the version with full tracking for targeted advertisements, which has been the standard version that Meta's platforms have always offered. Regulators and observers quickly identified the new system as "pay or consent." While "consent" users 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.³

In the aftermath of this announcement, both the European Data Protection Board⁴ and the European Commission⁵ 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 and a paid subscription service does not represent a choice at all. A high-enough price is equivalent to not offering a choice, and since control of personal data is a right, needing to pay for it is inconsistent with the law. 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.⁶ 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 March of 2024, the European Commission launched a noncompliance investigation into Meta for failing to meet its requirements under the DMA, the preliminary findings (June 2024) for which are cited above.⁷

Meta’s Current 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.⁸ 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 1, the new option (free services supported by the new type of ads) which is option 2, and the subscription offer (a service that carries a fee but no ads), which we denote as option 3. 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 have the option to opt out. In the same November 2024 update, Meta also reduced the 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

³ These categories include personalising 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/>

⁴ 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

⁵ 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

⁶ 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>

⁷ European Commission. (2024, March 25). *Commission opens non-compliance investigations against Alphabet, Apple, and Meta under Digital Markets Act*. Directorate-General for Competition. https://digital-markets-act.ec.europa.eu/commission-opens-non-compliance-investigations-against-alphabet-apple-and-meta-under-digital-markets-2024-03-25_en. For the findings, see note 5.

⁸ 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/>

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.

Assessing Meta's Approach

The menu hews closer to the requirements of European Union law, but we see three immediate problems.

1. Ad Type v. Processing of Personal Data

First, these options are differentiated by ad type, not by level of processing of personal data, while Meta's choice architecture conflates the two. 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. While the options do determine the kind of ads users (do not) see, they appear to have little relationship to the amount of data Meta processes about those users—both on and off Meta technologies—except for the single purpose of advertising. Yet users selecting between the three options likely expect their selection to influence this level of overall data processing. If Meta gathers personal data it does not need—because the user is receiving less personalized (or no) ads—the company may well be violating the data minimisation principle of the GDPR (Article 5(1)(c)). If the personal data are being processed for another reason, as appears to be the case according to the Privacy Policy, the user must give clear and affirmative consent to use the data for a purpose that is not advertising unless the data processing is necessary for the performance of the contract between Meta and the user.⁹

Within the descriptions of the three options, users are shown material that could cause them to believe that Meta is not processing the incremental personal data, particularly third-party data on the user. According to the company, Meta's free "less personalized" version 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."¹⁰

Users are likely to make an inference that a service with ads that do not *use* personal or third-party data is a service where such data are not *gathered*. The intuitive relationship between data sharing and ad personalization arises because businesses normally spend resources collecting information that they plan to use. Additionally, users might expect that only data necessary to serve the desired ad type will be collected because of the data minimisation principle in the GDPR. Exploiting this user intuition makes Meta's offer potentially misleading. Offering less personalized ads as an option in a privacy menu—without changing the intrusive level of data gathering—is a tactic that can successfully confuse users (who would need to opt out twice, once for personal data for advertising and then again for personal data for another use).

⁹ It is beyond the scope of the paper to analyse whether Meta can rely on the other legal bases in Article 6(1)(b)-(f) of the GDPR, which allows for data processing to e.g., perform a contract, comply with a legal obligation, or pursue a legitimate interest.

¹⁰ 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/>

Why would Meta continue to collect personal data if the user has chosen not to see ads based on those data? There are a number of possible business reasons that such data could be useful to a company. For example, Meta may want to use as much data as possible to train its algorithms. For this purpose, it would need to ask user consent to process these data. Other uses such as predicting the purchases or interests of friends of a user who has requested privacy, or storing the data in case the user in question reverts to a contract that allows targeted ads would be subject to the same requirement.

2. Difficulty of Access

Secondly, while Meta provides menu options that allow users to limit data processing (not just ad type), the options are difficult to access. The users in all three of these plans can navigate their way down the menus that control their personal data to make choices that limit processing. 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, however, 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 privacy settings at all, or with an even longer journey to their destination.¹¹ 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 the 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 1 above), which is identical to the one 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 1 and 2 above). Finally, there is one option (theoretically) 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 turned on until the time of writing.

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

¹¹ The “Privacy Checkup” is misleading in that it will not direct a user to any settings that control the processing of third-party data about users for advertising or other purposes but rather allows users to change their privacy settings in relation to *other users* (e.g., whether posts are public or friends only), not to Meta itself.

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.

