Beyond Informed Consent

Consumer Data Preferences and the Case for Enforcement-Oriented Transparency

Maximilian Becker & Catalina Goanta
University of Siegen & Utrecht University

WORKING PAPER SERIES | NO. 41 | JULY 2026
Collaborative Research Center 1187 Media of Cooperation

Working Paper Series
Collaborative Research Center 1187 Media of Cooperation

Print-ISSN 2567–2509
Online-ISSN 2567–2517
DOI: doi.org/10.25819/ubsi/10978
dspace.ub.uni-siegen.de/handle/ubsi/9448
URN urn:nbn:de:hbz:467-94487

This work is licensed under the Creative Commons Attribution-NonCommercial-No-Derivatives 4.0 International License.

This Working Paper Series is edited by the Collaborative Research Center Media of Cooperation and serves as a platform to circulate work in progress or preprints in order to encourage the exchange of ideas. Please contact the authors if you have any questions or comments. Copyright remains with the authors.

The Working Papers are accessible online at:
mediacoop.uni-siegen.de/working-papers-media-of-cooperation

Print copies can be ordered by sending an email to:
info@sfb1187.uni-siegen.de

Publication is funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – Project-ID 262513311 – SFB 1187.

Cover image: Yutong Liu & Digit, https://betterimagesofai.org
Layout: Dr. Karina Kirsten

Universität Siegen
SFB 1187 Medien der Kooperation
Herrengarten 3
57072 Siegen, Germany
mediacoop.uni-siegen.de
info@sfb1187.uni-siegen.de

Beyond Informed Consent
Consumer Data Preferences and the Case for Enforcement-Oriented Transparency

Maximilian Becker & Catalina Goanta
University of Siegen & Utrecht University

Abstract Digital markets have fundamentally altered the conditions under which consumers engage with data-driven platforms, yet regulatory frameworks, particularly in the EU, continue to rely on consent-based models that presuppose a level of technological literacy and informed agency that most users do not possess. Drawing on existing empirical evidence from five studies across the US, UK, and EU, this paper builds on the empirical argument that consumer preferences regarding personal data are highly unstable and shaped by framing and trust rather than genuine, well-formed values. Consumers systematically overestimate the privacy protections offered by paid services, accept personalization without understanding its commercial scope, and disregard privacy notices regardless of their clarity. This argument exposes the structural failure of transparency-as-disclosure as a regulatory strategy: informing consumers better does not fix markets distorted by asymmetric information and complex, layered business models. Rather than doubling down on consumer-facing transparency obligations, this paper proposes a shift toward enforcement-oriented business-model transparency, under which platforms would be required to disclose aspects such as data flows, monetization strategies, but also algorithmic processes to regulatory authorities and civil society. The Digital Services Act and the General Data Protection Regulation already point somewhat in this direction. Building on this logic, the paper proposes further machine-readable transparency as a complement to existing information obligations.

Keywords Consumer and data protection, digital regulation, enforcement, transparency, consent

1. Introduction

In January 2025, when the TikTok ban entered into force and TikTok was forced to temporarily shut down its activities, an unexpected phenomenon occurred. In the weeks leading to the ban, a swarm of TikTok users migrated to the Chinese app called Red Note, becoming known as 'TikTok refugees',[1] after starting trends such as 'goodbye to my Chinese spy' (Roth 2025).

This development illustrates a striking paradox: In passing the ban, the United States (US) had publicly relied on the narrative that the app is a national security liability, and peddled a moral panic about how TikTok could be used by China to send anti-democratic notifications and steal the data of US citizens (Moir 2024). And yet, in response, these very citizens the ban was supposed to protect showed their blatant disregard for privacy protection, while even the Terms of Service (ToS) were displayed in Chinese. This may be a display of nonchalance towards a right which they have been generally denied in the post 9/11 public surveillance society that merged with the capitalist surveillance developed by digital markets in the past decades.

The TikTok trend suggested that US citizens did not seem to care China could have access to their data. This pattern points to a more complex and context-dependent form of consumer responsiveness to privacy risks than the logic of consent presupposes.

1.1. The open information highway was closed all along

While this is a mere illustration reflecting consumer attitudes in a specific jurisdiction (US), it does raise a question that has been around for a while on the Internet: do consumers even care about their privacy? In the pre-commercial Internet era, when this technology was more about connecting networks than creating economic values (Leiner et al. 2009), the idea of an open 'information highway', as well as initial commercial limitations reflecting public policies (Greenstein 2000) laid the ground to expectations of free access. Coupled with some business models such as subscriptions or computer services (Mahadevan 2000) with 'freemium' characteristics, namely an approach where users can benefit from limited services for free, these developments have more or less shaped how consumers perceive, even today, the commercial dimension of the Internet.

The fast-paced development of platform business models, generally based on data collection and increased algorithmic profiling, made the Internet even more complex, and in many ways, more harmful. As the Cambridge Analytica scandal revealed ('Facebook Fined €1M over Cambridge Analytica Scandal' 2019; 'Cambridge Analytica', n.d.) when using a constellation of services such as social media, games and e-commerce, consumers fail to recognize what they should protect themselves from. The technology illiteracy resulting from the opacity of platform business models has not really improved over time, as the pace of the online world and its complexity are only exponentially accelerating (Azhar 2022).

1.2. 'Pay or OK' in an opaque environment

Instead of acknowledging this essential paradigm shift and promoting enforcement strategies focused on effective solutions for consumers, regulatory frameworks, particularly in the European Union (EU), retain doctrinal path dependencies that might no longer be fit for their original purpose. An example in this respect is the focus on user consent, which remains a raison d'être for both consumer and data protection. For consumer law, the consent paradigm reflects the private law conceptual tradition surrounding the principle of freedom of choice in contracting between private parties. For data protection consent is a facet – among others – of the inalienability of privacy as a fundamental right, which on the one hand can only be contractually limited to a restricted extent, and on the other hand requires that individuals be informed about the processing of their personal data. In addition, the underlying regulatory choice of embracing consumer agency while offering more transparency through mandated disclosures is slowly failing due to, among others, a legal fatigue potentially caused by information overload. For instance, recent developments in EU competition and data protection law that aimed to align Meta's business practices to EU standards led to the introduction of the company's Pay or OK model in November 2023 (D'Amico et al. 2024), giving users a choice between using the platform for free in exchange for their data, and paying between €5.99 and €7.99 for one account per month for Facebook or Instagram in case they did not want the platforms to use their personal data and display targeted ads. In Meta's words:

> You will only be charged for accounts on surfaces where we currently show ads, but your choice applies to all accounts added to the same Accounts Centre. This means that your information across those accounts will not be used for ads and you won't see ads on any of our Meta Products when using those accounts. Additionally, prices may vary slightly from what's listed below depending on the location that you purchase your subscription due to currency exchange rate differences, local taxes and ordinances, and inconsistencies in the pricing tiers of in-app purchases using Apple App Store and Google Play Store ('Help Center', n.d.).

