Ilmenau University of Technology

**Institute of Economics**

Ilmenau Economics Discussion Papers, Vol. 32, No. 214

# Neither Privacy nor Competition? – The Economics of "Freely-Given Consent" in Article 5(2) DMA

Nina Lena Färber, LL.M. (Utrecht)† &Florian Hey*

August 2026

Institute of Economics

Ehrenbergstraße 29
Ernst-Abbe-Zentrum

D-98 693 Ilmenau

Phone 03677/69-4030/-4032
Fax 03677/69-4203

https://www.tu-ilmenau.de/iedp/

ISSN 0949-3859

# Neither Privacy nor Competition? – The Economics of "Freely Given Consent" in Article 5(2) DMA

*Nina Lena Färber, LL.M. (Utrecht)†*

*Florian Hey**

**Abstract:** Article 5(2) of the Digital Markets Act (DMA) prohibits gatekeepers from combining personal data across core platform services unless end users consent within the meaning of the General Data Protection Regulation (GDPR). This paper argues that importing the GDPR's consent standard into a competition-driven provision produces a structurally mismatched regulatory design. Drawing on competition economics, we examine the underlying data combination rent and show that this rent, rather than raw data volume, constitutes the primary source of gatekeeper dominance. This rent is economically ambivalent: pro-competitive where combined data improves products, anti-competitive where it serves surplus extraction. Yet Article 5(2) DMA faces user-related constraints for acknowledging its economic ambivalence, because it rather restricts what is harmful only conditionally. We demonstrate that consent, when applied in markets characterized by pronounced power asymmetries, generates predictable welfare losses: entrenching incumbents, fragmenting data ecosystems, and reducing consumer welfare without effectively constraining the rent it targets. In particular, we argue that data-based payment constitutes an economically distinctive mode of exchange that, unlike monetary payment, does not directly deplete disposable income. The resulting two-fold regulatory impasse implies that neither widespread consent nor widespread refusal advances market contestability or data sovereignty. In response, we assess alternatives, including data fiduciaries, data intermediaries, and portability-based data markets, that target the data combination rent more directly. None dominates on all margins. The choice among imperfect institutions is comparative. We conclude that, if data combination is to be governed at all, effective regulation requires instruments calibrated to the economic structure of data-driven markets rather than to the individual autonomy framework of data protection regulation.

**Keywords:** Competition Policy, Consent, Data Combination, Data Sovereignty, Digital Markets Act (DMA), Gatekeepers, General Data Protection Regulation (GDPR), Platform Regulation.

**JEL Classification:** K21, L40, L51

† Nina Lena Färber, Law and Economics of Digitalization, Ilmenau University of Technology, Germany

*Florian Hey, Economic Theory Group, Ilmenau University of Technology, Germany.

## Table of Contents

**1. Introduction** ..... **2**

**2 Economics of data value creation and the role of consent** ..... **3**

*2.1 Data accumulation and its diminishing returns* ..... *4*

*2.2 Data combination rent: from volume to variety* ..... *5*

*2.3 Opaque value of data: the privacy and pricing failures* ..... *8*

*2.4 Consent as an economic instrument: distortions and welfare effects* ..... *11*

2.4.1 Behavioral failures: the limits of voluntary and informed choice ..... 12

2.4.2 Market and competitive distortions ..... 13

2.4.3 Structural ecosystem losses and welfare effects ..... 14

**3 Article 5(2) Digital Markets Act: regulatory impasse and its market consequences** ..... **15**

*3.1 The legal pathway of consent and its structural mismatch* ..... *16*

*3.2 Potential harms for the market as consequences of the regulatory impasse* ..... *17*

**4 Towards best practice: improvements and alternative frameworks** ..... **18**

*4.1 Reforms within the consent framework* ..... *19*

*4.2 Institutional options beyond individual consent* ..... *21*

*4.3 The limits of the alternatives: a comparative perspective* ..... *23*

**5 Conclusion** ..... **25**

**References** ..... **27**

## 1. Introduction

The Digital Markets Act (DMA) (Regulation (EU) 2022/1925) embodies a regulatory intervention in the governance of digital markets, explicitly acknowledging the link between the market power of a few designated undertakings (gatekeepers) and their capacity to leverage data across services (Recital 36 DMA). Among its provisions, Article 5(2) DMA occupies a particularly contested position: it prohibits designated gatekeepers from combining personal data across different core platform services unless the end users have been presented with the specific choice[1] (for an equivalent alternative) and have given consent within the meaning of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679). In doing so, the provision conflates two distinct regulatory regimes – a competition rationale aimed at curbing structural market dominance and a fundamental rights-based instrument premised on individual autonomy over personal data. This conflation is a legal transplant. The GDPR's consent standard, adopted because it was the established European benchmark, was moved into a contestability-driven provision. The result is a structurally mismatched regulatory design – a validity standard developed for bilateral privacy relations now governs a provision aimed at market structure. Meta's highly debated Pay-or-Consent model[2] and the sustained criticism of the proposed Joint Guidelines on the interplay between the GDPR and the DMA[3] exemplify the unresolved difficulties. The pattern extends to enforcement. In its first Article 5(2) implementation decision, the Commission assessed Meta's model exclusively through data-protection reasoning, prompting the observation that the provision risks being reduced to an enforcement tool for data protection regulation (Kerber, 2026). Against this background, this paper contributes an economic perspective to the debate.

Its central argument proceeds in two steps. First, it examines data combination rents – the incremental strategic and monetary value generated by merging separate user data streams from distinct platform services. We argue that these rents, rather than raw data volume, constitute the primary source of gatekeeper dominance. Data combination rents are economically ambivalent: they drive product innovation, sustain the zero-price business models from which consumers[4]

[1] There is a dissenting legal view by Hoeren & Fuchs (2025) that Article 5(2) DMA indicates by "specific choice" not an independent criterion but is rather identical to "specific" as given in Art. 4(11) GDPR.
[2] Whereas the European Commission fined Meta for non-compliance at first, commitments towards a DMA-compliant Pay-or-Consent model have been announced (European Commission, 2025).
[3] See, for example, Andriychuk et al. (2025) commenting on the Joint Guidelines concerning Article 5(2) DMA.
[4] We use 'end user' when referring to the regulatory subject defined by Article 2(20) DMA, which encompasses any natural or legal person using core platform services other than as a 'business user', and 'consumer' when discussing welfare-economic effects on natural persons. The two categories largely overlap but are not identical.

derive substantial welfare gains, and fuel research and development (R&D) in areas such as artificial intelligence (AI). But they simultaneously erect market barriers to entry, deepen ecosystem dependency, and enable the extraction of consumer surplus in ways that competition policy has legitimate reason to address.

Second, we demonstrate that the regulatory instrument chosen to meet this challenge – the GDPR's concept of consent, as transplanted into Article 5(2) DMA – is structurally incapable of properly addressing the competitive effects of data combination rents. Rather, the consent regime produces collateral economic inefficiencies that arise already under the GDPR and are compounded by the DMA transplant: it disadvantages smaller competitors, fragments data into silos, shifts regulatory burden onto cognitively overloaded end users, and reduces consumer welfare by curtailing the ability to pay with data. On this last point, we advance an argument that has not been adequately recognized in the existing literature: data-based payment constitutes an economically distinctive mode of exchange that, unlike monetary payment, does not directly deplete disposable income. While not entirely costless, restricting it forces a shift towards monetary exchange that makes consumers poorer in terms of immediate purchasing power – a welfare cost that any privacy regulation must overcompensate for if it is to produce a net gain.

Two research questions guide this paper. (1) What economic mechanism generates the data combination rent, and why does it make this rent simultaneously the core driver of gatekeeper revenue and the primary source of strategic market dominance? (2) Does the legal-economic design of Article 5(2) DMA create a regulatory impasse by anchoring a competition rule in the GDPR's concept of freely given consent?

The paper proceeds as follows. Section 2 develops the economic framework of data combination and examines the welfare distortions that consent introduces. Section 3 traces the legal roots of Article 5(2) DMA and maps its adverse market outcomes, resulting in what we describe as a regulatory impasse. Section 4 surveys potential design and policy alternatives. Section 5 concludes.

## 2 Economics of data value creation and the role of consent

The regulatory design of Article 5(2) DMA cannot be assessed in isolation from the economic phenomenon it seeks to govern. Thus, this section establishes that the marginal returns to raw data accumulation diminish at scale, that the decisive competitive lever lies in the combination of heterogeneous data streams, that the value of this combination is structurally opaque, and

that consent is prone to produce systematic welfare distortions. The question is whether a concept rooted in individual autonomy is an effective instrument for governing competitive concerns, or whether governing competition concerns requires tools calibrated specifically to the economic structure of data-driven markets.

### 2.1 Data accumulation and its diminishing returns

The competitive significance of data in digital markets has been extensively debated. Effective data deployment lowers search frictions and refines matching between supply and demand, for instance, through better-calibrated products or more precisely targeted advertising (de Cornière & Taylor, 2025). However, these efficiency gains come with competitive costs: the accumulation of large datasets can facilitate price discrimination, enable excessive surplus extraction, and erect barriers to entry (Crémer et al., 2019; Furman et al., 2019; Scott Morton et al., 2019).

One strand of literature foregrounds scale advantages: data may generate increasing returns, with exclusive control over large datasets erecting significant obstacles for prospective entrants (Rubinfeld & Gal, 2017; Tirole, 2023). Moreover, data may exhibit the characteristic of an essential facility (Abrahamson, 2014), and what Gregory et al. (2021) describe as data-enabled feedback effects can amplify this advantage, as an expanding user base generates more granular data.

An equally substantial body of work challenges this view. Data resources are often neither unique nor inimitable: they can be replicated or assembled from alternative sources (Lambrecht & Tucker, 2015), and digitalization has eroded the scarcity properties necessary for data to function as a bottleneck (Tucker, 2019). Data in isolation lack economic value – their significance materializes only in combination with the organizational capacity to process them (Basaure et al., 2025), the same capability condition that moderates the feedback loop above (Hagiu & Wright, 2023). The non-rivalrous character of data reinforces this point (Rubinfeld & Gal, 2017), and pronounced information asymmetries characterize personal data as a good: the collecting platform knows far more about quality and completeness than any prospective acquirer (Schweitzer et al., 2022), while value is contingent on format, timing[5], and analytical sophistication (Gal & Rubinfeld, 2019). Diminishing returns become empirically relevant at exceedingly high data volumes (De Fortuny et al., 2013; van de Waerdt, 2023a). Corrado et al.

[5] While the value of information increases with quantity, its quality can decrease over time (Moody & Walsh, 1999).

(2022) clarify the pathway from data to value through a three-layer taxonomy: first, data stores for raw and unstructured information, second, databases for structured data sets ready for analysis, and third, data intelligence for actionable commercial insights. What matters for monetization is not the breadth of the first layer but the sophistication of the third. Thus, the literature converges on a central point: while data accumulation generates competitive advantages, these are subject to diminishing marginal returns to scale.