3. Problematic Consent Process

Thirdly, 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, Meta does not ask users' consent to process personal data in a way that ensures users are not exploited, as is required by both the GDPR and the DMA. As described in the previous section, if a user properly consents, Meta may lawfully use the resulting personal data for targeted advertising. Consent, however, is not valid if a user is coerced, regardless of what text is used in the consent process. A data processor's market power is highly relevant because that power can be used to coerce users. The DMA gatekeeper platforms have tremendous market power and therefore must be very careful in how they seek consent. In the case of Meta, a user wanting to check up on their friends on Instagram or Facebook has no other place to go if friends do not post information about a recent wedding or holiday on LinkedIn or YouTube. 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.

Meta's current consent process does not appear to satisfy the requirements of the GDPR and the DMA. As discussed above, when users join Facebook or Instagram, Meta supposedly interprets their joining to mean that they consent to the processing of third-party data into their back-end Meta profile, though users are never clearly informed of the "choice" they have made.¹² Under the DMA, if personal data Meta is collecting come from off of the platform, such as a user browsing the open web or another business's website, then the DMA requires Meta to obtain consent from those users before the gatekeeper combines those data from different sources. Without properly-obtained consent, it is illegal for Meta to merge personal data from its own platform (e.g. Instagram) with personal data from users' activities that the users may think are private (e.g. browsing a labour union's website or buying a medication).

After the account creation, a user is asked to make a (potentially) two-step choice. Until this choice is made, the user will not be shown any ads. 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 choice between "personalised ads" and "less personalised ads" with brief descriptions of the different options.¹³ As described above, however, there is no link to or discussion of the various data options available in the Accounts Center as described above. If, later, a user wants to change

¹² In fact, joining Facebook does not even require being confronted with the long text full of legal language. Users are only [reminded](#) in small print that "By clicking Sign Up, you agree to our [Terms](#), [Privacy Policy](#) and [Cookies Policy](#). 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 this setting, though we have not confirmed that they are.

¹³ Before taking users to this second choice, Meta presents them with an option not to make this choice, in which case they are automatically placed in the "personalised ads" plan. This ability is problematic because users may think they are simply deferring a choice, but Meta interprets this decision not to review the setting as consent to put the user in the "personalised ads" plan until they decide otherwise (which Meta never prompts them to do).

that decision, that option is available in the Accounts Center as well, though users in our testing are not prompted to reevaluate.

One reason this series of choices is problematic is that the DMA does not allow a gatekeeper to coerce a user into sharing personal data by offering a “degraded” version of the service. The law is unclear on whether charging money falls in this category, though the European Data Protection Board (a body created to ensure consistent application and enforcement of the GDPR) has issued an opinion that it generally does, on the grounds that users should not be charged money to exercise a fundamental right.¹⁴

Another issue is whether the changed advertising format of option 2 makes that version “degraded.” Under the “less personalised” version, Meta claims that users will be shown advertisements that draw on a more limited set of data points, including basic demographic and geographic information, user device usage, and the user’s current browsing experience, as opposed to the whole history of user posts and interactions on Meta platforms used under option 1. It remains unclear, however, whether any fewer data are *collected* on individuals in option 2 versus option 1, though it does appear to be the case that third-party data are not *used* to advertise to “less personalised” users. In addition, Meta notes that some of the ads shown to users in option 2 will fill the whole screen and be unskippable, whereas regular ads appear in a user’s feed and can be scrolled past in the conventional way. If a user selects option 1, Meta interprets this choice as a general consent to use effectively unlimited amounts of personal data for targeted advertising.¹⁵

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. Importantly for regulators, the extent to which option 2 constitutes a real degradation to actual users can be determined with empirical examination of user behaviour. If users are offered the current options 1 and 2 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 2 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.

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) continues to fail to secure the form of thoughtful consent these regulations require, the updated menu falls short of compliance under current law.¹⁶ Further, if the intrusive ads in option 2 are effectively coercion designed to drive users to share their personal data, then those users do not experience meaningful choice. Additionally, a degraded service—such as the one resulting from having to

¹⁴ European Data Protection Board. (2024, 17 April). *EDPB Opinion 2024/08 on Consent or Pay*. EDPB. https://www.edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf

¹⁵ Meta Platforms, Inc. "Privacy Policy." Facebook, accessed March 12, 2025. https://www.facebook.com/privacy/policy/?entry_point=facebook_settings.

¹⁶ Unless Meta can use a different grounds specified in the GDPR that allows data processing.

see more intrusive ads—would be a violation of the law Article 5(2) DMA and under the meaning of recitals 36 and 37.