1 See for instance (Xu 2025; 'What Is RedNote, the Chinese App That US "TikTok Refugees" Are Flocking to? | CNN Business', n.d.).

This model was subsequently declared incompliant with EU data protection law by the European Data Protection Board (EDPB) due to the fact that consent did not seem to be freely given.[2] This raises issues vis-à-vis other services that offer the same model, and who have so far not been in the spotlight of the EDPB. Of course, it can also be argued that very few other services have the same ubiquity as Meta's products, given that the company's online tracking models, including the Meta Pixel (Wernerfelt et al. 2025; El fraihi et al. 2024; Bekos et al. 2025) can have more significant implications for advertising (van der Vlist et al. 2022). Apart from the question of whether this interpretation of consent actually limits consumer agency, there are also a lot of concerns about consumer preferences not really aligning with the goals of EU law.

1.3. The wider interpretation of free consent: transparency obligations towards enforcement authorities

Even if consumers had a perfect interface to offer their free consent – would they choose to have more (but paid for) privacy, or more free services?

To unpack these questions, our aim is to contribute to ongoing debates in European regulatory policy around consumer and data protection by analyzing what role consumer preferences and platform business models should have in the interpretation of 'free consent', and explore whether further empowering consumers through information, transparency and consent can help preserve their autonomy in digital markets. The paper puts forth the argument that a narrow interpretation significantly reduces consumer agency, while not really solving the underlying issues of the data economy in respect to protecting weaker parties such as consumers. Moreover, the focus on consent raises the risk of legal convergence, as it is a concept playing a fundamental role in data protection and consumer protection alike, albeit in diverging ways which may lead to issues of doctrinal and practical inconsistency. Instead of focusing on transparency for consumers, the paper argues, EU legislators should shift their attention to introducing more transparency obligations towards enforcement authorities. To exemplify how this could be done, several transparency obligations from the Digital Services Act (DSA) will be discussed.

1.4. Structure of the paper

The paper is structured as follows. After the Introduction, Section 2 provides a theoretical starting point for the discussion by mapping out some recent regulatory concerns with sharing and paying with personal data across data and consumer protection. To better contextualize the discussion, the paper addresses the social media industry as an example and elaborates on emerging business models that are relevant for consumers, particularly in the light of Meta's German case with the Bundeskartellamt.[3]

Section 3 provides a general overview of academic literature on consumer preferences in terms of their willingness to share personal data in the context of commercial transactions on the Internet. The section outlines and describes a number of selected empirical studies which are leading in their fields (e.g. consumer behavior and computer science), and aggregates observations across jurisdictions and consumer preferences. Section 4 proposes an alternative to the consent paradigm illustrated by transparency obligations as enshrined in the DSA, with the purpose of proposing a new hypothesis for regulatory reform such as the expected Digital Fairness Act.

2. Sharing your data or paying with it

The internet as we know it has a complicated history reflecting a long-standing tug-of-war between a utopian dream to access to information in a free and democratic manner, and a cash register supporting fast (and often ruthless) innovation. The combination of these two perspectives shows colliding incentives. The internet began inside universities and government labs as a military research project. ARPANET was funded by public funds in the US and built by academics at a time when information sharing was not a business model, but rather the goal of scientific research (Lukasik 2011; Packard 2023; Paloque-Bergès and Schafer 2019). This created the first illusion of free information: it was free at the point of use, not free to produce.

With the advent of personal computing and access to the World Wide Web, the Internet escaped its scientific laboratory environment and went mainstream. Anyone with a computer and an Internet connection could publish a website and read the content of other websites. This led to the first search engines and information portals that brought with them advertising

2 EDPB, 'Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms', 17 April 2024, <https://www.edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf> accessed 12 January 2026; ('Statement on EDPB "Pay or Okay" Opinion', n.d.)

3 Bundeskartellamt, 'Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing', Case B6-22/16, Decision of 6 February 2019, https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf; see also CJEU, Case C-252/21, Meta Platforms Inc. and Others v. Bundeskartellamt, EU:C:2023:537 (July 4, 2023), GRUR 2023, 1131.

(ad banners) as the earliest business model maintaining online information. Advertising also contributed to the shaping of a powerful consumer habit – that online information is free of charge, and the main cost that consumers would have to pay with real money would be access to Internet Service Providers (ISPs). Against this background, platforms such as early social networks perfected the illusion of gratuity, and promised 'free' services forever, in exchange for consumer attention and data which turned advertising into behavioral mirrors for the users of such services, and leading to the motto that if a product is free, the user is actually the product (Goanta and Mulders 2019).

More recently however, we see a wave of consumer willingness to pay for certain services, when such services bring value, or when the payment can make their experience more convenient. For instance, a lot of consumers turned to streaming services when it became easier to pay for Netflix than engage in piracy, but piracy intent may still depend on the range of content available on demand (Frick, Fletcher, and Smith 2023).

At the same time, we see that apps are starting to offer a rich menu of possibilities to combine gratuitous experiences (paying with your data) with paid for content.[4] As Annabell et al explore in their analysis of TikTok's platform documentation and creator monetization (Annabell, Bishop, and Goanta 2025), platforms like TikTok are powerful private regulators shaping economic relationships with users. Instead of a single, straightforward contract (such as "terms of service"), TikTok's governance is dispersed across a large and fragmented set of 85 policy documents that influencers must navigate. These include terms, guidelines, eligibility requirements, and product-specific rules, often nested through hyperlink networks that are hard to interpret and inconsistently accessible. TikTok constructs the category of "creator" to blur the line between ordinary users and monetizing users. In doing so, it downplays professional identity and softens eligibility hierarchies shaped by metrics and region. The platform's governance intentionally remains vague on its obligations while tightly defining influencer responsibilities, thereby generating user dependence on its monetization products (ibid. 2025).