### 2.2 Data combination rent: from volume to variety

If the returns to raw data accumulation diminish at scale, the enduring source of competitive advantage for large digital platforms lies elsewhere: in the combination of qualitatively different data across services. This lateral approach gives rise to the data combination rent. Unlike volume-based advantages, data combination exhibits increasing returns to scope: each additional data source yields qualitatively new insights that no single-source dataset can produce.

The concept builds on the growing literature on digital conglomerates (Bourreau & de Streel, 2019; Condorelli & Padilla, 2020; Crémer et al., 2019). Van de Waerdt (2023b) argues that what distinguishes the largest platforms is the centrality of personal data to their entire operational architecture. These ecosystems channel user activity across multiple services, generating data-based feedback effects at the conglomerate level. Through targeted advertising, the integration of these data streams enables profit-maximizing strategies unattainable from any single service. Competition in such a setting is not for individual markets, but for ecosystem rents. Where the data-enabled feedback loops run unchecked, this contest promotes ecosystem dominance. Van de Waerdt (2023b) reads this as a distinct theory of competitive harm rooted in increasing dependency rather than traditional foreclosure dynamics.

Prüfer & Schottmüller (2021) formalize the mechanism through which data combination advantages propagate across markets. In their model, data-driven indirect network effects occur where accumulated user data continuously lowers a firm's marginal cost of innovation, driving markets towards tipping. A dominant firm can leverage its aggregated data advantage from a primary market to outcompete rivals in adjacent markets, initiating a competitive cascade effect. This dynamic illustrates why the combination rent is self-reinforcing: once a platform has assembled a sufficiently broad data ecosystem, each additional service both exploits existing data synergies and generates new data that strengthens the firm's position. These advantages are not traditional network effects but data-enabled learning (Hagiu & Wright, 2023): a

demand-side size advantage that materializes through the firm's production side as higher product quality or a lower marginal cost of innovation (Prüfer & Schottmüller, 2021).[6] Among the several size advantages of digital ecosystems, the data-combination channel is the one Article 5(2) DMA singles out for governance, and the one whose value is least legible to the parties whose choice is supposed to govern it.

The strategic importance of data combination is further reinforced by work on data complementarity. Whereas scale-based models demonstrate that competitive advantage depends on the volume of user data driving learning curves (Hagiu & Wright, 2023), the combination rent operates on a different margin: data is more valuable when complementary to other data types and reusable across diverse contexts (Iansiti, 2021). Schweitzer & Metzger (2023) specifically identify the cross-service combination of personal data as the foundation for individualized product development and personalized advertising – the primary growth drivers for large platforms.

The data combination rent also interacts with the distinction between Schumpeterian rents, generated through R&D investment, and Ricardian rents, accruing to holders of scarce resources (Petit & Teece, 2021; Simone & Laudando, 2025). Applying this distinction to data combination leads to a governance trade-off: platforms invest heavily in data infrastructure and analytics (a Schumpeterian activity), yet the returns on this investment partly reflect the scarcity value of an ecosystem position that rivals cannot replicate at comparable cost (a Ricardian component). Competition policy traditionally preserves Schumpeterian rents while constraining Ricardian ones. Because both components accrue to the same asset, an instrument that restricts data combination as default cannot constrain the Ricardian component without suppressing the Schumpeterian one.

The data combination rent is thus economically ambivalent – a source of value creation for consumers through cross-service functionality, personalization quality, fraud detection, and the zero price access it funds (de Cornière & Taylor, 2025), and a constraint for a competitive

[6] Network effects in the strict sense denote preference interdependence. An individual user's utility increases directly with the number of other users (Katz & Shapiro, 1994). According to Hagiu & Wright (2023), data-enabled learning instead operates through the production side. Firms improve their products by learning from customer data, which raises willingness-to-pay rather than lowering production costs – the stated contrast to traditional learning-by-doing. They distinguish the mechanism from standard network effects endogenously only under specific conditions, namely across-user learning combined with consumers' forward-looking expectations. What Prüfer & Schottmüller (2021) label data-driven indirect network effects are best understood in this sense. Nor is data the only source of size advantages at the ecosystem level. For example, one-stop-shopping preferences and shared infrastructure generate scope advantages of their own (Bourreau & de Streel, 2019).

landscape. The privacy cost is not simply additive: combining datasets from different services enables inferences, such as predicting protected attributes pursuant to Article 9 GDPR (health status, political or sexual orientation) from ostensibly innocuous behavioral data (Mühlhoff, 2023; Tian et al., 2026; Yeom et al., 2018), which no single-service dataset in isolation would support. The inference space, and with it the privacy exposure, grows with the diversity of the combined data. De Cornière & Taylor (2025) provide a theoretical framework identifying a fundamental trade-off between a universally pro-competitive mark-up effect, where better data increases profitability per consumer and induces firms to compete harder, and a highly ambiguous surplus extraction effect.[7] They demonstrate that data is pro-competitive when used to improve products, anti-competitive when used for price discrimination, and ambiguous for advertising.[8] Applying this framework to data combination, where combined data improves quality or enables welfare-enhancing innovation, the mark-up effect dominates, and the rent is pro-competitive. Where combined data serves granular price discrimination or manipulative targeting – advertising that exploits individual behavioral biases to induce purchases the consumer would reject under full information (Fourberg et al., 2021) – the surplus extraction effect dominates, and the rent is anti-competitive (Gradwohl & Tennenholtz, 2022; Jones & Tonetti, 2020; Jorzik et al., 2024). Article 5(2) DMA, however, does not distinguish between these uses. It restricts data combination as the default if not exempted by the end users' consent.

Despite this economic ambivalence of the data combination rent, the DMA adopts a rigid stance seeking to open gatekeepers' data silos in the interest of contestability rather than to break ecosystems up (Bostoen, 2023).[9] By restricting data combination, the regulation targets one channel of market concentration – the combination advantage. Although, its effect on concentration is uncertain to the extent that the underlying data remains reproducible (see Section 2.1). At the same time, it sets boundaries for value creation and innovation through the limited cross-service scope economies, reduced ad-funded coverage, and, to an uncertain extent, constraints on AI training data (Cennamo et al., 2025) (see Section 5). This raises the

[7] Although de Cornière & Taylor (2025) do not explicitly use the term data combination, their theoretical framework functionally treats any pooling, acquisition, or integration of data as an increase in the firm's overall data quality parameter, making their analysis directly applicable.
[8] This might be, for example, the case in the medical sector (Hulsen, 2020).
[9] It is worth noting that while the DMA restricts data combination primarily to ensure inter-platform contestability, the initial German Federal Cartel Office's case against Meta was before the adoption of the DMA and found data combination practices towards end users as an abuse of dominance infringement under § 19(1) GWB.

design question at the center of this paper: not whether the data combination rent warrants governance, but whether consent is the right instrument.

### 2.3 Opaque value of data: the privacy and pricing failures

Any regulatory instrument that conditions data combination on an individual transactional choice – consenting or rejecting – presupposes that the parties can meaningfully evaluate what is being exchanged. This presupposition neglects that the value of the data combination is structurally opaque.

Data combines partial excludability with non-rivalry: access can be restricted by the holder, yet use by one party does not diminish availability to another (Purtova & van Maanen, 2024). What distinguishes data is not this structure, but the combination advantage, the superadditivity of its value under combination, and the inferences it enables about parties not involved in the exchange. Large platforms capitalize on excludability by enclosing data within proprietary ecosystems. This exclusion operates on the dataset and its linkage, not on the underlying behavioral information. Rivals with their own user relationships can collect substantially the same raw data in parallel (see Section 2.1). What cannot be replicated is the cross-service linkage at gatekeeper scale, precisely the objective of Article 5(2) DMA. The absence of rivalry, meanwhile, means that multiple firms could draw value from identical datasets simultaneously. Yet holders of large datasets have little commercial reason to share, even where broader sharing would improve economy-wide outcomes (Jones & Tonetti, 2020). This generates a structural inefficiency.

Article 5(2) DMA conditions data combination on end users' consent, tacitly presupposing that the consenting party can meaningfully evaluate what is at stake and assess its price. However, for an incremental data point, the marginal value is negligible on both sides of the exchange. The gatekeeper's models improve imperceptibly, and the users give up nothing they cannot supply again elsewhere, since data is reproducible. If consent governed marginal data points, it would price a good whose value approaches zero at the margin. Yet Article 5(2) DMA governs something else: the durable cross-service linkage of a user's entire profile. At this level, a well-defined per-user magnitude exists. In the ad-funded context, it is the revenue differential between personalized and non-personalized advertising – the implicit data price of the ad-funded option (Kerber, 2026). In this context, the informational positions are sharply asymmetric. The gatekeeper observes this differential through its own advertising infrastructure. The end user observes neither the differential nor the inferential uses to which a

linked profile may subsequently be put (Acquisti et al., 2016). Advertising is merely the most measurable manifestation. The same cross-service linkage drives personalization across the platform's services more broadly. Moreover, the user's exposure is a stock rather than a flow. While data remains re-usable, inferences drawn from a combined profile persist and compound. The pricing failure is therefore not that end users undervalue a known quantity, but that no individual-level price exists that both parties could observe, as the rent is emergent at the level of combination, and the privacy cost is emergent at the level of inference (see Section 2.2). Structural features compound the problem: the marginal cost of digital services approaches zero, making cost-based pricing uninformative. The multi-sided platform architecture means that user-side prices are subsidized by advertising revenues, and the absence of competitive benchmark markets deprives regulators of reference points for 'fair pricing'(Mancini & Volpin, 2018).[10] The behavioral dimension of consenting is equally severe: the effort required to evaluate a consent decision far exceeds any informational benefit end users could plausibly extract. Acquisti et al. (2017) identify several structural reasons why privacy decisions are particularly susceptible to default effects, including information difficulty, preference uncertainty, and the reading of defaults as implicit recommendations.[11] What is formally an end user decision practically reveals as substantially shaped by interface design.

A distinct dimension of this pricing failure concerns the economic nature of data-based payment. When gatekeepers implement a pay-or-consent model, the normative assessment implicitly treats monetary payment and data provision as substitutable.[12] However, they differ fundamentally. A monetary payment directly reduces disposable income: every euro spent on a subscription is unavailable for other consumption. Data provision, by contrast, does not draw on the consumer's monetary budget: the same data can be provided repeatedly without direct depletion. Paying with data, therefore, preserves the full range of consumption possibilities that income affords.[13]

---

[10] For a practical discussion of what constitutes an appropriate fee in pay-or-consent models see, for example, Information Commissioner's Office (ICO) (2025).

[11] Empirical work on post-GDPR consent interfaces substantiates the mechanism: Nouwens et al. (2020) show that removing a reject all button raises acceptance rates by up to 23 percentage points, while only around 12 percent of live interfaces meet minimal GDPR requirements.