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 as fully compliant with the DMA.¹⁷ It claims that the introduction of what we refer to as “option 2” is “beyond what is written in the law” and not required by the DMA.¹⁸ Meta also describes the options available to users of the personalised ads version (option 1) to control the data used to show them ads and the types of ads they see. (As noted, all of these settings are on an opt-out basis and are difficult to find.)¹⁹ 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.

The most charitable reading of Meta’s compliance report is that, in the company’s view, giving a user the option to opt out of the data collection and processing that requires consent under European Union law is sufficient to comply with the DMA. As we have explained, there are numerous reasons to reject this view. However, the company’s position is consistent with our suggestion that Meta already offers the foundations of an option that would likely satisfy regulators and courts alike.

Aggregating the collection of opt-outs that Meta already allows into one default free version could bring the company into compliance with European law. These settings include turning off the back-end integration of third-party data into a user’s profile, turning off the use of third-party data for advertisements, turning off the use of Meta’s advertising tools and data on third-party sites, and a few other options. Meta already offers all of these settings to users worldwide without charge. By aggregating them into a default version, Meta would avoid both coercion and degradation.

A requirement that the gatekeeper default users into an option that involves sharing only data that does not require explicit consent would ensure that Meta does not use choice architecture that

¹⁷ 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>.

¹⁸ Meta. 2025. *Meta's Compliance with the Digital Markets Act: Non-Confidential Public Summary of Meta's Compliance Report*. March 6, 14.

¹⁹ Meta. 2025. *Meta's Compliance with the Digital Markets Act: Non-Confidential Public Summary of Meta's Compliance Report*. March 6, 17-22.

hampers consumer choice. If the default choice is less profitable for Meta, it will want to encourage users to choose to share their personal data. Such a structure would give Meta the right incentives to make choosing alternative options easy and hassle-free. Indeed, Meta will want users to engage with the available choices and it may even try and incentivize users to do so. This is an additional benefit to ensuring the default version uses data that do not require consent from users.

By selecting a different default, a version of the service *that it already supplies*, Meta can thus comply with the relevant laws as we understand them. This simple solution seems like it could form the basis of a specification decision under Article 8 of the DMA if Meta continues to fall short.

Preserving Access to Users' Personal Data Under European Law

The clear consequence of our recommendations—and indeed of European Union law itself, whatever the compliant solution Meta ends up offering—is that Meta will no longer be able to process the quantity and breadth of personal user data it used to because users must now freely consent to that processing.

We first note it is important to draw a distinction within this issue: the evidence suggests that securing consent to deliver personalized ads is far easier than securing consent to track users across the Internet. Companies can deliver²⁰ the former with surprisingly little data and a good algorithm, and some evidence suggests users may *prefer* targeted ads.²¹ However, we know that when users are confronted with a clear and unambiguous choice between tracking and no tracking, they overwhelmingly opt for the latter. Evidence from American users offered Apple's App Tracking Transparency choice screen suggests this portion of users may be as high as 85%.²²

However, the data suggest that with current technology, user aversion to tracking across the internet will impose costs on Meta and advertisers. For example, there is evidence about the difference in price Meta can charge between fully targeted ads and ads that rely on less personal data. Researchers have measured the difference between ads that use personal data generated only from a user's own activity on Meta's platforms; these less targeted ads generate fewer clicks and are therefore 37% less effective at the median than those that use full targeting.²³ 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%.

As we discuss above, Meta cannot excuse itself from following the law by citing the lower profits it may earn if it cannot sell as many fully targeted ads. Firms will typically earn less

²⁰ Kelleher, A., Cutbill, D., Lee, J., & Brinker, M. (2021, 19 October). *The future of marketing in a third-party cookieless world*. Deloitte Insights. <https://www2.deloitte.com/us/en/insights/topics/marketing-and-sales-operations/global-marketing-trends/2022/the-future-of-marketing-in-a-third-party-cookieless-world.html>

²¹ Al Qudah, D. A., Al-Shboul, B., Al-Zoubi, A., Al-Sayyed, R., & Cristea, A. I. (2020). Investigating users' experience on social media ads: perceptions of young users. *Heliyon*, 6(7), e04378. <https://doi.org/10.1016/j.heliyon.2020.e04378>

²² Wetzler, T. (2023, 5 July). *App tracking transparency opt-in rates*. Adjust Blog. <https://www.adjust.com/blog/app-tracking-transparency-opt-in-rates/>

²³ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4176208&download=yes

profit when a fundamental right affects their business model. Consider the profit difference between a firm's use of enslaved labour versus workers belonging to a modern union. The former would likely yield more profit, and the firm would lose some of that profit when slavery is outlawed. If the platform has data obtained legally, however, then how much of that data goes into the choice of an ad is a business decision that the data protection laws do not directly regulate in reasonable cases.²⁴

If Meta can no longer push users into sharing their personal data across the web, how then, can Meta convince a user to share data? If the default is choosing not to share data, and most users are comfortable with that, even consumers who are almost indifferent to sharing their data could simply opt out of doing so.