This study shows that modern social media no longer operates via a single contract and a single service; instead, monetization and participation are governed by a web of layered, product-specific agreements. This reflects how digital platforms increasingly offer a suite of interconnected products (creator funds, marketplaces, tipping, branded content), each with its own rules, making contractual engagement more complex and opaque for users. Such complexity shifts power toward platforms, challenges traditional notions of consumer contracts, and turns even the most basic legal questions (e.g. how many contracts does a consumer conclude with/on a platform every month) into cutting edge explorations of how to apply traditional rules and principles to an increasingly complex digital ecosystem of interlinked services and products.

3. Consumer willingness to share personal data: insights from empirical studies

Consumer fatigue to legal information that results in ignoring legal disclaimers about how their data may be processed has long been mapped by empirical legal research. In 2016, Ben-Shahar and Chilton did a series of experiments on a representative sample of the US adult population (n=1,484) and found that their behavior towards sharing personal data did not change with simplified disclosures. In other words, users did not care that they were giving away personal data, and not even easy disclosures meant to make consumers more suspicious of predatory data extracting services changed that attitude. This is in contrast with recent empirical research based on EU and UK (Kozyreva et al. 2021; Leszczynska and Baltag 2024), showing that consumers generally express unwillingness to share their data, but also that this willingness would increase in exchange for a free digital service (e.g. an app), which is perceived as a fair trade-off.

Empirical work on consumer willingness to share personal data is very complex, particularly due to different regulatory frameworks and different resulting business practices and consumer preferences. In spite of a growing body of literature on this topic, no comprehensive literature reviews are available. This section discusses a selection of five recent studies ranging from 2019 to 2024. Although not systematic, the section aims to showcase clear patterns across different consumer cultures and jurisdictions (e.g. US, UK, EU), as well as ambiguities that will not be soon solved by additional empirical work due to their complexity.

3.1 The studies

Winegar and Sunstein examined the monetary value individuals place on data privacy through a series of experimental surveys aimed at measuring willingness to pay (WTP) for privacy and willingness to accept (WTA) compensation for personal data sharing (Winegar and Sunstein 2019). The study sought to quantify how much consumers value privacy in financial terms and explores behavioral inconsistencies in these valuations. The authors find a large disparity between WTP and WTA, a phenomenon known as the 'endowment effect'. Participants asked for significantly more money to give up their privacy than they were willing to pay to protect

4 See also https://www.businessofapps.com/data/top-grossing-apps/.

it. For example, individuals were reluctant to share their browsing or financial data without high compensation, but at the same time showed limited willingness to pay for privacy-preserving alternatives. This suggests that privacy valuations are highly context-dependent and sensitive to framing. The study also highlights considerable heterogeneity among respondents. Some people place substantial value on privacy, while others appear indifferent, particularly when the data is less sensitive or the benefits of sharing are framed positively.

In a multidisciplinary law and computer science study in the US, Bamberger et al. (2020) looked at the question of whether consumers can pay for greater privacy in mobile apps.[5] The study combines empirical analysis of Android app behaviors with consumer survey data to assess whether paid apps actually offer better privacy protections than free ones, and whether consumers expect them to. Analyzing over 5,800 apps, the researchers found that paid apps are not consistently more privacy-preserving than free ones. Many paid apps still request extensive permissions and engage in data-sharing practices. While some paid apps collect less data than free versions, the overall variance within both categories undermines the assumption that payment reliably buys privacy. Surveys conducted alongside the technical analysis reveal a significant gap between consumer expectations and actual app behavior. Most users assume that paid apps will collect less data and provide better privacy protections. This disconnect raises concerns about informed consent and market transparency. Consumers neither receive clear, actionable information about privacy practices nor have meaningful options to choose privacy through payment.

Leszczynska and Baltag (2024) explored how willing consumers are to share personal data in exchange for personalized digital services and advertisements. Regulators, courts, and scholars are currently debating the legality of data processing for personalization purposes. Should businesses require separate consent for processing user data for personalized advertising, especially when offering free services reliant on such ads for revenue? Or is general consent for the contract enough, given personalized advertising's role in fulfilling contractual obligations (see Article 6(1)(b) GDPR)? This study investigates whether these legal distinctions reflect differences in people's willingness to share data with businesses for personalization. Are consumers less willing to share their data for personalized advertising than for personalized services that they clearly contracted for? Does that change if the service is offered for free? Drawing from both the privacy calculus and privacy as contextual integrity theory, the hypothesis posits that individuals would be more inclined to share their data when it is used to personalize the services offered by businesses (e.g., music or news recommendations). Drawing on a large-scale survey across multiple EU countries, the study examines preferences for personalization versus privacy and assesses how factors such as trust, perceived benefits, and awareness of data practices influence these preferences. The findings reveal a nuanced consumer landscape. While a majority of respondents express privacy concerns and support for non-personalized options, a significant share still opts for personalization when it is framed as beneficial (e.g. better content or convenience), which is still important for contractual freedom of choice. However, this willingness to share data diminishes when consumers are made aware of the scale and purpose of data collection, especially for behavioral advertising. The study shows that there is a demand for choice and transparency. Many consumers prefer having the option to use digital services in a non-personalized mode and expect that refusing personalization should not reduce service quality. Trust in the service provider, together with clear communication about how data will be used, is shown to significantly increase the likelihood of consumers accepting personalization.

Kozyreva et al. (2021) investigated public perceptions of algorithmic personalization and the use of personal data across Germany, the UK, and the US. The study uses representative survey data from over 3,000 participants to assess how people perceive the benefits and risks of personalization, how much control they feel they have over their data, and their preferences for digital governance. The results reveal widespread skepticism about algorithmic personalization. While some respondents recognize potential benefits, a lot of concerns were raised about loss of control, privacy intrusion, and the opaque nature of the algorithmic economy. Across all three countries, in spite of cultural and economic differences, a clear majority of participants report discomfort with the use of personal data for content curation, advertising, and news delivery, considering it to be exploitative and unfair.