[12] This normative understanding can also be found in the ruling of the Court of the European Union (CJEU) in *Meta Platforms Inc. and Others v. Bundeskartellamt*. See in more detail Section 3.1.

[13] This does not deny that individuals with high privacy valuations willingly pay for privacy-preserving services. The argument concerns the removal of the data-payment option, which forces monetary payment upon the group with low willingness to pay for privacy. That privacy-focused providers compete successfully in competitive segments supports the screening logic discussed below and confines the problem to gatekeeper settings.

Of course, data provision is not costless. Its primary non-monetary cost is privacy loss (Acquisti et al., 2016). Beyond this, combined user profiles allow platforms to extract consumer surplus more efficiently, through granular price discrimination and through personalized advertising designed to stimulate purchases consumers would otherwise not make (de Cornière & Taylor, 2025). There may also be indirect monetary costs. The British Competition and Markets Authority (CMA), for instance, asserts that digital advertising costs are reflected in the prices of goods and services across the economy (CMA, 2020). Whether such pass-through occurs is contested: in models of informative advertising, product prices are independent of advertising costs (Varian, 2022), and the available economy-wide evidence suggests that the direction of advertising's price effect tracks its information content, meaning that informative advertising lowers consumer prices, persuasive advertising raises them (Rauch, 2013). However, even where the indirect costs arise, they are categorically different from the direct and immediate income depletion of a subscription fee. The indirect costs are lagged, dispersed, and largely invisible during the act of consent. Any regulation that restricts data-based payment forces a shift toward monetary payment, thereby reducing real income. If such regulation is to produce net welfare gain, the privacy benefits must overcompensate for this income loss – a condition that existing frameworks have not attempted to quantify.

This opacity – the absence of an observable individual-level price established above – is compounded by the framing of platform access as free, which obscures the economic reality that users provide personal information as compensation. As Newman (2015, 2016) establishes, zero-price transactions are genuine economic exchanges within the scope of antitrust scrutiny. The boundary between data provided as payment and data provided for functional benefit is itself blurred (Botta & Wiedemann, 2019), leaving the commercial value of personal data structurally unquantified.

One might object that pay-or-consent functions as a screening mechanism: by offering a binary choice, the gatekeeper elicits private information about users' heterogeneous privacy valuations, inducing self-selection (Acquisti et al., 2013; Acquisti & Grossklags, 2005; Posner, 1978; Stigler, 1980). However, this presupposes conditions that do not hold in gatekeeper markets: First, the price of the privacy-preserving option is set unilaterally, not disciplined by competition. Second, the choice architecture is distorted by loss aversion: consumers habituated to zero-price platform access perceive even a modest fee as a loss overshadowing potential gains (Cziehso et al., 2019; Heidhues & Köszegi, 2004). Third, the two options are not

commensurable because the costs of data provision are structurally opaque, while the monetary cost is immediate and salient.

Against this background, the analysis revealed two distinct failures: The first is a privacy failure. Considering the power asymmetry between gatekeepers and end users and their behavioral constraints, consent does not reliably protect informational self-determination. This failure is inherent to the concept of consent, although 'freely given' as a condition for 'valid' consent attempts to compensate for this. The second is a pricing failure. Where personal data serves as counter-performance, no price mechanism exists that could perform the valuation and coordination functions that money prices perform. This is a failure of the market for personal data itself, located in contract law's treatment of data as consideration,[14] rather than in data protection. Because the data price is unobservable to the paying side, paying with data is not comparable to paying with money, and consent cannot repair the defect (Schweitzer, 2017; Kerber & Hornung, 2026).[15] [16] Considering that Article 5(2) DMA relies on GDPR's consent, it inherits both failures because it treats data and monetary payment as substitutable counter-performances. Therefore, we do not neglect the consent's objective of data sovereignty. Rather, we reflect on whether consent as a concept is the right mechanism to address both failures.

### 2.4 Consent as an economic instrument: distortions and welfare effects

Keeping in mind the privacy and pricing failures, we now shift the perspective on the economic effects of the concept of consent. According to economic theory, consent introduces systematic distortions for the market, grouped into three categories: failures rooted in the behavioral limits, distortions of market competition, and structural losses to the data ecosystem.

---

[14] See Article 3(1) of the Digital Content Directive (Directive (EU) 2019/770).

[15] Our reliance on Schweitzer's diagnosis might appear to be inconsistent with the income argument developed above: Schweitzer regarded paying with data as dysfunctional, whereas we treat the availability of data-based payment as welfare-relevant. The two claims concern different properties of the exchange. Schweitzer's critique targets its coordination function. Because the data price is unobservable, it cannot measure value or discipline the terms of the exchange the way a monetary price does (Kerber & Hornung, 2026). The income argument targets its budget effect. Whatever its informational defects, data-based payment does not deplete disposable income, thus, suppressing it is not costless for consumers. The claims are compatible and jointly ground our conclusion: the first explains why individual consent cannot govern the exchange, the second why prohibiting the exchange imposes welfare costs of its own. This is why Section 4 examines mechanisms that operate on the terms of the exchange rather than on its existence.

[16] This pricing failure concerns the coordination function of a price. It should be kept distinct from the separate welfare cost of prohibiting data-based payment, meaning its effect on disposable income, which we develop below.

*2.4.1 Behavioral failures: the limits of voluntary and informed choice*

First, consent operates under conditions that limit its voluntariness. Although Article 5(2) DMA acknowledges the imbalance of power between the gatekeeper and end user, it uses users' consent for the situation of power asymmetries that make 'freely given' consent structurally difficult to obtain, illustrated by pay-or-consent models.

When gatekeepers operationalize the consent requirement through pay-or-consent models, the economic and the legal standards for 'freely given' are in tension: what is economically an unremarkable consumption decision – declining a fee that exceeds one's willingness to pay – may still fail the stricter legal standard of Article 4(11) and Recital 42 GDPR, under which consent is not freely given where refusal carries detriment and no genuinely equivalent alternative exists. Further, the European Data Protection Board (EDPB) concludes that consent extracted against a paid-only alternative will usually fail this standard (EDPB, 2024).[17] Three features of gatekeeper markets drive the wedge between the two standards. First, the price of the privacy-preserving option is set unilaterally by the party whose business model depends on its rejection and is not disciplined by competition. Second, the resulting consent shares are uninformative as preference revelation. Acceptance rates close to 99 % are observed for pay-or-consent walls (Müller-Tribbensee et al., 2024). Under Meta's model, fewer than 1 % of end users chose the paid option (European Commission, 2025; Kerber, 2026). What market power removes is thus not the nominal choice, i.e., the formal accept-or-pay-option, which remains, but the outside option: a genuine competitive alternative to which the user could otherwise turn. In competitive segments, users with high privacy valuations can migrate to providers with better privacy terms. Vis-à-vis a gatekeeper, exit is unavailable, and the fee is the only alternative. Third, the consequence is distributional. Where effective data protection is available only against payment, privacy becomes a good priced by the gatekeeper, accessible according to ability to pay rather than preference.

Second, the behavioral preconditions for informed consent are unmet. End users face information overload, systematically discount long-term consequences, and are exposed to interface designs building on complexification and asymmetric friction, thereby exploiting cognitive biases (Acquisti et al., 2017; Nouwens et al., 2020). In the specific context of Article 5(2) DMA, Zolna (2025) concludes that end users are overwhelmed and refrain from making

[17] See also Morel et al. (2025) on cookie paywalls.

fully informed choices. The difficulty is not the monetary side of the choice, whose cost is immediate and salient, but the counter-performance side: what a linked profile will reveal and enable over time is precisely what end users cannot assess (see Section 2.3). The GDPR's insistence on informed and specific consent is in fundamental tension with the operational logic of data-driven platforms, whose business models depend on the continuous, retrospective discovery of analytical patterns that cannot be specified in advance (van de Waerdt, 2020). Consent thus transfers regulatory responsibility to the party least equipped to exercise it while leaving structural market power intact.[18]

*2.4.2 Market and competitive distortions*

First, consent creates competitive distortions that favor the very incumbents the DMA targets. Privacy regulation shrinks the volume of consumer data available to firms, and this contraction disproportionately burdens smaller and more data-dependent enterprises (Johnson, 2022; Johnson et al., 2023; Peukert et al., 2022). Individuals are far more inclined to authorize data processing by a brand they already use than by an unfamiliar third party (Martin & von Grafenstein, 2026).[19] Newer firms, which have not yet built the consumer relationships that predispose users to grant permission, are structurally disadvantaged, despite being the very firms whose strategies most depend on secondary and third-party data. Goldberg et al. (2024) find that smaller sites exhibit substantially higher non-consent rates, consistent with the argument that consent regimes structurally favor incumbents (Campbell et al., 2015). Geradin et al. (2021) document this dynamic in digital advertising, finding that the GDPR has strengthened the largest platforms because consent-based data collection systematically advantages firms operating a broad portfolio of consumer-facing services.[20]

A potential objection is that Article 5(2) DMA binds only designated gatekeepers and could thus benefit competitors. However, the distortions arise primarily from the underlying GDPR consent regime, which applies to all data controllers. Article 5(2) DMA compounds this effect,

---

[18] The structural difficulty of satisfying the informed and specific criterion is not merely informational. Rockenbach et al. (2021) show experimentally that even in an idealized public-good setting, users do not reduce their provision of personal information in response to asymmetric rent capture by a non-contributing larger player – in contrast to monetary contributions. The behavioral form of data-based exchanges thus neutralizes the market-disciplining function that the consent mechanism is asked to perform.

[19] Consent rates for well-known brands reach about 72 %, while consent sharing collapses to around 3.5 % (Martin & von Grafenstein, 2026).

[20] Geradin et al. (2021) illustrate this with two episodes involving Google: first, Google withdrew advertising YouTube advertising from its open ad exchange (AdX), cutting rivals off from valuable demand. Second, Google restricted data portability from DoubleClick, its ad-serving measurement product. In both cases, GDPR compliance was invoked as a justification for conduct that foreclosed competing ad-tech intermediaries.

but because gatekeepers are best equipped to obtain consent (Martin & von Grafenstein, 2026), the additional restriction is least likely to bind where the competitive asymmetry is greatest. Gal & Aviv (2020) identify seven cumulative market dynamics through which the GDPR creates more concentrated structures, highlighting that obtaining informed consent for data sharing with third parties is sometimes entirely infeasible. Prüfer & Schottmüller (2021) provide a consistent theoretical framework: the marginal cost of innovation decreases in a firm's accumulated data stock, so a dominant firm's historical advantage translates into a persistent cost advantage in innovation that no prospective withdrawal of consent can undo – the algorithmic insight already derived from historical data persists regardless of whether future data flows are curtailed.[21] Aridor et al. (2020) document that post-GDPR the population of trackable consumers shrinks while the remaining consumers become more valuable – both reinforcing incumbent data advantages.