There are two economic answers to why consumers may share their data. First, consumers may prefer to see "relevant" rather than "irrelevant" ads whenever they have to view ads. This would be true, for example, if advertising is perceived by consumers to contain 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. (Of course, the information may also be used to persuade the consumer by exploiting her susceptibility to framing or various forms of persuasion, and consumers could be weary of sharing their data for this reason.) Meta may inform users that argue that option 2 is not suitable for them because they will actively like personalised ads more than less personalised ads. Consumer preference for targeted ads will increase Meta's ability to enrol users in the data-intensive version of the service, making complying with the law less costly. Furthermore, Meta will be incentivized to ensure that ads stay attractive to users.

Second, the consumer could be compensated for the ads they are being shown. For example, some consumers may think that they should share in the financial gain from the targeted ads they are watching because they know those ads significantly raise Meta's profits. Again, Meta may be incentivized to share the incremental profit rather than not earning it at all. A user who did not share her data has access to an undegraded service and will still be able to benefit fully from the network effects. Therefore, attracting users with a payment for sharing their data does not risk Meta exploiting users via network effects.

In this environment, a broader critical question is whether such a benefit to the user is equivalent to offering a better product in exchange for data, something which is explicitly forbidden by the DMA. In one light, the extra benefit—whether it is subscription discount or money—raises the users' utility just as a premium service does (e.g., more prominence for a user's posts). However, our concern with allowing a gatekeeper to offer a premium version of its own service (unlike for money or a third-party benefit) is that over time it is likely to become coercive. If Meta was 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 product. 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

²⁴ If this is a scenario where the gatekeeper *has* processed (even simply collected) *on-CPS* data but refuses to use them for (cleverer) advertising in order to justify vexatious ads, then 5(2) DMA may have a say in terms of possible unjustifiable degradation.

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, or access to 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 without any exploitation. 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 resistant to fraud when it requires that the user subscribe to a newspaper or mobile phone carrier, or watch a film, for example.

Some options require closer study. For example, if Meta offered a gift subscription giving access to certain movies or videos hosted by itself, a decision needs to be made whether not having access to these extra services—movies and videos in our example—constitutes a downgraded service. As a matter of principle, if these videos or movies are part of the social-media conversation, not allowing access to them could constitute a downgraded service. If, on the other hand, they are not part of the social media experience itself but just one of many topics people may converse about, then offering such access would not amount to a downgraded service and could be a permitted form of benefit. Cash or access to completely independent goods or services do not raise any of these issues and therefore, in our view, should fall into a “safe harbour.” Benefits offered somewhere on the Meta properties would require Meta to bear the burden of showing that the service without benefits is not degraded.

Recitals 36 and 37 of the DMA describe the equivalence of the service:

Recital 36: To ensure that gatekeepers do not unfairly undermine the contestability of core platform services, gatekeepers should enable end users to freely choose to opt-in to such data processing and sign-in practices by offering a less personalised but equivalent alternative, and without making the use of the core platform service or certain functionalities thereof conditional upon the end user’s consent.

Recital 37: The less personalised alternative should not be different or of degraded quality compared to the service provided to the end users who provide consent, unless a degradation of quality is a direct consequence of the gatekeeper not being able to process such personal data or signing in end users to a service...

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. The service remains the same. 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.²⁵

Such a position harms competition, consumers, and business users in our view. Effectively forbidding a gatekeeper to offer 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.

Towards a Better Menu

As the European Commission works to bring Meta and other gatekeepers into compliance with European Union law, a number of decisions and opportunities await. Notably, compliance does not require the end of the ad-supported internet or of personalised ads.

Across a wide variety of media products for many decades, businesses and users have been accustomed to contextual ad personalisation relying only on data obtained on the platform on which the ads are shown. Such a use of on platform consumer data allows for a range of viable business models. In its default setting, Meta could continue to choose the ads based on this less-personal data, including contextual data generated by users’ activity on the platform.

It is clear from the discussion thus far that a menu of options that is clear and simple should provide users with tiered levels of data protection (low, default, high) that map cleanly onto ad type (personalized, contextual, ad-free). And this simple menu must be offered to users in a choice architecture that is specific and unambiguous and gives users a free choice without coercion. This final condition implies that the placement and “annoyingness” of the ads and functionality of the service must be sufficiently constant across the menu to avoid coercion. This will be an empirical issue that varies across services but can be easily measured with ordinary course tools used by platforms.