Grande et al. (2022) investigated how willing consumers are to share personal digital information, but also what kind of information they would be more willing to share for health-related purposes. Using a nationally representative survey of US adults, the study looks at user attitudes toward data sharing across various health use cases and identifies the factors that influence willingness. The findings show that consumer willingness to share digital information varies significantly depending on the type of data and the intended use. Participants were more open to sharing data for public health and research purposes than for commercial uses. For instance, over 60% were willing to share search history or smartphone data if it helped control disease outbreaks or improve healthcare services, but far fewer agreed to share the same data with technology

5 Bamberger, K. A., Egelman, S., Han, C., On, A. E. B., & Reyes, I. (2020). 'Can You Pay for Privacy? Consumer Expectations and the Behavior of Free and Paid Apps'. *Berkeley Technology Law Journal*, 35(1), 327–365.

companies or advertisers. Trust is seen as a key element of the willingness to share. Respondents expressed greater comfort sharing information with universities and health systems compared to tech companies or insurance providers. Privacy concerns, perceived sensitivity of the data, and clarity about how data would be used also strongly influenced decisions.

3.2. Discussion

Taken together, these studies show how difficult it is to make confident claims about what consumers actually want when it comes to privacy and data protection and personalization in digital markets. Preferences appear unstable and context-dependent, being deeply shaped by framing, trust, and institutional design rather than reflecting fixed or well-formed consumer values.

Winegar and Sunstein's (2019) findings illustrate this instability particularly clearly. The large gap between willingness to pay (WTP) for privacy and willingness to accept (WTA) compensation for giving it up suggests that privacy is not valued in a straightforward market sense. Instead, valuations depend on psychological reference points and framing effects. Consumers appear to treat privacy as something they strongly resist losing once it is framed as "theirs", yet they show little proactive demand for privacy-protective alternatives when these require upfront payment. This tension complicates any attempt to infer consumer welfare or preference satisfaction from observed choices alone.

Information asymmetry emerges as a central explanatory factor across the selected literature. Bamberger et al. (2020) demonstrate that even when consumers are willing to pay, payment does not reliably translate into better privacy outcomes. The assumption that paid apps are more privacy-preserving is widespread but empirically unsupported. Consumers lack clear, actionable information about data practices, which undermines informed consent and makes preference expression through market mechanisms largely illusory. In such conditions, observed consumer choices cannot be taken as meaningful signals of preference for or against privacy.

The studies by Leszczynska and Baltag (2024) and Kozyreva et al. (2021) further highlight how consumer attitudes shift as awareness increases. While many users accept personalization when framed as beneficial or convenient, this acceptance erodes when the scale, opacity, fairness and commercial purpose of data collection become salient. Notably, Kozyreva et al. find widespread discomfort with algorithmic personalization across different national contexts, suggesting that skepticism is more than merely a product of local regulation or culture. This reinforces the idea that consumers' apparent willingness to trade data for services often rests on incomplete understanding rather than genuine endorsement.

Grande et al.'s (2022) work adds another layer of nuance by showing that willingness to share data is highly purpose-specific. Consumers distinguish sharply between socially beneficial uses, such as public health and research, and commercial exploitation. Trust in the data recipient plays a decisive role, with universities and health institutions viewed far more favorably than technology companies. This again suggests that consumer preferences are relational and institutional, not simply transactional.

Across all five studies, a common theme emerges: agency cannot be meaningfully grounded in digital illiteracy. Consumers are routinely asked to make complex trade-offs in environments characterized by opaque data flows and processing, involving a plethora of layered contracts and asymmetric power. Under such conditions, expecting individuals to express stable preferences for their own welfare through consent or payment is unrealistic. Rather than revealing what consumers truly want, current digital markets often expose the limits of choice in the presence of complexity and information asymmetry. This fundamentally challenges regulatory approaches, particularly whether protecting consumer agency requires moving beyond consent-based models toward stronger structural safeguards and defaults that do not presume high levels of technical understanding on the side of the consumer/user.

The empirical evidence suggests that the structural conditions for meaningful choice are absent. Regulatory approaches based on individual consent fail because the market architecture within which consent is obtained is fundamentally distorted. This shifts the regulatory question from "How do we better inform consumers?" to "How do we make platform business models intelligible to those who can hold them accountable?".

4. From consumer transparency to enforcement transparency

So far in this paper, we have explored the dilemma of empowering consumers through consent in an environment that exceeds the technological literacy of ordinary users. With its rapid pace and increasing complexity, the digital space makes it impossible for consumers to rely on information to give genuinely free consent. As pessimistic as this may sound, consumers simply face too many structural constraints and too many cognitive limitations to plausibly claim meaningful individual agency, and advertisers use information to their advantage. There may be some consumers who are more

technologically literate than others, but this does not take away from the fact that consumers are generally bombarded with overwhelming volumes of information and with levels of technological - and at times legal - complexity that even experts struggle to fully grasp. Indeed, this complexity has itself become an object of scientific inquiry.

4.1. The dilemma of transparency and consent

Obtaining consent in this environment must be understood through the lens of an Akerlof "market for lemons" (1970). It constitutes a classic case of adverse selection driven by asymmetric information: the less well-informed party fails to recognize its disadvantage under data protection (and often contract) law, with the result that higher-quality offers cannot prevail. This dynamic produces market failure, triggering a "race to the bottom" toward increasingly deficient consent conditions.[6]

This has been an old problem in the field of data protection information obligations (Art. 12 et seq. GDPR) – the *transparency conflict* between comprehensibility and completeness – the complexity of data processing benefits the provider side. This is not limited to the fact that extensive "privacy centers", CMPs, etc., discourage users from gaining a genuine understanding of how their data is processed.7 The problem runs deeper: even the most comprehensible description of the actual technical processes would, in data-financed services, be too extensive or overwhelming for data subjects and would not enable a genuinely freely given consent. While this is only one factor that has contributed to the permissive culture of consent described above, it carries particular weight and marks the decisive interface where industrial personal data processing collides with the political orientation of the GDPR, which aims to place limits on commercial personal data processing.