Second, consent-based siloing impairs data-driven efficiencies without effectively reducing incumbent market power. Examining the DMA draft,[22] Krämer & Schnurr (2022) show that restricting the data combination across a gatekeeper's services sacrifices the economies of scope that make aggregate data holding analytically valuable, yet gatekeepers can obtain opt-in consent for data combination more easily than niche entrants, so siloing default has only a marginal impact on dominance. The result is an asymmetric burden: efficiency losses that bind consumers and entrants while leaving incumbent advantages structurally intact. By restricting data sharing, the consent regime prevents the realization of data synergies – the source of the combination rent's productive potential (Gal & Aviv, 2020). Zolna (2025) argues that Meta's loss of cross-service economies of scope reduces its ability to invest in novel products requiring integrated datasets (the AI dimension is developed in Section 3.2).

*2.4.3 Structural ecosystem losses and welfare effects*

First, formal welfare models confirm that consent targets the wrong margin. Natvik & Tangerås (2023) model a setting where platform access is compensated through personal data. A striking result is that in ad-funded equilibria, aggregate data transfer is welfare-optimal: consumers calibrate engagement to the point where additional use no longer justifies the corresponding privacy loss. The source of inefficiency lies instead in the platforms' non-price decisions,

[21] The application to consent is an inference of this paper from their model, not the claim of Prüfer & Schottmüller (2021).
[22] For the DMA draft version see COM(2020) 842 final.

yielding distortions whose sign depends on the relative weight of nuisance and advertising costs. A consent mandate would curtail a dimension of exchange that is already efficient while leaving this distortion untouched. Ke & Sudhir (2023) show that in a monopoly setting, rights to erasure and portability reduce the firm's incentive to offer low introductory prices, and consumer welfare declines whenever the risk of privacy breaches is sufficiently low – precisely the configuration for established gatekeeper platforms. Xu et al. (2025) show that data-collection restrictions can prompt retailers and suppliers to raise prices strategically, and that for products with sufficiently high consumer valuation, this indirect pricing effect can dominate the direct privacy gain.

Second, consent is structurally unable to address the data externalities that pervade digital markets. Acemoglu et al. (2022) formalize the mechanism: because consumers' data is statistically correlated, any individual's decision to share reveals information about others whose privacy preferences may differ. This negative externality depresses the equilibrium price of data and generates excessive data sharing – the opposite of the concern motivating consent-based regulation. Platform competition does not correct this inefficiency, but the resulting fragmentation of user distribution exacerbates it. A consent mechanism cannot internalize these externalities: each individual's choice is evaluated against a baseline already determined by others' choices. A parallel externality operates on the competition side: an individual consent decision also disregards its external effect on contestability, which accrues to competitors and future consumers rather than to the consenting end user (Kerber, 2026).

Overall, the concept of consent produces welfare losses along multiple dimensions. It entrenches incumbents, fragments data ecosystems, shifts an unperformable regulatory burden onto users, and reduces real consumer income. Agent-based simulations reinforce this conclusion: restricting data combination does not improve market contestability, even when targeted exclusively at very large platforms (Basaure et al., 2025). These findings do not deny the necessity for regulatory attention. They imply that the specific mechanism chosen is structurally mismatched to the competitive dynamics of data-driven markets.

## 3 Article 5(2) Digital Markets Act: regulatory impasse and its market consequences

Having established the economic limitations of consent in data-driven markets, we now trace the legal pathway through which this concept was incorporated into Article 5(2) DMA. We argue that this embedding produces a two-fold regulatory impasse and risks generating adverse market outcomes.

### 3.1 The legal pathway of consent and its structural mismatch

The legal roots of Article 5(2) DMA lie in the German Facebook case (now and in the following Meta)[23] from 2019, which exposed the fundamental tension regarding platforms' enhanced access to combined data as abusive leverage under ex-post competition law (Bundeskartellamt, 2019). The proceedings directed the legal debate towards the realization that privacy protection and competition law constitute overlapping areas that require reconciliation (Kerber & Zolna, 2022; Witt, 2024). Article 5(2) of the DMA embodies the first regulatory attempt within the European Union's digital rules for online platforms to reconcile these two objectives.

When we look back at the legal reasoning in the German Meta case (Meta Platforms Inc. and Others v. Bundeskartellamt),[24] it becomes evident why this approach has attracted sustained criticism (see, for example, Paul, 2025; Podszun, 2022; Ribera Martínez, 2022, 2026; Zolna, 2025). The German Federal Cartel Office (Bundeskartellamt, BKartA) found that Meta had abused its dominant position by combining and cross-using end users' data from different core platform services without obtaining valid consent as required by the GDPR. This data practice enabled Meta to extract data combination rents: through dataset combination, detailed user profiles were generated and monetized via personalized advertising. The legal reasoning was anchored in Meta's dominance and its bundling of consent, which violates the GDPR requirements for freely given consent. Interestingly, in the following court proceedings against the decision, the Court of Justice of the European Union (CJEU) held it generally possible for a dominant undertaking to offer an equivalent alternative against an appropriate fee *(Meta Platforms Inc. and Others v. Bundeskartellamt, 2023, para. 50)*. This is an admission that doctrinally entrenches the substitutability of data and monetary payment. This substitutability was identified as economically unfounded (see Section 2.3). Fundamentally, the conclusion of substitutability serves as the basis for the pay-or-consent architecture. Article 5(2) thus attempts to reconcile the conflicting interests revealed in the Meta case: data combination rents constitute a core revenue source, funding R&D and ecosystem growth, yet, cross-use of data primarily benefits undertakings that combine extended data access with the analytical capacity to exploit it, further entrenching their market position. Simultaneously, end users' control over personal data is undermined by (bundled) consent designs that breach GDPR's standards. Article 5(2) DMA aims to lower market barriers by stipulating a general prohibition of cross-use and data

[23] See Podszun (2020) for an illustrative summary of the Meta case in Germany.
[24] See Mendelsohn & Färber (2024) for a more in-depth analysis of the court rulings.

combination across core platform services, subject to the exemption that the end user has given consent according to the GDPR. In practical terms, Meta's Pay-or-Consent model was and presumably is still[25] the first use case for assessing compliance with Article 5(2) DMA.

Considering that consent suffers several systemic distortions (see Section 2), the design of Article 5(2) DMA risks undermining its own objectives, thereby creating the regulatory impasse.[26] The *Meta Platforms Inc. and Others v. Bundeskartellamt (2023, para. 50)* proceeding confirmed that when the concerned undertaking holds a dominant position, this constitutes a significant factor for assessing the imbalance of power and is highly likely to cause invalid consent. Beyond this, the lack of a quantifiable value for data recalls the pricing failure: Article 5(2) DMA allows subscription-based models but specifies no benchmark for the fee, and simultaneously treats data and monetary payments as substitutes.

### 3.2 Potential harms for the market as consequences of the regulatory impasse

The market outcomes produced by Article 5(2) DMA replicate the systemic distortions identified in Section 2, undermining both the DMA's contestability objective and the GDPR's data sovereignty objective.

Regarding market and ecosystem distortions, Article 5(2) DMA may shrink the aggregate value of datasets, impairing capacity for R&D and AI purposes (Gal & Aviv, 2020; Zolna, 2025) and degrading service quality, for instance, through reduced ad targeting precision (Lamb, 2025). Such a degradation could only be justified if smaller firms benefited. Yet, as Section 2.4.2 established, they typically lack the scale and the processing capacity to do so (Prüfer & Schottmüller, 2021).

The effects on consumer welfare are equally consequential. As established in Section 2.3, restricting data-based payment forces a shift toward monetary payment and thereby reduces disposable income. For a net welfare gain, privacy benefits must compensate for this loss – a comparison that is methodologically contested since it requires commensuration of a

[25] Currently, the European Commission is monitoring compliance, a process that has attracted sustained criticism over the model's potential deficiencies (Baker, 2026; Datta, 2026; The European Consumer Organisation (BEUC), 2025).

[26] From a regulatory-theory perspective, Blockx (2025) traces the poor compliance with European digital laws to their design as 'meta-regulation', which delegates the implementation of regulatory objectives to the regulated firms themselves. Such delegation succeeds only where the incentives of the regulated align with the regulatory goal and where non-compliance carries a credible threat of sanctions – conditions the author finds absent in the digital sector, since personal data constitute these firms' core input and public enforcement remains weak. Granted discretion over how to comply, a gatekeeper will therefore tend to design its compliance so as to preserve, rather than relinquish, the data combination rent. Meta's Pay-or-Consent model can be read as an instance of this dynamic.

fundamental right with a monetary magnitude. Additionally, restricting data access may lead to higher consumer prices more broadly, as gatekeepers relying on data combination rents from online advertising may be forced toward fee-based models.

The provision's effectiveness is thus caught by a two-fold regulatory impasse (Bamberger & Corren, 2026; Botta & da Costa Leite Borges, 2023): neither the DMA's contestability objective nor the GDPR's data sovereignty objective can be achieved.[27] Widespread consent perpetuates existing data asymmetries – as the sub-1 % paid-option take-up under Meta's model illustrates (see Section 2.4.1) – while widespread refusal would fragment data ecosystems without delivering contestability. At the same time, end users' limited awareness of data value hinders the increase in individual data sovereignty.

The scope of the problem extends beyond the enforcement context. Combined cross-service data constitutes a critical input for generative AI, whose foundational models rely on vast and heterogeneous training. To the extent that Article 5(2) DMA restricts data combination, it affects not only targeted advertising but also the data infrastructure underlying AI development. Retroactive data siloing has limited efficacy once a model has already been trained on combined datasets, and gatekeepers may circumvent the restriction by claiming sufficient de-identification (Kirkwood, 2025). The consent instrument is therefore confronted with a challenge reaching beyond advertising-funded services: it must govern data flows shaping AI markets, a domain in which the individual transactional logic of consent is even less suited to the collective nature of the underlying data processes.[28]

## 4 Towards best practice: improvements and alternative frameworks

One might defend Article 5(2) DMA on fundamental-rights grounds – the right to informational self-determination underlying the GDPR: cross-service profiling can reveal sensitive attributes (see Sections 2.2 and 3.2), and a consent mechanism at least gives users the option of preventing such inferences. This objective is legitimate, but, as shown above, the consent mechanism produces a two-fold regulatory impasse. Hence, this section surveys alternative regulatory approaches that target the data combination rent more directly.

---

[27] Bamberger & Corren (2026) frame the same tension more pointedly around privacy as a value threatened by the surveillance capacity of platforms, whereas the present analysis approaches it from the perspective of the data combination rent and its competitive effects. We read the underlying diagnosis as substantively congruent.

[28] See also footnote 23. By delegating the design of compliance to the very gatekeeper whose business model depends on data combination, the provision entrusts its own enforcement to an actor structurally disinclined to deliver it (Blockx, 2025).

The proposals surveyed fall into two categories.[29] The first encompasses reforms within the consent framework that seek to mitigate its mismatch through improved design, stricter standards, or supplementary tools. The second comprises institutional alternatives that move beyond individual consent entirely.