The interesting economic result that jumps out of this menu is that only one option can serve as a default. The data harvesting option requires consent, which in turn requires a choice process that affords consumers a clear basis for making informed decisions; that decision is burdensome for consumers and will discourage participation. But the ad-free option requires payment of money

²⁵ 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.”

which involves the consumer going through a payment process that likewise leads to attrition. This leaves the middle option that does not require active consent on the part of the consumer because they pay no money and the data being used are those that may be used under a legitimate interest justification. This option allows the user the most immediate access to the service. The middle option therefore makes the best default.

Luckily, such an option exists already and is offered by Meta today. A user of the Meta service can enter the privacy menus, as mentioned above, and turn off tracking on third-party websites as well as data sharing with third parties. A user is also able to turn off hardware functions such as the microphone and camera that Meta can use to gather data. Because this version involves processing only data on the Meta platform itself to use in targeted advertising on the Meta platform, such a use may satisfy the descriptions in Article 5(2) above. In the arguments below we assume that a service that minimizes all data sharing using the current Meta menu will satisfy the law without requiring consent.

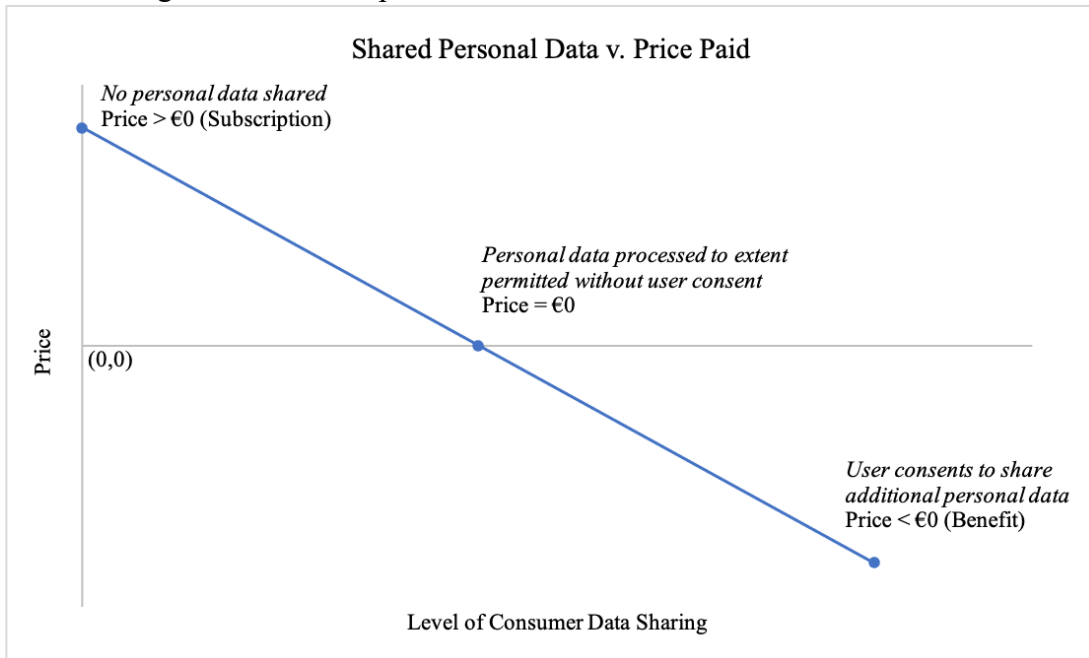
Not only is a “minimum sharing” version likely to satisfy the requirements in Article 5(2), it is also a convenient compliance solution for Meta. Replacing (or supplementing) Meta’s degraded version (option 2) with a legally-compliant version and making it the default is low cost for Meta because all the infrastructure to control these data choices has already been built. The choice is simpler for Meta because it does not need to change the nature of the service. Meta will be incentivized to seek consent with an attractive choice architecture if it wants the user to agree to higher levels of data sharing, including third-party data.²⁶

The result of non-exploitative competition over users’ personal data would be a menu like the one below, with three options affording different levels of data sharing at three different benefit levels, or prices.²⁷ The data sharing under the zero-money option would be at the level permitted by European law without the need for consent. This will be the default version of the service. Consumers could upgrade by purchasing an ad-free service for a fee. The fee represents only one source of value, freedom from ads. The user’s personal data is already protected.