However, insufficient information for data subjects does not seem to be the central problem in industrial data processing. As the rather negative attitude of users towards pay-or-okay models demonstrates, a significant part of the conflict lies in financing open but costly business models such as news, weather forecasts, or entertainment and communication services.

As has been shown, users generally value privacy and are not categorically opposed to paying. It is, however, understandable that they are unwilling to enter into a paid subscription with every news, weather, or social media service each for a couple of Euros per month. The alternative of micropayments has failed to gain widespread adoption to replace the "ok" model, largely due to their high actual and mental transaction costs – paying small amounts (e.g. €0.01 to access a weather forecast) directly to individual providers is disproportionately burdensome (Ali, Clarke, and McCorry 2017).

Faced with users' low willingness to pay, providers respond with far-reaching, sometimes aggressive data processing, which users in turn - partly consciously, partly unconsciously - tolerate. Said transparency conflict is therefore better understood as a downstream consequence of a more fundamental cause, namely the replacement of monetary payments with an advertising-based, data-intensive form of financing.

This is precisely the gap exploited by the advertising industry, which offers website operators very small amounts for each "impression" of an advertisement. For standard display advertising, these amounts may reach prices around USD 0.7 per 1,000 ad impressions,[8] i.e. approximately USD 0.0007 per impression. The price of not being tracked exceeds these advertising revenues: users must not only compensate for the lost advertising income but also pay an additional premium.[9]

Returning to the transparency problem, the persistent focus on transparency as a tool for consumer decision-making rests on an assumption that is increasingly untenable in digital markets: that individuals can meaningfully process complex information and translate it into informed choices. As discussed throughout the paper, consumers face a multitude of unclear contracts, opaque data practices that go beyond their comprehension, and in general – technologically sophisticated business models that even (legal) experts struggle to fully understand. In such conditions, information duties leading to transparency for consumers only shift responsibility from firms to users, while leaving underlying power asymmetries untouched.

Consumer transparency reform alone cannot resolve what is, at its core, an economic conflict. The

6 See for instance Maximilian Becker, 'Ein Recht auf datenerhebungsfreie Produkte' (2017) 72 *JuristenZeitung* 170, 174; Maximilian Becker, 'Die DSGVO als Marktverhaltensregel (§ 3a UWG) – Eine Chance für europäische KI-Anbieter?' (2025) 71 Wettbewerb in Recht und Praxis 1522, [48].

7 See for example Skop and Burkhardt (forthcoming) 'All the News That's Fit to Track', *Computational Culture* (showing, inter alia, the difficulties involved in retrieving the very extensive privacy manager information from common CMPs used by digital news publishers).

8 See for instance Rene Laub, Klaus M Miller and Bernd Skiera, 'The Economic Value of User Tracking for Publishers' (SSRN Working Paper No 4251233, 14 April 2024) 16 https://doi.org/10.2139/ssrn.4251233; Łukasz Olejnik, Minh-Dung Tran and Claude Castelluccia, Selling Off Privacy at Auction (NDSS Symposium 2014, *Internet Society* 22 Feb 2014) https://www.ndss-symposium.org/ndss2014/ndss-2014-programme/selling-privacy-auction.

9 For more details, see Timo Müller-Tribbensee, Klaus M. Miller and Bernd Skiera, 'Paying for Privacy: Pay-or-Tracking Walls' (arXiv Working Paper arXiv:2403.03610, 6 March 2024) 4 https://arxiv.org/abs/2403.03610 („We observe that the price for not being tracked exceeds the advertising revenue that publishers generate from users who consent to being tracked, indicating that users seeking privacy have to pay a premium.").

question is therefore not how to improve disclosures, but how to make personal data industries legible to those capable of acting on them.

4.2. Regulatory proposal: Business-model transparency aimed at enforcement authorities

Since micropayments do not currently offer a viable way out, and no fundamental solution to the dilemma between data protection and the personal data economy is in sight, a short-term, practically implementable improvement is proposed here: A shift from consumer-facing transparency toward business-model transparency aimed at enforcement authorities (Goanta and Spanakis 2022). Rather than asking individuals to evaluate privacy policies and consent banners including hundreds of advertising "partners" in making their decisions, the European legislator should require platforms to make their data processing as well as data flows, monetization strategies, algorithmic incentives, and contractual dependencies legible to those tasked with oversight, so they can verify compliance with regulatory regimes in a more in-depth manner than a consumer ever could. This would allow enforcement bodies to act ex-ante and identify practices that are harmful, misleading, or exploitative. This approach treats transparency not as a *substitute* for regulation, but as an *input* to it. By exposing how value is extracted and risks are distributed within digital business models, transparency becomes a governance tool rather than a cognitive burden on consumers. In complex digital ecosystems, effective accountability depends less on informed individual choice and more on institutional capacity to monitor harmful practices at their source.

This shift toward business-model transparency aligns closely with the logic of the DSA, which deliberately moves beyond the idea that transparency primarily serves individual consumer choice (Leerssen 2023). While the DSA still contains user-facing disclosure obligations, its most consequential transparency duties are explicitly designed to enable regulatory oversight and enforcement rather than to improve day-to-day consumer decision-making. This oversight does not only regard the authorities tasked with the implementation and enforcement of the DSA (e.g. Digital Services Coordinators at national level), but even civil society at large. It thus serves not only a role in public enforcement, but also in private enforcement.[10]

For example, the DSA's layered obligations for Very Large Online Platforms (VLOPs) require platforms to disclose information about their systemic risks, including risks related to the dissemination of illegal content, fundamental rights (including the principle of consumer protection), and overall democracy harms such as election interference (Eder 2024; Goanta et al. 2025). These risk assessments, together with mandatory risk mitigation measures and their subsequent audits as per Article 37 DSA are not intended to be digested by ordinary users, but rather by the public bodies tasked with the enforcement of the DSA. Similarly, the DSA's provisions on algorithmic transparency and advertising repositories (Articles 26 and 27 DSA) reflect this enforcement-oriented approach. While users receive some explanatory rights, the deeper value lies in enabling Digital Services Coordinators, the Commission, and vetted researchers to scrutinize platforms and their practices at scale. Transparency here functions as a diagnostic instrument, allowing authorities to detect patterns of abuse that would remain invisible at the level of individual consent. Such provisions equip regulators with insight into how platforms' business models (including monetization strategies) and algorithmic infrastructures contribute to harmful outcomes. This information can be further triangulated and used in national or European-level investigations into DSA compliance.