### 4.1 Reforms within the consent framework

Several authors propose modifications that retain the GDPR's autonomy-based logic but adapt it to the specific power asymmetries at stake (see Sections 2 and 3). Paul (2025) argues that the DMA should adopt a consent standard specifically tailored to gatekeeper-end user relationships, under which platforms would default to the minimal data-processing configuration strictly necessary for service provision, with end users actively opting into additional processing through a structured interface.[30]

Zolna (2025) discusses recent regulatory and institutional demands aimed at practically addressing this dynamic. Following the approach of the German Federal Cartel Office and the European Commission, he emphasizes the need for gatekeepers to more effectively unbundle consent requests, allowing end users to authorize specific types of data processing independently, rather than facing a binary choice between full data combination and a monetary alternative. For data uses not directly linked to advertising, such as cross-platform functionality or AI research, Zolna echoes the position of the EDPB, which advocates for a third option: a service variant funded exclusively by contextual advertising without cross-service data combination (EDPB, 2024).

Botta & da Costa Leite Borges (2023) propose a one-time, granular privacy-setting mechanism presented upon first interaction, allowing end users to specify permitted categories of data combination without repeated consent requests, though settings would remain adjustable. Podszun (2022) suggests independent rating entities, termed as data guides, that evaluate and certify gatekeepers' data-processing options, translating choices into simplified assessments,

---

[29] Beyond design and institutional reforms, fiscal instruments, such as taxes on advertising revenues derived from combined data or regulatory levies proportional to gatekeepers' market share, could complement the alternatives discussed here. Such instruments, however, inherit the two problems identified earlier (see in Section 2.3): While advertising revenues are observable, calibrating a levy to the data combination rent itself would require isolating the rent component. A simple revenue tax avoids this only by being untargeted, burdening welfare-enhancing and anti-competitive uses of combined data alike, thereby replicating the use-blindness for which this paper criticizes Article 5(2) DMA. They additionally raise distinct questions of tax policy and administrative feasibility beyond the scope of this paper.

[30] Paul (2025) further observes that the European Commission could pursue such reforms through two existing DMA mechanisms: a market investigation under Article 19 DMA or an implementing act under Article 13(7).

analogous to energy efficiency labels or food safety ratings. He further discusses requiring written confirmation of consent via email, mandating disclosure of the estimated monetary value of consent, and prohibiting interface designs that render the data-minimizing option less attractive. The disclosure proposal, however, builds on the (lacking) individual-level valuation identified as the pricing failure (see Section 2.3): the marginal value of a single user's consent approaches zero, while the profile-level value is firm-specific, use-contingent, and non-verifiable for any external party. Mandated disclosure would therefore either report a value near zero or assert a magnitude that no outside party can audit.

Kerber (2026) develops two further strategies within the current wording of Article 5(2) DMA: establishing the free, less-personalized option as the de facto default through active choice-architecture regulation, and, more far-reaching, restricting or even eliminating the consent exception for gatekeepers whose data power is most pronounced. In his assessment, such restrictions could serve contestability and data protection simultaneously, since end users cannot assess data combination, its private benefits are uncertain (better matching versus better steering), and individual consent ignores contestability externalities. On our analysis, however, they operate on a costly margin: eliminating the consent option removes data-based payment and thereby imposes the income loss (see Sections 2.3 and 3.2). The disagreement reduces to an unmeasured empirical parameter – whether behavioral advertising under combined data primarily generates matching gains or extracts surplus through steering – and both strategies intensify the informational demands on the regulator (see Section 4.3).

Apple's App Tracking Transparency (ATT), introduced with iOS 14.5 in April 2021, provides a real-world test case for a significantly simplified consent architecture. Every app must obtain a single, binary opt-in before accessing the device’s advertising identifier (IDFA), which had previously enabled cross-app tracking and profile-building by third-party advertising platforms, most notably Meta. Compared with the multi-layered consent interfaces common under the GDPR, this design eliminates many of the informational and design-related frictions discussed above. The empirical evidence, however, confirms the structural distortions predicted by the present analysis. Opt-out rates have been high, and the resulting restriction of cross-app data flows has redistributed advertising revenues toward platforms with large first-party data reserves – most notably Apple itself (Kollnig et al., 2022; Krämer, 2026). Aridor et al. (2025) quantify the downstream effects on e-commerce firms, finding revenue declines in the range of 8 to 40 % for firms with high pre-ATT dependence on targeted advertising via Meta, with smaller firms disproportionately affected. Kesler (2023) documents a corresponding shift from

ad-funded to paid monetization models among app developers. At the same time, the privacy gains remain ambiguous: Kollnig et al. (2022) show that tracking libraries persisted in many apps despite ATT, and Nam & Kwon (2026) find that ATT increased rather than alleviated users' privacy concerns in the short term. The competitive implications have prompted enforcement action by several European competition authorities.[31] The ATT experience thus illustrates that even a substantially improved consent design reproduces the competitive asymmetries identified in this paper – entrenching incumbents with first-party data advantages while burdening smaller competitors.

While the last example and framework-based proposals indicate meaningful improvements, they share a common limitation: they continue to place the decisional burden on the individual end user, albeit under improved conditions. The behavioral distortions, such as loss aversion, default bias, consent fatigue, and structural opacity of data value, are not fully resolved by simplified interface design alone. This motivates scrutiny of institutional alternatives that shift governance away from the individual.

### 4.2 Institutional options beyond individual consent

A growing body of literature proposes replacing or supplementing individual consent with institutional arrangements that aggregate end users' bargaining power and professionalize data combination governance. The most prominent is the data fiduciary model (also known as 'information fiduciaries' and 'data trustees'), imposing legally binding duties analogous to those borne by professionals entrusted with clients' confidential information.

Building on this fiduciary concept, Dobkin (2018) operationalizes it through prohibitions on covert manipulation and on differential pricing based on sensitive attributes, transfer restrictions whose obligations extend to recipients, and substantially simplified privacy policies. Wilson & Reid (2024) extend this by embedding data protection rules within broader fiduciary duties of care, loyalty, and confidentiality. Most notably, they propose a reversal of the evidentiary burden of proof: any entity subject to consumer privacy regulation would be presumed to be a data controller unless it demonstrates otherwise, significantly lowering the evidentiary threshold for enforcement. Richards & Hartzog (2019) advance a related, though

[31] The competitive implications of ATT are currently under active scrutiny: the BKartA is conducting a market test on the impact of Apple's revised ATT prompts (Federal Cartel Office (Bundeskartellamt), 2025). Beyond the German market test, the Italian and French Competition Authorities both investigated Apple's ATT framework and imposed fines (French Competition Authority (Autorité de la concurrence), 2025; Italian Competition Authority (Autorità Garante della Concorrenza e del Mercato), 2025).

distinct shift. Rather than reversing the evidentiary burden of proof, they reallocate the compliance burden from end users to data-processing entities by imposing non-waivable fiduciary duties and deploying consumer protection law to prohibit manipulative extraction techniques.[32]

Alongside fiduciary duties, several authors propose intermediary institutions. Bergemann et al. (2023) develop a model of data intermediaries operating as exclusive agents for end users. A regulator, which the authors envisage as established under a new regulatory framework rather than identifying any existing authority, would establish standardized tiers of data sharing, ranging from fully anonymized sharing, for which end users would pay a fee, to comprehensive sharing including purchase attribution (linking an ad exposure to the resulting purchase), which would generate financial compensation for participating end users. Platforms would only collect data for free, limited to the purpose of the core platform service.[33] Further processing would require purchasing data access rights from intermediaries. Competition among intermediaries would create incentives for favorable payout rates and data security. Krämer & Schnurr (2022) propose complementary institutional mechanisms: independent data trusts that securely aggregate and anonymize data, and data sandboxes permitting third-party algorithms to be trained on raw data without exposing personal information. These structures enable the realization of data synergies for research, innovation, and AI development while maintaining enforceable privacy standards – precisely the productive dimension of data combination that the current design sacrifices.

A further strand emphasizes data portability frameworks and market-based mechanisms. Sen (2022) examines whether data markets based on individual data portability can yield improved welfare outcomes, finding that markets in which end users sell data to third parties could produce Pareto improvements, outcomes in which at least one party is made better off without making any other party worse off. Parker et al. (2020) propose adapting the European Union's revised Payment Services Directive (PSD2) framework (Directive (EU) 2015/2366)[34] as a

[32] This reliance on consumer protection law carries a structural caveat: as an ex-post instrument, it is triggered only once an infringement has occurred, and someone pursues it, which is time-consuming and burdensome for the individual consumer. The shift toward consumer law, therefore, risks lowering the effective level of protection relative to ex-ante prohibition, unless paired with proactive enforcement.

[33] Notably, this mirrors the data minimization principle already enshrined in Article 5(1)(c) GDPR. Thus, the model's contribution lies less in the substantive standard than in its enforcement, since the mandatory act of purchasing access rights makes minimization more likely to be observed in practice.

[34] PSD2 requires account-servicing payment service providers to grant authorized third-party providers access to customer payment account data via standardized interfaces, provided the customer has given explicit consent. By

blueprint for mandated data-sharing.[35] Notably, the consent underlying a PSD2-style framework differs structurally from the consent we criticize: our critique targets the transactional, take-it-or-leave-it consent demanded by a dominant gatekeeper under conditions of pronounced power asymmetry, whereas the PSD2 model embeds user authorization within a mandated, standardized infrastructure of regulated interfaces and licensed third parties. The decisional act is one of directing portability, not of choosing between full data combination and a paid alternative.

Taken together, these proposals point towards a regulatory architecture in which the governance of data combination is professionalized, collectivized, and calibrated to the economic structure of data-driven markets. These approaches are not mutually exclusive but complementary: fiduciary duties establish the normative framework, intermediary institutions provide the operational infrastructure, and portability mechanisms create the competitive pressure that disciplines both. Each of these approaches has inherent weaknesses, and even in combination, they are not without limitations. What they share is that they target the data combination rent through structural mechanisms rather than through the individual transactional choice that Article 5(2) DMA currently prescribes.[36]

### 4.3 The limits of the alternatives: a comparative perspective

So far, consent has been assessed against its observed failures for privacy and pricing, while the institutional alternatives appear – admittedly – only as idealized descriptions. A consistent assessment must compare imperfect institutional arrangements as they can realistically be expected to operate. These two failures of consent must therefore be set against the institutional weaknesses of the alternatives.

The institutional alternatives share five generic weaknesses. First, there is a knowledge problem. A regulator, fiduciary, or intermediary that sets standardized sharing tiers, certifies data practices, or prices data access must know the value of data combinations – the very value

---

mandating open data access in a previously closed market, PSD2 serves a s a regulatory precedent for structured data-sharing obligations that reduce incumbents‘ exclusive control over user-generated data (European Central Bank, 2018; Parker et al., 2020).

[35] A related but distinct approach is proposed by Acemoglu et al. (2022), who model a mediated data-sharing mechanism in which end users supply data to a trusted third-party mediator that algorithmically removes correlations between non-sharers' data and other users. Their analysis reinforces the argument that collective institutional governance is more promising than either individual consent or fiscal instruments.