²⁶ Indeed, the “max privacy” version of option 1 is likely to be an improvement for Meta over the current option 2 because it allows the use of users’ personal data from past visits to Facebook and Instagram to target advertising, which should increase value for advertisers. (In Meta’s description of the differences between the two ad-supported versions, the company notes that under the less personalised option, the ads that a user sees each time she opens a Meta product are “not based on the content she viewed while browsing last time.”) See Meta. (n.d.). *Facebook Business Help Center: Manage whether you see personalized or less-personalized ads*. Retrieved March 18, 2025, from <https://www.facebook.com/business/help/468797095528474/>.

²⁷ We draw here from Scott Morton, F. (2023, 13 December). *Meta’s offer*. VoxEU—Centre for Economic Policy Research (CEPR). <https://cepr.org/voxeu/columns/metass-offer>

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



Under a neutral choice architecture, some users might freely choose to share personal data because they do not mind getting zero for themselves while Meta profits from their online activity, but the evidence suggests many will not. If Meta wishes more users to allow the company to benefit from sharing their personal data, it may have to offer them some sort of benefit which might include the enjoyment that comes from personalised ads or a monetary payment. The benefits flowing to businesses that buy the ads would be part of the value that could be shared with users. Users who value the benefit being offered by Meta more than their personal data could choose the data sharing option after going through proper consent.²⁸

Data and Testing

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.²⁹ 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

²⁸ 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>

²⁹ We of course exempt differences that *necessarily* follow from the differences in the amount of data shared, such as the level of personalisation of advertisements.

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.

In the specific context of unskippable ads in a less personalised version of Facebook or Instagram, the Commission can require Meta to report on what fraction of users would choose less targeting if the ads are unskippable full-screen ads and what fraction would choose less targeting if the ads permitted use of past behaviour on the platform but took the usual format. If the gap between the two is large, the regulator may be concerned that the unskippable ads are a degradation of the service. The Commission may find the relative profitability of the different forms of ads relevant to the analysis. For example, if the role of the unskippable ad is to drive the user out of the privacy-preserving group into the data harvesting group where they become much more profitable, this would be problematic. It is possible that a court may decide that, in the case where additional profit *is* earned from the unskippable ads, such profit is not relevant when set against a fundamental right. But certainly if there is no additional profit, this argument cannot be used in the first place.

Meta cannot meet this burden of proof by arguing that unskippable full-screen ads are 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. The concern is the environment within which a user decides which version of the service to choose, not whether the user goes to a different service. This is particularly so when the end-user has no choice to switch because the platform is a gatekeeper.

In light of the significance of the choice problem and the ease with which Meta can answer questions concerning user behaviour with internal data, the Commission will want to require that Meta provide studies or data on these issues. Meta has all the resources—users, data, testing platform—necessary to show that its menu design is not coercive and the service across the three choices is comparable. Again, the data from these tests should be available in the public compliance reports that Meta submits under the DMA.

If Meta refuses to carry out or publicly disclose the needed A/B testing, then an inference that the company's product menu is noncompliant is appropriate because the gatekeeper is not demonstrating compliance, as required by Art 8(1) DMA. Litigation may be additionally revealing through discovery of internal documents. It seems very likely that Meta chose its current menu design after careful internal study. The A/B testing that the company carried out in the normal course of choosing the type of ads to show in each version may show exactly how the choice architecture and product design drives consumers to "choose" the data harvesting version.

Conclusion: Procompetitive Control of Personal Data

European regulators and Meta have a clear way forward to bringing the company into compliance with European Union law. While the current menu is a step in the right direction, a likely route to compliance is the aggregation of the pro-privacy options Meta already gives its users into a default account setting. With this compliant version, Meta will have the ability to offer additional options along the line described above, allowing users to select for greater or lesser data sharing in exchange for positive or negative compensation.

If negative prices for data collected through tracking are the natural consequence of the regime created by European law, the future might deliver functional and non-exploitative markets for access to personal data. Changed defaults combined with neutral choice architecture is likely to require even a dominant firm to offer a share of digital advertising profits to its end-users. Furthermore, because there are many places and ways to advertise, 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. For example, authenticated users might receive benefits like discounts on their mobile bills or a certain number of free in-app purchases. As of now, Meta has enormous financial incentives to prevent such a regime from taking hold, which in and of itself suggests that Meta knows such benefits would be both necessary and very popular with users.