In this sense, the DSA is a great example of how a structural understanding of transparency can be operationalized: not as a means of empowering technologically overburdened users, but as a regulatory infrastructure that makes complex platform business models legible to those capable of enforcing compliance and addressing systemic harm.

In the light of these implications, we propose said increase in enforcement transparency (disclosure of data collection and processing, algorithms, networks, partners). This could serve to make processing practices transparent to experts, as the Meta proceedings before the German Federal Cartel Office have already demonstrated.[11] This first step would not yet alter industrial personal data processing itself. The transparency thus created, however, could form the basis for new regulatory approaches or a political debate in a second step – the aim is not to inform data subjects indirectly via experts, but to enable new regulation. Making data processing transparent to professionals could, on the one hand, help uncover problematic practices. This is meant as a complementary, not an alternative, form of transparency. Data subjects, for instance, should be able to download all relevant information on personal data processing by websites/platforms in a comprehensive, structured, commonly used and machine-readable format, in addition to the information obligations under

10 See Regional Court Berlin II (LG Berlin II), Judgment of May 13, 2025 – 41 O 140/25 eV, ZUM-RD 2025, 439 (holding that Art. 40(12) DSA establishes a directly enforceable statutory data-access obligation [for private plaintiffs]; refusal of access may constitute actionable harm, giving rise to claims for injunctive relief and damages under Art. 54 DSA in conjunction with § 823(2) BGB); see also Higher Regional Court of Bamberg (OLG Bamberg), Judgment of February 5, 2025 – 3 UKl 11/24e, GRUR-RS 2025, 6221 (granting an injunction sought by a consumer protection organization against a ticket reseller for violations of Art. 25(1) and (3) DSA due to the use of dark patterns).

11 See Bundeskartellamt, Facebook Decision (n 3), para. 629 et seq. and passim.

Art. 12 et seq. GDPR. The wording is partly taken from Art. 3(1) of the Data Act, a legislative instrument closely related to the GDPR, which likewise targets the industrial-scale disclosure of data contemplated here. This would constitute a decisive complement to Art. 12(1) GDPR, which relies on linguistic explanations of data processing and can easily be exploited through the kind of information overload described above—by means of sprawling texts and layered submenus that further exacerbate the information asymmetry at issue. A right of this nature would facilitate[12] not only enforcement by authorities but also enforcement by associations and competitors.[13]

On the other hand, it could also highlight legitimate processing needs of the industry and provide a foundation for an appropriate financing of the open internet. From a legal-policy perspective, professional transparency of complex data processing could foster a better understanding of a sector that is regulated in principle but in practice protected by its complexity. This would be disadvantageous for many providers, as unlawful data processing practices would increasingly be uncovered. But it would benefit law-abiding companies by removing competitive disadvantages vis-à-vis violators. Professional transparency could contribute to the creation of a level playing field, particularly for European providers competing with US providers.[14]

5. Results

Data protection in personal data markets such as the advertising market examined here requires systemic change rather than better privacy information. The DSA illustrates how transparency can function as an effective regulatory instrument.

The reviewed studies show that consumer preferences in digital markets are unstable, inasmuch as they are context-dependent. At the same time, preferences are strongly shaped by framing, trust, but also by institutional design. Consumers tend to demand significantly more compensation to relinquish their privacy than they are willing to pay to protect it. Acceptance of personalization is often based on an incomplete understanding of data processing and erodes once the scale and commercial purpose of data use become salient. Moreover, willingness to share data is highly purpose- and trust-dependent: socially beneficial uses are evaluated very differently from commercial exploitation.

Consumers' willingness to pay – whether through subscriptions or micropayments – is generally low. Technological illiteracy and information overload lead users to disregard privacy notices; even simplified versions fail to meaningfully alter behavior.

While the GDPR assigns high value to the free will of data subjects, the consent-based model rests on assumptions that break down under conditions of asymmetric information. In Akerlof's "market for lemons," users are unable to assess privacy quality, enabling platforms to deploy "pay-or-okay" models (as exemplified by Meta) that formally offer choice but are structurally coercive. Even complete information is of little help when it is too complex to process. Users ultimately click "accept" out of resignation.

Regulation must address this problem through systemic solutions that complement individual responsibility. Rather than consumer-facing transparency in the form of ineffective notice texts, what is needed is enforcement-oriented transparency. The DSA already requires platforms to disclose algorithms and data flows to supervisory authorities (see Arts. 37 and 40 DSA), enabling the identification of harmful practices ex ante and relieving users of the burden of oversight.

Building on this approach, we propose a regulatory concept of business-model transparency in data and consumer protection law, that can also inform platform liability regulation. In addition to the information obligations under Articles 12 et seq. GDPR, data subjects should be able to download all relevant information on personal data processing by websites and platforms in a comprehensive, structured, commonly used, and machine-readable format.

This would not expand companies' data processing powers but would increase transparency in industrial personal data processing by shifting from "clear and plain language" explanations (Art. 12(1) GDPR) to the provision of data in a "commonly used and machine-readable format," drawing on Article 3(1) of the Data Act, and equivalent conditions in the DSA. Designed as an individual right of data subjects, such access would also be available to competitors and civil society organizations. Combined with the Court of Justice's recognition that Member States may provide additional avenues of enforcement (for example through unfair competition law),[15] this approach would significantly strengthen the practical enforcement of data protection law.

12 See Skop and Burkhardt (forthcoming) 'All the News That's Fit to Track', *Computational Culture* (a downloadable version of the privacy manager information, e.g. as a JSON file, would facilitate access to the information contained in CMPs as opposed to thousands of clicks).