[36] Data constitute one component of a complementary asset bundle, alongside talent, computing power, and industry expertise, required for developing advanced technologies such as AI (Berg et al., 2023; Hartmann & Henkel, 2020).

that remains structurally opaque (see Section 2.3) and cannot be solved by these institutions. Second, incentive and agency problems exist. Fiduciaries and intermediaries are agents with objectives of their own. Their revenue may depend on maximizing data sharing, an interest that can diverge from users' privacy preferences, while end users can monitor them no more easily than they can monitor gatekeepers. Either way, the reform relocates the information asymmetry to another level. Third, collectivization comes with a cost. Standardized tiers and collective bargaining necessarily suppress the heterogeneity of privacy preferences that individual choice, whatever its defects, at least registers. Fourth, a mandatory intermediary layer creates concentrated interests and durable institutions whose budgets depend on the problem persisting, and gatekeepers are better resourced than any other party to shape the standards under which intermediaries operate. Fifth, shifting decisions away from end users carries a normative cost for data sovereignty, the value that the GDPR's consent model is meant to protect.

The presented proposals inherit these weaknesses in varying degrees. The intermediary model of Bergemann et al. (2023) presupposes a newly created regulator that defines payout-relevant sharing tiers – administered data prices that inherit the pricing failure (see Section 2.3) – and competition among intermediaries reintroduces a complex individual choice of precisely the kind end users systematically mishandle (see Section 2.4.1). Fiduciary duties are only as effective as their enforcement, so the gap between under-resourced supervision and well-resourced regulated gatekeepers remains. Data trusts and sandboxes raise questions of governance, funding, security, and the extent to which anonymization endangers the combination rent value they are meant to preserve. Portability-based markets face the standardization and uptake problems observed in enforcing the PSD2. Further, the model of Acemoglu et al. (2022) reveals the inherent issue that individual data is statistically correlated, so property-rights solutions do not internalize data externalities any better than consent does.

This comparative perspective also clarifies what our analysis establishes and what it does not. It shows that transposing consent into Article 5(2) DMA yields a dominated instrument: regardless of the weight placed on contestability and data sovereignty, consent delivers less of both than the institutional alternatives could, while imposing welfare costs of its own. It does not establish that regulating the data combination rent is welfare-increasing. What it does not show is that constraining the data combination rent is welfare-increasing in the first place – a prior question that turns on weighing the competitive harm of the rent (see Section 2) against the implementation costs and failure risks set out here (Kerber & Hornung, 2026; Schweitzer, 2017), an error-cost comparison that varies with the specific gatekeeper and data use. Our

conclusion is therefore conditional: if the legislator seeks to enhance contestability by constraining the rent, as Article 5(2) DMA does, then instruments calibrated to the rent's economic structure are preferable to the consent mechanism.

## 5 Conclusion

This paper has argued that relying on the GDPR's consent framework creates a structural mismatch inherent to Article 5(2) DMA. The mismatch is systematic. It follows from the economic characteristics of the data combination rent and the structural limitations of consent as an instrument.

The analysis showed that the decisive competitive lever in data-driven markets lies fundamentally in the integration of heterogeneous data streams across services. This data combination rent is economically ambivalent – it drives innovation, sustains zero-price business models, and funds R&D, while simultaneously erecting barriers to entry, deepening ecosystem dependency, and enabling consumer surplus extraction. Against this background, GDPR consent causes recurrent distortions: it potentially entrenches end users' inertia to give consent for well-known incumbents (i.e., gatekeepers), fragments data ecosystems, overstretches end users' capacity for informed choice for data sovereignty in closed ecosystems, and reduces consumer welfare by restricting data-based payment. Therefore, Article 5(2) DMA generates a two-fold regulatory impasse: neither widespread consent nor widespread refusal advances the data competition or strengthens effective data sovereignty – the latter largely stemming from the lack of (quantifiable/ observable) value of combined data from the perspective of end users

Alternative approaches exist, but none is a cure-all. Within the consent framework, stricter standards tailored to gatekeepers' core platform services, granular consent architectures, and independent rating entities (see Section 4.1) represent improvements. Still, none removes the decisional burden from the least-equipped party. Institutional alternatives target the data combination rent more directly but carry failure risks of their own. They relocate rather than resolve the valuation problem, create new agency dependencies (end users vs. institutional actors), and impose collectivization costs (see Section 4.3). The choice between the alternatives is therefore of a comparative nature and implies a degree of imperfect institutions.

Several implications for future research emerge. First, the interaction between data combination restrictions and AI development warrants closer examination. As combined cross-service data constitutes a critical training input for generative AI, the effects of restricting data combination under Article 5(2) DMA extend to the competitive landscape for AI services. Second, the

welfare comparison between data-based and monetary payment requires empirical quantification. This paper has identified the theoretical asymmetry, but the magnitude of the income effect and its distributional incidence remain open questions, as does the relative weight of matching gains and surplus extraction in behavioral advertising – the parameter on which the assessment of stricter consent requirements turns (see Sections 2.2 and 4.1). Third, the institutional design questions (see Section 4.3) remain open and merit dedicated empirical and theoretical work.

Overall, the regulatory challenge posed by data combination in digital markets is real. Article 5(2) DMA represents an important recognition of this challenge. But effective regulation requires instruments calibrated to the economic structure of the phenomenon they govern. The consent mechanism, transplanted from a fundamental rights framework premised on individual autonomy, is structurally mismatched to the dynamics of data-driven competition. Our conclusion is accordingly conditional: if the European legislator maintains the DMA objectives of contestability and fairness, the alternatives surveyed in this paper are conceivable instruments that are better calibrated to that objective than consent, though each carries institutional failure risks of its own, and whether any of them also dominates non-intervention remains an open empirical question. Their systematic comparative assessment, rather than their immediate implementation, should be the priority for scholars and policymakers.

**References**


Abrahamson, Z. (2014). Essential Data. *The Yale Law Journal*, *124*(3), 867–881.

Acemoglu, D., Makhdoumi, A., Malekian, A., & Ozdaglar, A. (2022). Too Much Data: Prices and Inefficiencies in Data Markets. *American Economic Journal: Microeconomics*, *14*(4), 218–256. https://doi.org/10.1257/mic.20200200

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y., & Wilson, S. (2017). Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys*, *50*(3). https://doi.org/10.1145/3054926

Acquisti, A., & Grossklags, J. (2005). Privacy and Rationality in Individual Decision Making. *IEEE Security and Privacy*, *3*(1), 26–33. https://doi.org/10.1109/MSP.2005.22

Acquisti, A., John, L. K., & Loewenstein, G. (2013). What is privacy worth? *Journal of Legal Studies*, *42*(2), 249–274. https://doi.org/10.1086/671754

Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature*, *54*(2), 442–492. https://doi.org/10.1257/jel.54.2.442

Andriychuk, O., Podszun, R., Hubková, P., Zheng, K., Ganesh, A., Hinck, S., & Van Den Boom, J. (2025). *Consultation on the Joint Guidelines on the Interplay between the Digital Markets Act and the General Data Protection Regulation*. https://doi.org/https://dx.doi.org/10.2139/ssrn.5884542

Aridor, G., Che, Y.-K., Hollenbeck, B., Kaiser, M., & Mccarthy, D. (2025). *Evaluating the Impact of Privacy Regulation on E-Commerce Firms: Evidence from Apple's App Tracking Transparency* (Forthcoming; Law & Economics Center at George Mason University Scalia Law School Research Paper Series). https://doi.org/https://dx.doi.org/10.2139/ssrn.4698374

Aridor, G., Che, Y.-K., & Salz, T. (2020). *The Economic Consequences of Data Privacy Regulation: Empirical Evidence from GDPR* (26900; NBER Working Paper Series). https://doi.org/https://dx.doi.org/10.2139/ssrn.3522845

Baker, J. (2026, March 16). *Few changes, little benefit for consumers: Meta's latest "pay or ok" model draws familiar fire*. Euperspectives.Eu. https://euperspectives.eu/2026/03/meta-pay-or-ok/

Bamberger, K. A., & Corren, E. (2026). Untangling Privacy and Competition. *Iowa Law Review*, *111*(Forthcoming), 1331. https://doi.org/https://dx.doi.org/10.2139/ssrn.5567858

Basaure, A., Töyli, J., & Mähönen, P. (2025). Regulating data platforms from a value of data approach. *Digital Policy, Regulation and Governance*, *27*(3), 369–385. https://doi.org/10.1108/DPRG-06-2024-0119

Berg, J. M., Raj, M., & Seamans, R. (2023). Capturing value from artificial intelligence. *Academy of Management Discoveries*, *9*(4), 424–428. https://doi.org/10.5465/amd.2023.0106

Bergemann, D., Crémer, J., Dinielli, D., Groh, C.-C., Heidhues, P., Schäfer, M., Schnitzer, M., Morton, F. M. S., Seim, K., & Sullivan, M. (2023). Market Design For Personal Data. *Yale Journal on Regulation*, *40*, 1056–1120.

Blockx, J. (2025). The failure of the EU's "meta-regulation" of the digital sector-Too much paperwork, too few sanctions. *The Many Faces and Faces of the Enforcement of European Union Law: Adapting in the Ever-Evolving Landscape and Empowering Change for Successful Policies, 11-12 December 2025,Utrecht University*. https://repository.uantwerpen.be/docman/irua/53e149motoMf6

Botta, M., & da Costa Leite Borges, D. (2023). *User Consent at the Interface of the DMA and the GDPR. A Privacy-setting Solution to Ensure Compliance with ART. 5(2) DMA* (68; Robert Schuman Centre for Advanced Studies Research Paper). https://doi.org/https://dx.doi.org/10.2139/ssrn.4650373

Botta, M., & Wiedemann, K. (2019). Exploitative Conducts in Digital Markets: Time for a Discussion after the Facebook Decision. *Journal of European Competition Law & Practice*, *10*(8), 465–478. http://www.oecd.org/daf/competition/big-data-bringing-competition-

Bourreau, M., & de Streel, A. (2019). *Digital Conglomerates and EU Competition Policy*. https://doi.org/https://dx.doi.org/10.2139/ssrn.3350512

Bundeskartellamt (2019, February 6). Case B6-22/16: Facebook Inc. i.a. - The Use of Abusive Business Terms Pursuant to Section 19 (1) GWB. Retrieved April 15, 2026, from https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf

Campbell, J., Goldfarb, A., & Tucker, C. (2015). Privacy Regulation and Market Structure. *Journal of Economics and Management Strategy*, *24*(1), 47–73. https://doi.org/https://doi.org/10.1111/jems.12079

Cennamo, C., Kretschmer, T., Constantiou, I., & Garcés, E. (2025). *Economic Impact of the Digital Markets Act on European Businesses and the European Economy*. https://www.dmcforum.net/wp-content/uploads/2025/06/120625-FINAL-CCIA-DMA-Report-.pdf

COM(2020) 842 Final. Proposal for a Regulation of the Euorpean Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act).