Appendix

We provide below some examples of the text and settings which 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)

The screenshot shows a Facebook Help Center page. At the top left, it says '1/31/25, 11:52 AM' and 'How we show ads in the European Region | Facebook Help Center'. The Facebook logo and 'Help Center' are visible. The main heading is 'How we show ads in the European Region'. Below the heading, there is a paragraph: 'This subscription is only available in the [European Region](#).' Another paragraph follows: 'To comply with regulatory requirements in the [European Region](#), we’re introducing a new choice about how you see ads and use our Products. You can [subscribe to use our Products without ads](#), or you can [use them free of charge with ads](#). We’ve updated our Terms and Privacy Policies to reflect these options. You can review the updated terms and policies here:'

- [Meta Terms of Service](#)
- [Instagram Terms of Use](#)
- [Meta Privacy Policy](#)

If you use our Products free of charge with ads	If you subscribe to use our Products without ads
You will see ads.	You won't see ads on our Products. You'll still see posts, messages, or other branded content from businesses and creators, like if you follow a brand or creator.
You won't pay a fee to use our Products.	You'll be charged a monthly fee. You can learn more about pricing .
Your data will be processed for ads. You'll have access to Ad preferences, including your Ad settings. You'll be able to adjust your ad experience setting to manage whether you see personalized or less-personalized ads. Learn more about this choice . You can review the Meta Privacy Policy to learn more about how we process your data for ads or other purposes.	Your data won't be processed for ads. You can review the Meta Privacy Policy to learn more about how we process your information for other purposes.

We hope that you'll continue to use Meta Products. If you don't want to accept the changes, you can choose to leave our services, and we would be sorry to see you go.

Download your account information before you go

- [Facebook](#)
- [Instagram](#)
- [Meta](#)

Leave our services by deactivating or deleting your account

- [Facebook](#)

Feedback

Image 2: Text explaining the difference between personalised and non-personalised ads³⁰

1/31/25, 11:52 AM

Manage whether you see personalized or less-personalized ads | Facebook Help Center



Help Center

Manage whether you see personalized or less-personalized ads

[Android App Help](#) [Computer Help](#) [iPad App Help](#) [iPhone App Help](#) [More](#) ▾

This option is only available in the [European Region](#).

If you choose to use Meta Products free of charge with ads, you can manage whether you see personalized or less-personalized ads.

Personalized ads

If you choose personalized ads, you can discover products and brands that relate to your interests and activity on Meta Products. Your browsing won't be paused by ad breaks.

We'll use your information for ads, including the following:

- Your activity on our Products, such as if you like Pages or comment on posts
- How you engage with ads, such as clicking or liking them
- Content you view or interact with on our Products
- Topics we think you may be interested in
- Your profile information, such as your age, gender you provide, location, work and education

Learn more about the information we use for ads in the [Privacy Policy](#).

Less-personalized ads

If you choose less-personalized ads, you'll have a different ad experience. You'll see a variety of products and brands through ads that are less related to your interests. Your browsing may be paused by ad breaks. Your ability to advertise and monetize with ads will be limited. Learn more about [these limitations](#).

We'll use some of your information for ads:

- How you engage with ads, such as clicking or liking them
- Your age, the gender you provide and your location
- Your device information, like the device or browser you're using
- Information about the content you're viewing while you browse on our Products.
- For example, Bente opens Instagram in the morning and she scrolls her Feed. She sees ads based on the content she's viewing while she browses. This information is used to show her ads only while she's browsing this time. When she opens Instagram again in the afternoon, she sees ads related to the content she's viewing while she browses this time. Her ads are not based on the content she viewed while browsing last time.

Feedback

<https://www.facebook.com/help/468797095528474>

1/3

³⁰ For a depiction of the user experience on Instagram, see van den Boom, J. (2024, 4 December). *Meta's "less personalised ads": A compliance facade?* SCiDA Project. <https://scidaproject.com/2024/12/04/metas-less-personalised-ads-a-compliance-facade/>.


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”)

1/31/25, 12:16 PM

View and manage the info we've collected about you | Privacy Center | Manage your privacy on Facebook, Instagram and Messenger | Facebook ...