13 See Maximilian Becker, ‚Die DSGVO als Marktverhaltensregel (§ 3a UWG) – Eine Chance für europäische KI-Anbieter?' (2025) 71 *Wettbewerb in Recht und Praxis* 1522, [11]–[15].

14 See Becker (n 13).

15 Case C-21/23, Lindenapotheke, ECLI:EU:C:2024:846.

Bibliography

Akerlof, George A. 1970. 'The Market for "Lemons": Quality Uncertainty and the Market Mechanism'. *The Quarterly Journal of Economics* 84 (3): 488–500. https://doi.org/10.2307/1879431.

Ali, Syed Taha, Dylan Clarke, and Patrick McCorry. 2017. 'The Nuts and Bolts of Micropayments: A Survey'. arXiv:1710.02964. Preprint, arXiv, October 9. https://doi.org/10.48550/arXiv.1710.02964.

Annabell, Taylor, Sophie Bishop, and Catalina Goanta. 2025. *You and TikTok Are, and Will Remain at All Times, Independent Contractors*. 23 July 2025. https://doi.org/10.14763/2025.3.2014.

Azhar, Azeem. 2022. *Exponential: Order and Chaos in an Age of Accelerating Technology*. London: Penguin Books.

Bamberger, Kenneth A., Serge Egelman, Catherine Han, Amit Elazari Bar On, and Irwin Reyes. 2020. 'Can You Pay for Privacy? Consumer Expectations and the Behavior of Free and Paid Apps'. *Berkeley Technology Law Journal* 35 (1): 327–66. https://doi.org/10.15779/Z38XP6V40J.

Becker, Maximilian. 2017. 'Ein Recht auf datenerhebungsfreie Produkte'. *JuristenZeitung* 72 (4): 170–181. https://doi.org/10.1628/002268817X14845656323252.

Becker, Maximilian. 2025. 'Die DSGVO als Marktverhaltensregel (§ 3a UWG) – Eine Chance für europäische KI-Anbieter?'. *Wettbewerb in Recht und Praxis* 71 (12): 1522–1532.

Bekos, Paschalis, Panagiotis Papadopoulos, Nicolas Kourtellis, and Michalis Polychronakis. 2025. 'PIIxel Leaks: Passive Identification of Personally Identifiable Information Leakage through Meta Pixel'. *Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security* (New York, NY, USA), CCS '25, 22 November 2025, 4229–43. https://doi.org/10.1145/3719027.3765113.

Ben-Shahar, Omri, and Adam Chilton. 2016. 'Simplification of Privacy Disclosures: An Experimental Test'. *The Journal of Legal Studies* 45 (S2): S41–67. https://doi.org/10.1086/688405.

'Cambridge Analytica: il Garante privacy multa Facebook per 1 milione di euro'. n.d. Accessed 30 November 2022. https://www.garanteprivacy.it:443/home/docweb/-/docweb-display/docweb/9121352.

D'Amico, Alessia, Dionysios Pelekis, Cristiana Teixeira Santos, and Bram Duivenvoorde. 2024. 'Meta's Pay-or-Okay Model: An Analysis under EU Data Protection, Consumer and Competition Law'. *Technology and Regulation* 2024 (September 2024): 254–72. https://doi.org/10.71265/tkk29041.

Eder, Niklas. 2024. 'Making Systemic Risk Assessments Work: How the DSA Creates a Virtuous Loop to Address the Societal Harms of Content Moderation'. *German Law Journal* 25 (7): 1197–218. https://doi.org/10.1017/glj.2024.24.

El Fraihi, Asmaa, Nardjes Amieur, Walter Rudametkin, and Oana Goga. 2024. 'Client-Side and Server-Side Tracking on Meta: Effectiveness and Accuracy'. *Proceedings on Privacy Enhancing Technologies* (Bristol, United Kingdom) 2024 (3): 431–45. https://doi.org/10.56553/popets-2024-0086.

'Facebook Fined €1M over Cambridge Analytica Scandal'. 2019. *POLITICO*, 28 June 2019. https://www.politico.eu/article/facebook-fined-cambridge-analytica/.

Frick, Sarah J., Deborah Fletcher, and Austin C. Smith. 2023. 'Pirate and Chill: The Effect of Netflix on Illegal Streaming'. *Journal of Economic Behavior & Organization* 209 (May 2023): 334–47. https://doi.org/10.1016/j.jebo.2023.03.013.

Goanta, Catalina, and Stephan Mulders. 2019. '"Move Fast and Break Things": Unfair Commercial Practices and Consent on Social Media'. *Journal of European Consumer and Market Law* 8 (4). https://kluwerlawonline.com/journalarticle/Journal+of+European+Consumer+and+Market+Law/8.4/EuCML2019026.

Goanta, Catalina, and Jerry Spanakis. 2022. 'Discussing the Legitimacy of Digital Market Surveillance'. *Stanford Computational Antitrust* 2 (2022): 44–55.

Goanta, Catalina, Savvas Zannettou, Rishabh Kaushal, Jacob van de Kerkhof, Thales Bertaglia, Taylor Annabell, Haoyang Gui, Gerasimos Spanakis, and Adriana Iamnitchi. 2025. 'The Great Data Standoff: Researchers vs. Platforms Under the Digital Services Act'. arXiv:2505.01122. Preprint, arXiv, May 2. https://doi.org/10.48550/arXiv.2505.01122.

Grande, David, Nandita Mitra, Raghuram Iyengar, Raina M. Merchant, David A. Asch, Meghana Sharma, and Carolyn C. Cannuscio. 2022. 'Consumer Willingness to Share Personal Digital Information for Health-Related Uses'. *JAMA Network Open* 5 (1): e2144787. https://doi.org/10.1001/jamanetworkopen.2021.44787.

Greenstein, Shane. 2000. 'Commercialization of the Internet: The Interaction of Public Policy and Private Choices or Why Introducing the Market Worked so Well'. *Innovation Policy and the Economy* 1 (January 2000): 151–86. https://doi.org/10.1086/ipe.1.25056144.

'Help Center'. n.d. Accessed 14 December 2025. https://help.instagram.com/923021729404927/?helpref=related_articles.