Competition & Markets Authority (CMA). (2020). *Online platforms and digital advertising - Market study final report*. https://assets.publishing.service.gov.uk/media/5efc57ed3a6f4023d242ed56/Final_report_1_July_2020_.pdf

Condorelli, D., & Padilla, J. (2020). Harnessing Platform Envelopment in the Digital World. *Journal of Competition Law and Economics*, *16*(2), 143–187. https://doi.org/10.1093/joclec/nhaa006

Corrado, C., Haskel, J., Iommi, M., & Jona-Lasinio, C. (2022). *The value of data in digital-based business models: Measurement and economic policy implications* (1723; OECD Economics Department Working Papers, Vol. 1723). https://doi.org/10.1787/d960a10c-en

Crémer, J., de Montjoie, Y.-A., & Schweitzer, H. (2019). *Competition policy for the digital era. Final report.* https://doi.org/10.2763/407537

Cziehso, G. P., Schaefers, T., & Kukar-Kinney, M. (2019). Free no more - investigating customer reactions to unexpected free-to-fee switches. *Journal of Business Research*, *101*, 229–242. https://doi.org/10.1016/j.jbusres.2019.03.050

Datta, A. (2026, March 7). *Meta's ad model still violates EU tech rules, say consumer groups*. Euractiv.Com. https://www.euractiv.com/news/metas-ad-model-still-violates-eu-tech-rules-say-consumer-groups/

De Cornière, A., & Taylor, G. (2025). Data and Competition: A Simple Framework. *RAND Journal of Economics*, *56*(4), 494–510. https://doi.org/10.1111/1756-2171.70020

De Fortuny, E. J., Martens, D., & Provost, F. (2013). Predictive modeling with big data: Is bigger really better? *Big Data*, *1*(4), 215–226. https://doi.org/10.1089/big.2013.0037

Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on Payment Services in the Internal Market, Amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1923/2010, and Repealing Directive 2007/64/EC.

Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on Certain Aspects Concerning Contracts for the Supply of Digital Content and Digital Services.

Dobkin, A. (2018). Information Fiduciaries in Practice: Data Privacy and User Expectations. *Berkeley Technology Law Journal*, *33*, 1. https://doi.org/10.15779/Z38G44HQ81

European Central Bank. (2018, March). *The revised Payment Services Directive (PSD2) and the transition to stronger payments security*. Ecb.Europa.Eu. https://www.ecb.europa.eu/press/intro/mip-online/2018/html/1803_revisedpsd.en.html

European Commission. (2025, December). *Meta commits to give EU users choice on personalised ads under Digital Markets Act*. Digital-Markets-Act.Ec.Europa.Eu. https://digital-markets-act.ec.europa.eu/meta-commits-give-eu-users-choice-personalised-ads-under-digital-markets-act-2025-12-08_en

European Data Protection Board (edpb). (2024). *Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms - Adopted on 17 April 2024*. https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-082024-valid-consent-context-consent-or_en

Federal Cartel Office (Bundeskartellamt). (2025, December 2). *Bundeskartellamt assesses solutions proposed by Apple in ATTF proceedings - market test has started*. Bundeskartellamt.De. https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2025/12_02_2025_ATTF.html

Fourberg, N., Tas, S., Wiewiorra, L., Godlovitch, I., de Streel, A., Jacquemin, H., Hill, J., Nunu, M., Bourguigon, C., Jacques, F., Ledger, M., & Lognoul, M. (2021). *Online advertising: the impact of targeted advertising on advertisers, market access and consumer choice*.

https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662913/IPOL_STU(2021)662913_EN.pdf

French Competition Authority (Autorité de la concurrence ). (2025, March 31). *Targeted advertising: the Autorité de la concurrence imposes a fine of €150,000,000 on Apple for the implementation of the App Tracking Transparency ("ATT") framework.* Autoritedelaconcurrence.Fr. https://www.autoritedelaconcurrence.fr/en/press-release/targeted-advertising-autorite-de-la-concurrence-imposes-fine-eu150000000-apple

Furman, J., Coyle, D., Fletcher, A., McAuley, D., & Marsden, P. (2019). *Unlocking digital competition - Report of the Digital Competition Expert Panel*. https://www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel

Gal, M. S., & Aviv, O. (2020). The Competitive Effects of the GDPR. *Journal of Competition Law and Economics*, *16*(3), 349–391. https://doi.org/https://doi.org/10.1093/joclec/nhaa012

Gal, M. S., & Rubinfeld, D. L. (2019). Data Standardization. *New York University Law Review*, *94*(4). www.researchgate.net/profile/James_Hendler/publication/12011854_

Geradin, D., Karanikioti, T., & Katsifis, D. (2021). GDPR Myopia: how a well-intended regulation ended up favouring large online platforms - the case of ad tech. *European Competition Journal*, *17*(1), 47–92. https://doi.org/10.1080/17441056.2020.1848059

Goldberg, S. G., Johnson, G. A., & Shriver, S. K. (2024). Regulating Privacy Online: An Economic Evaluation of the GDPR. *American Economic Journal: Economic Policy*, *16*(1), 325–358. https://doi.org/10.1257/pol.20210309

Gradwohl, R., & Tennenholtz, M. (2022). Pareto-Improving Data-Sharing. *Arxiv.Org*. https://doi.org/10.48550/arxiv.2205.11295

Gregory, R. W., Henfridsson, O., Kaganer, E., & Kyriakou, H. (2021). The Role of Artificial Intelligence and Data Network Effects for Creating User Value. *Academy of Management Review*, *46*(3).

Hagiu, A., & Wright, J. (2023). Data-enabled learning, network effects, and competitive advantage. *RAND Journal of Economics*, *54*(4).

Hartmann, P., & Henkel, J. (2020). The Rise of Corporate Science in AI: Data as a Strategic Resource. *Academy of Management Discoveries*, *6*(3). https://doi.org/https://doi.org/10.5465/amd.2019.0043

Heidhues, P., & Köszegi, B. (2004). *The impact of consumer loss aversion on pricing* (SP II 2004-17; WZB Discussion Paper). https://nbn-resolving.org/urn:nbn:de:0168-ssoar-197327

Hoeren, T., & Fuchs, N.-M. (2025). *Compatibility of subscription-based models with Article 5 (2) of the DMA - Case Study: Commission v Meta Platforms Inc*. https://doi.org/https://dx.doi.org/10.2139/ssrn.5490206

Hulsen, T. (2020). Sharing Is caring - Data Sharing Initiatives In Healthcare. *International Journal of Environmental Research and Public Health*, *17*(9). https://doi.org/10.3390/ijerph17093046

Iansiti, M. (2021). *The Value of Data and Its Impact on Competition* (22–002; NOM Unit Working Paper). https://www.hbs.edu/ris/Publication%20Files/22-002submitted_835f63fd-d137-494d-bf37-6ba5695c5bd3.pdf

Information Commissioner's Office (ICO). (2025, January 21). *Consent or Pay*. Cy.Ico.Org.Uk. https://cy.ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/online-tracking/consent-or-pay/appropriate-fee/

Italian Competition Authority (Autorità Garante della Concorrenza e del Mercato). (2025, December 22). *A561 - The Italian Competition Authority fines Apple over 98 million euro for abuse of a dominant position*. Agcm.It. https://en.agcm.it/en/media/press-releases/2025/12/A561

Johnson, G. (2022). *Economic Research on Privacy Regulation: Lessons from the GDPR and Beyond* (30705; NBER Working Paper Series). https://doi.org/https://doi.org/10.3386/w30705

Johnson, G., Shriver, S. K., & Goldberg, S. G. (2023). Privacy & market concentration: Intended & unintended consequences of the GDPR. *Management Science*, *69*(10), 5695–5721. https://doi.org/https://dx.doi.org/10.2139/ssrn.3477686

Jones, C. I., & Tonetti, C. (2020). Nonrivalry and the Economics of Data. *American Economic Review*, *110*(9), 2819–2858. https://doi.org/10.1257/aer.20191330

Jorzik, N., Kirchhof, P. J., & Mueller-Langer, F. (2024). Industrial data sharing and data readiness: a law and economics perspective. *European Journal of Law and Economics*, *57*(1–2), 181–205. https://doi.org/10.1007/s10657-023-09787-4

Katz, M. L., & Shapiro, C. (1994). Systems Competition and Network Effects. *Journal of Economic Perspectives*, *8*(2), 93–115.

Ke, T., & Sudhir, K. (2023). Privacy Rights and Data Security: GDPR and Personal Data Markets. *Management Science*, *69*(8), 4389–4412. https://doi.org/https://doi.org/10.1287/mnsc.2022.4614

Kerber, W. (2026). *The Commission's Art. 5(2) DMA Meta Decision Between Data Protection Law and Competition Policy: A Missed Opportunity?* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=6982261

Kerber, W., & Hornung, P. (2026). *Decentralised Coordination Order, Market Regulation and Economics: The Perspective of Heike Schweitzer*. https://doi.org/https://dx.doi.org/10.2139/ssrn.6282779

Kerber, W., & Zolna, K. K. (2022). The German Facebook case: the law and economics of the relationship between competition and data protection law. *European Journal of Law and Economics*, *54*(2), 217–250. https://doi.org/10.1007/s10657-022-09727-8

Kesler, R. (2023). *The Impact of Apple's App Tracking Transparency on App Monetization*. https://doi.org/https://dx.doi.org/10.2139/ssrn.4090786

Kirkwood, M. (2025, September 26). *Will the EU Designate AI Under the Digital Markets Act?* Techpolicy.Press. https://www.techpolicy.press/will-the-eu-designate-ai-under-the-digital-markets-act/

Kollnig, K., Shuba, A., Van Kleek, M., Binns, R., & Shadbolt, N. (2022). Goodbye Tracking? Impact of iOS App Tracking Transparency and Privacy Labels. *ACM International Conference Proceeding Series*, 508–520. https://doi.org/10.1145/3531146.3533116

Krämer, J. (2026). Balancing privacy and platform power in the mobile ecosystem: The case of Apple's App Tracking Transparency. *Computer Law & Security Review*, *60*. https://doi.org/10.1016/j.clsr.2025.106255

Krämer, J., & Schnurr, D. (2022). Big Data and Digital Markets Contestability: Theory of Harm and Data Access Remedies. *Journal of Competition Law and Economics*, *18*(2), 255–322. https://doi.org/https://doi.org/10.1093/joclec/nhab015

Lamb, T. (2025, July 2). *Why the Commission's Decision Undermines the Goals of the DMA*. About.Fb.Com. https://about.fb.com/news/2025/07/why-the-commissions-decision-undermines-the-goals-of-the-dma/

Lambrecht, A., & Tucker, C. E. (2015). *Can Big Data Protect a Firm from Competition?* https://doi.org/https://doi.org/10.2139/ssrn.2705530

Mancini, J., & Volpin, C. (2018). *Quality Considerations in Digital Zero-Price Markets: OECD Background Paper (October 9, 2018) - DAF/COMP(2018)14*. https://doi.org/https://doi.org/10.2139/ssrn.3862529

Martin, N., & von Grafenstein, M. (2026). Innovation and the GDPR: Much ado about quite a lot. *Computer Law and Security Review*, *60*. https://doi.org/10.1016/j.clsr.2026.106270

Mendelsohn, J., & Färber, N. L. (2024). Pay or Consent - Datenschutz im Spannungsfeld zwischen Nutzereinwilligung und Überwachungskapitalismus. In C. Heinze & B. Steinrötter (Eds.), *KI und Daten - Digitalregulierung auf dem Höhepunkt. DSRI-Herbstakademie 2024* (pp. 103–124). Oldenburger Verlag für Wirtschaft, Informatik und Recht.