×

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

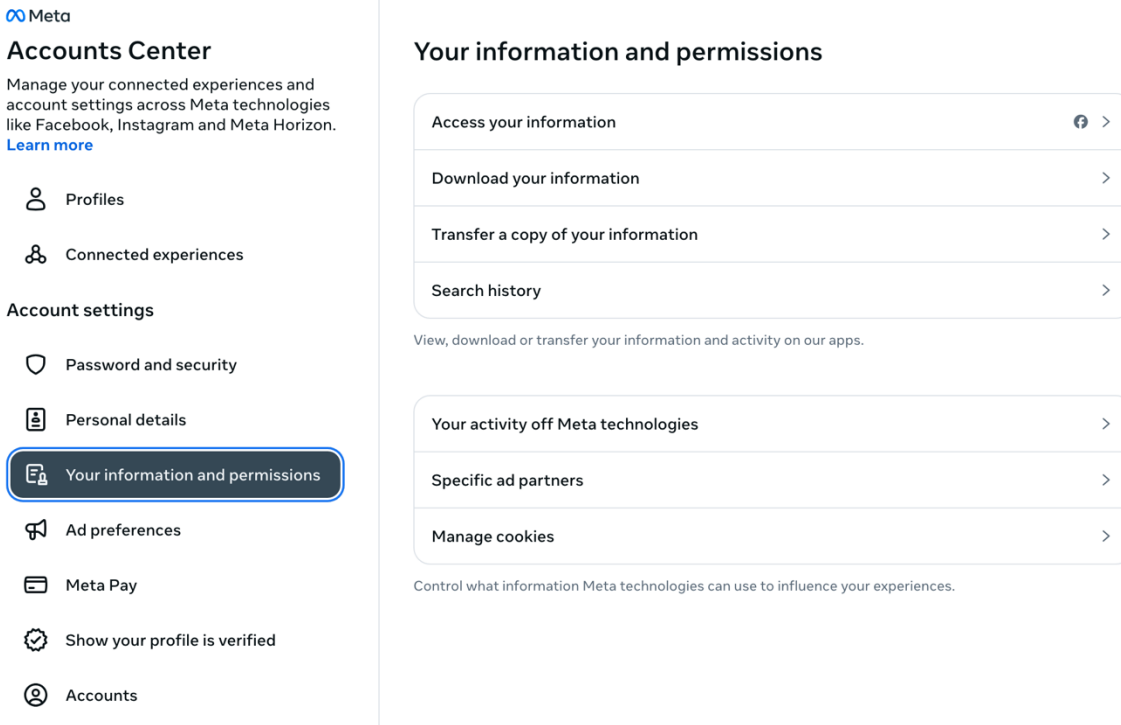
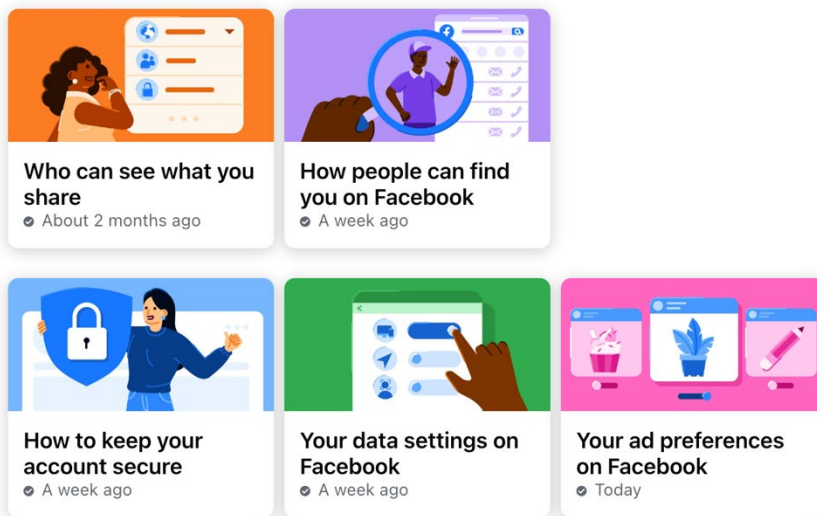


Image 5: A view of the Meta “Privacy Checkup” (note that the checkup does not allow users to change their advertisement settings or disable the integration of 3rd party data into their accounts)









Privacy Checkup

We'll guide you through some settings so you can make the right choices for your account. What topic do you want to start with?



You can check more privacy settings on Facebook in [Settings](#).


Image 6: The Homepage of the Meta Privacy Center

-  Meta
- Privacy Center**
-  Privacy Center home
-  Search
-  Common privacy settings
-  Privacy topics
-  More privacy resources
-  Privacy Policy ▼
-  Other policies and articles ▼


Privacy Center

Make the privacy choices that are right for you. Learn how to manage and control your privacy on Facebook, Instagram, Messenger, and other Meta Products.

We build privacy into our products



Privacy Checkup
Tools like Privacy Checkup make it easy for you to take control of your privacy.



Private messaging
Our messaging products offer end-to-end encryption so your conversations stay safe and secure.

Settings to help control your privacy

We build easy-to-use settings you can use to make the privacy choices that are right for you.



[Review settings](#)

Author Disclosures for

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

Giorgio Monti: Giorgio Monti is 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.

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.