Kozyreva, Anastasia, Philipp Lorenz-Spreen, Ralph Hertwig, Stephan Lewandowsky, and Stefan M. Herzog. 2021. 'Public Attitudes towards Algorithmic Personalization and Use of Personal Data Online: Evidence from Germany, Great Britain, and the United States'. *Humanities and Social Sciences Communications* 8 (1): 117. https://doi.org/10.1057/s41599-021-00787-w.

Laub, Rene, Klaus M. Miller, and Bernd Skiera. 2024. 'The Economic Value of User Tracking for Publishers'. SSRN Working Paper No. 4251233, April 14. https://doi.org/10.2139/ssrn.4251233.. SSRN Working Paper No. 4251233, April 14. https://doi.org/10.2139/ssrn.4251233.

Leerssen, Paddy. 2023. 'An End to Shadow Banning? Transparency Rights in the Digital Services Act between Content Moderation and Curation'. *Computer Law & Security Review* 48 (April 2023): 105790. https://doi.org/10.1016/j.clsr.2023.105790.

Leiner, Barry M., Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolff. 2009. 'A Brief History of the Internet'. *ACM SIGCOMM Computer Communication Review* 39 (5): 22–31. https://doi.org/10.1145/1629607.1629613.

Leszczynska, M., and D. Baltag. 2024. '"Can I Have It Non-Personalised?" An Empirical Investigation of Consumer Willingness to Share Data for Personalized Services and Ads'. *Journal of Consumer Policy* 47 (3): 345–72. https://doi.org/10.1007/s10603-024-09568-9.

Lukasik, Stephen. 2011. 'Why the Arpanet Was Built'. *IEEE Annals of the History of Computing* 33 (3): 4–21. https://doi.org/10.1109/MAHC.2010.11.

Mahadevan, B. 2000. 'Business Models for Internet-Based E-Commerce: An Anatomy'. *California Management Review* 42 (4): 55–69. https://doi.org/10.2307/41166053.

Moir, Aidan. 2024. 'Attempts to Ban TikTok Reveal the Hypocrisy of Politicians Already Struggling to Relate to Voters'. The Conver-

sation, March 15. http://theconversation.com/attempts-to-ban-tiktok-reveal-the-hypocrisy-of-politicians-already-struggling-to-relate-to-voters-225870.

Müller-Tribbensee, Timo, Klaus M. Miller, and Bernd Skiera. 2024. 'Paying for Privacy: Pay-or-Tracking Walls'. arXiv:2403.03610, March 6. https://doi.org/10.48550/arXiv.2403.03610.

Olejnik, Łukasz, Minh-Dung Tran, and Claude Castelluccia. 2014. 'Selling Off Privacy at Auction'. *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, February 22. https://www.ndss-symposium.org/ndss2014/ndss-2014-programme/selling-privacy-auction.

Packard, Noel. 2023. 'INTERNET Prehistory: ARPANET Chronology'. *Cogent Social Sciences* 9 (2): 2245237. https://doi.org/10.1080/23311886.2023.2245237.

Paloque-Bergès, Camille, and Valérie Schafer. 2019. 'Arpanet (1969–2019)'. *Internet Histories* 3 (1): 1–14. https://doi.org/10.1080/24701475.2018.1560921.

Roth, Emma. 2025. '"Goodbye to My Chinese Spy" Might Be the Last Great TikTok Trend'. The Verge, January 13. https://www.theverge.com/2025/1/13/24343063/tiktok-ban-goodbye-chinese-spy-trend.

Skop, Yarden, and Marcus Burkhardt. Forthcoming. 'All the News That's Fit to Track: Encountering the Tracking Ecosystem on News Publishers Websites Through Personal Data Requests'. *Computational Culture*.

'Statement on EDPB "Pay or Okay" Opinion'. n.d. Accessed 28 May 2025. https://noyb.eu/en/statement-edpb-pay-or-okay-opinion.

Vlist, Fernando N. van der, Anne Helmond, Marcus Burkhardt, and Tatjana Seitz. 2022. 'API Governance: The Case of Facebook's Evolution'. *Social Media + Society* 8 (2): 205630512210862. https://doi.org/10.1177/20563051221086228.

Wernerfelt, Nils, Anna Tuchman, Bradley T. Shapiro, and Robert Moakler. 2025. 'Estimating the Value of Offsite Tracking Data to Advertisers: Evidence from Meta'. *Marketing Science* 44 (2): 268–86. https://doi.org/10.1287/mksc.2023.0274.

'What Is RedNote, the Chinese App That US "TikTok Refugees" Are Flocking to? | CNN Business'. n.d. Accessed 17 February 2025. https://edition.cnn.com/2025/01/14/tech/rednote-china-popularity-us-tiktok-ban-intl-hnk/index.html.

Winegar, A. G., and C. R. Sunstein. 2019. 'How Much Is Data Privacy Worth? A Preliminary Investigation'. *Journal of Consumer Policy* 42 (3): 425–40. https://doi.org/10.1007/s10603-019-09419-y.

Xu, Jian. 2025. 'US "TikTok Refugees" Are Fleeing to Chinese App RedNote. It's a New Phase of the Digital Cold War'. The Conversation, January 16. http://theconversation.com/us-tiktok-refugees-are-fleeing-to-chinese-app-rednote-its-a-new-phase-of-the-digital-cold-war-247342.

Authors

Maximilian Becker is a Professor at the Institute of Media and Communication Law at the University of Siegen, where he holds the Chair of Civil Law, Intellectual Property Law, and Media Law. Until 2021, he was a Professor at the Institute of Legal Informatics at Leibniz University Hannover, where he held the Chair of Data Protection Law and IT Law. His research focuses on intellectual property law, data law (including data protection law and data economy law), AI law, and civil law. He co-leads the project "The Industry of Personal Data" at the Collaborative Research Centre 1187 Media of Cooperation.

Catalina Goanta is an associate professor in consumer law and technology at Utrecht University and Mercator Fellow at the Collaborative Research Centre 1187 Media of Cooperation. She is also the Principal Investigator of an ERC Starting Grant (HUMANads) focus on fairness in social media monetization, and is co-leader of the Data and AI research platform at Utrecht University's law faculty.