Meta Platforms Inc. and Others v. Bundeskartellamt, Case C-252/21, ECLI:EU:C:2023:537 (2023).

Moody, D., & Walsh, P. (1999). Measuring The Value Of Information: An Asset Valuation Approach. *European Conference on Information Systems (ECIS'99)*. https://blogs.ed.ac.uk/edneuro/wp-content/uploads/sites/11612/2026/02/1000.pdf

Morel, V., Karegar, F., & Santos, C. (2025, October 22). "I will never pay for this" - Perception of fairness and factors affecting behaviour on 'pay-or-ok' models. *Privacy Technologies and Policy: 13th Annual Privacy Forum, APF 2025*. https://doi.org/https://doi.org/10.1007/978-3-032-07574-1_1

Mühlhoff, R. (2023). Predictive privacy: Collective data protection in the context of artificial intelligence and big data. *Big Data and Society*, *10*(1). https://doi.org/10.1177/20539517231166886

Nam, S., & Kwon, Y. (2026). The impact of platform-level privacy policies on users' privacy concerns: Evidence from Apple App Tracking Transparency via a dynamic difference-in-difference analysis. *Telecommunications Policy*, *50*(6). https://doi.org/10.1016/j.telpol.2026.103192

Natvik, G. J., & Tangerås, T. P. (2023). *Paying with Personal Data* (1481; IFN Working Paper). https://www.econstor.eu/bitstream/10419/297277/1/wp1481.pdf

Newman, J. M. (2015). Antitrust in Zero-Price Markets: Foundations. *The University of Pennsylvania Law Review*, *164*(1), 149–206. https://repository.law.miami.edu/fac_articles

Newman, J. M. (2016). Antitrust in Zero-Price Markets: Applications. *Washington University Law Review*, *94*(1), 2016. http://openscholarship.wustl.edu/law_lawreviewhttp://openscholarship.wustl.edu/law_lawreview/vol94/iss1/5

Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. *Conference on Human Factors in Computing Systems - Proceedings*. https://doi.org/10.1145/3313831.3376321

Parker, G., Petropoulos, G., & van Alstyne, M. (2020). *Digital platforms and antitrust* (6; Bruegel Working Paper). https://doi.org/https://dx.doi.org/10.2139/ssrn.3608397

Paul, N. (2025). Smokescreens of digital markets—choice manipulation and the illusion of consent. *Journal of European Competition Law and Practice*, *16*(3), 208–222. https://doi.org/10.1093/jeclap/lpaf050

Petit, N., & Teece, D. J. (2021). Innovating Big Tech firms and competition policy: favoring dynamic over static competition. *Industrial and Corporate Change*, *30*(5), 1168–1198. https://doi.org/10.1093/icc/dtab049

Peukert, C., Bechtold, S., Batikas, M., & Kretschmer, T. (2022). Regulatory Spillovers and Data Governance: Evidence from the GDPR. *Marketing Science*, *41*(4), 318–340. https://doi.org/10.1287/mksc.2021.1339

Podszun, R. (2020, August 28). *Facebook Case: The Reasoning*. D-Kart.De. https://www.d-kart.de/blog/2020/08/28/facebook-case-the-reasoning/

Podszun, R. (2022). Should gatekeepers be allowed to combine data? Ideas for Art. 5(a) of the draft Digital Markets Act. *GRUR International*, *71*(3), 197–205. https://doi.org/https://doi.org/10.1093/grurint/ikab131

Posner, R. A. (1978). An Economic Theory of Privacy. *AEI Journal on Government and Society (Regulation)*, (May/June), 19–26.

Prüfer, J., & Schottmüller, C. (2021). Competing With Big Data. *The Journal of Industrial Economics*, *69*(4), 967–1008. https://www.stati

Purtova, N., & van Maanen, G. (2024). Data as an economic good, data as a commons, and data governance. *Law, Innovation and Technology*, *16*(1), 1–42. https://doi.org/10.1080/17579961.2023.2265270

Rauch, F. (2013). Advertising expenditure and consumer prices. *International Journal of Industrial Organization*, *31*(4), 331–341. https://doi.org/10.1016/j.ijindorg.2013.05.001

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation).

Regulation (EU) 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).

Ribera Martínez, A. (2022). The Circularity Of Consent In The DMA: A Close Look Into The Prejudiced Substance of Articles 5(2) And 6(10). *Rivista Concorrenza e Mercato*, *29*(Numero Speciale Concorrenza e Regolazione nei Mercati Digitale), 191–212. https://doi.org/https://dx.doi.org/10.2139/ssrn.4643462

Ribera Martínez, A. (2026). If I Could Have, I Would Have: Data Governance and Trust in the Implementation of Article 5(2) of the DMA. In G. Enes, I. Neves, & T. Morais Rocha (Eds.), *A Digital Europe for Citizens: Data Governance, Data Markets, Data Services* (pp. 137–156). Springer. https://doi.org/https://doi.org/10.1007/978-3-032-02500-5_8

Richards, N. M., & Hartzog, W. (2019). The Pathologies of Digital Consent. *Washington University Law Review*, *96*, 1461–1503. https://scholarship.law.bu.edu/faculty_scholarship/3067

Rockenbach, B., Sadrieh, A., & Schielke, A. (2021). Paying with your personal data: the insensitivity of private information provision to asymmetric benefits. *Journal of the Economic Science Association*, *7*(1), 64–73. https://doi.org/10.1007/s40881-021-00102-y

Rubinfeld, D. L., & Gal, M. S. (2017). Access Barriers to Big Data. *Arizona Law Review*, *59*(2), 339–381. http://sloanreview.mit.edu/article/how-big-data-is-different/.

Schweitzer, H., & Metzger, A. (2023). Data Access under the Draft Data Act, Competition Law and the DMA: Opening the Data Treasures for Competition and Innovation? *GRUR International*, *72*(4), 337–356. https://doi.org/10.1093/grurint/ikad012

Schweitzer, H., Metzger, A., Blind, K., Richter, H., Niebel, C., & Gutmann, F. (2022). *Data access and sharing in Germany and in the EU: Towards a coherent legal framework for the emerging data economy - A legal, economic and competition policy angle - Final Report*. https://doi.org/https://dx.doi.org/10.2139/ssrn.4270272

Scott Morton, F., Bouvier, P., Ezrachi, A., Jullien, B., Katz, R., Kimmelman, G., Melamed, A. D., & Morgenstern, J. (2019). *Committee for the Study of Digital Platforms. Market Structure and Antitrust Subcommittee. Report.* https://research.chicagobooth.edu/-/media/research/stigler/pdfs/market-structure---report-as-of-15-may-2019.pd

Sen, A. (2022). Are data markets a solution to big tech market power? A competitive analysis. *Journal of Government and Economics*, *7*. https://doi.org/10.1016/j.jge.2022.100052

Simone, C., & Laudando, A. (2025). Principles and obligations of the Digital Markets Act in regulating the economic power of gatekeepers: Positive, negative or trade-off effects? *Electronic Markets*, *35*(1). https://doi.org/10.1007/s12525-025-00788-6

Stigler, G. J. (1980). An Introduction to Privacy in Economics and Politics. *Journal of Legal Studies*, *9*, 623–644.

The European Consumer Organisation (BEUC). (2025). *BEUC Assessment of Meta's Latest Pay-Or-Consent Policy For Facebook and Instagram Users*. https://www.beuc.eu/sites/default/files/publications/BEUC-X-2025-002_Meta_s_latest_pay-or-consent_policy.pdf

Tian, L., Turjeman, D., & Levy, S. (2026). Privacy-Preserving Data Fusion. *Marketing Science*, *0*(0). https://doi.org/10.1287/mksc.2023.0068

Tirole, J. (2023). Competition and the Industrial Challenge for the Digital Age. *Annual Review of Economics*, *15*, 573–605. https://doi.org/10.1146/annurev-economics

Tucker, C. (2019). Digital Data, Platforms and the Usual [Antitrust] Suspects: Network Effects, Switching Costs, Essential Facility. *Review of Industrial Organization*, *54*(4), 683–694. https://doi.org/10.1007/s11151-019-09693-7

van de Waerdt, P. J. (2020). Information asymmetries: recognizing the limits of the GDPR on the data-driven market. *Computer Law and Security Review*, *38*. https://doi.org/10.1016/j.clsr.2020.105436

van de Waerdt, P. J. (2023a). "Everything the Data Touches Is Our Kingdom": Market Power of "Data Ecosystems." *World Competition*, *46*(1), 65–98. https://www.britannica.com/topic/conglomer

van de Waerdt, P. J. (2023b). From monocle to spectacles: competition for data and "data ecosystem building." *European Competition Journal*, *19*(2), 191–225. https://doi.org/10.1080/17441056.2023.2169366

Varian, H. (2022). Advertising Costs and Product Prices. *Journal of Law and Economics*, *65*(6 S2: A Special Issue in Honor of Sam Peltzman), S419–S431. https://doi.org/https://doi.org/10.1086/721269

Wilson, N., & Reid, A. (2024). Data Controllers as Data Fiduciaries: Theory, Definitions & Burdens of Proof. *University of Colorado Law Review*, *95*(1), 175–218.

Witt, A. C. (2024). Meta v Bundeskartellamt - data-based conduct between antitrust law and regulation. *Journal of Antitrust Enforcement*, *12*. https://ssrn.com/abstract=4763434

Xu, F., Wang, X., & Zhang, F. (2025). Consumer Privacy in Online Retail Supply Chains. *Management Science*, *71*(10). https://doi.org/https://doi.org/10.1287/mnsc.2022.01819

Yeom, S., Giacomelli, I., Fredrikson, M., & Jha, S. (2018). Privacy Risk in Machine Learning: Analyzing the Connection to Overfitting. *IEEE 31st Computer Security Foundations Symposium*, 268–282. http://arxiv.org/abs/1709.01604

Zolna, K. K. (2025). *The law and economics of Art. 5(2) DMA: The case of Meta* (22; MAGKS Joint Discussion Paper Series in Economic). https://www.econstor.eu/handle/10419/333562