International Center for Law & Economics

# The Privacy-Antitrust Curse: Insights from GDPR Application in EU Competition Law

*Giuseppe Colangelo*

ICLE White Paper 2023-10-12

laweconcenter.org | icle@laweconcenter.org
1104 NW 15th Ave. Ste 300 Portland, OR 97209

@laweconcenter
503.770.0076

# The Privacy-Antitrust Curse: Insights from GDPR Application in EU Competition Law

*Giuseppe Colangelo*[*]

## Abstract

The integrated approach that many competition and privacy regulators have endorsed for oversight of the major online platforms, whose business models rely on collecting and processing large troves of personal data, has often been justified on grounds that competition and data protection are complementary ends. In this respect, Europe represents a testing ground for evaluating how privacy breaches may inform antitrust investigations. Indeed, the European Union's General Data Protection Regulation (GDPR) and the recent German antitrust decision concerning Facebook may be considered polestars for this emerging regulatory approach that links market power and data power. This paper tests the degree to which such an approach is viable in concrete terms by analyzing how the European Commission and national competition authorities have applied data-protection rules and principles in antitrust proceedings. Notably, the paper aims to demonstrate the fallacy of characterizing the relationship between privacy and antitrust in terms of synergy and complementarity. Further, the paper maintains that the principles the European Court of Justice recently affirmed in its *Meta* decision do not appear to address the issue conclusively. The tension between these areas of law is illustrated by allegations raised in the numerous Apple ATT investigations concerning the strategic use of privacy as a business justification to pursue anticompetitive advantages. Rather than strengthening antitrust enforcement against gatekeepers and their data strategies, the inclusion of privacy harms in antitrust proceedings may turn out to be a potential curse for competition authorities, as it allows firms opportunities for regulatory gaming that can serve to undermine antitrust enforcement.

[*] Giuseppe Colangelo is the Jean Monnet Professor of EU Innovation Policy and an associate professor of law and economics at University of Basilicata; a Transatlantic Technology Law Forum (TTLF) Fellow at Stanford Law School and the University of Vienna; Academic and an academic affiliate of the International Center for Law & Economics (ICLE). ICLE has received financial support from numerous companies, foundations, and individuals, including firms with interests both supportive of and in opposition to the ideas expressed in this and other ICLE-supported works. Unless otherwise noted, all ICLE support is in the form of unrestricted, general support. The ideas expressed here are the authors' own and do not necessarily reflect the views of ICLE's advisors, affiliates, or supporters.

## I. Introduction

A significant share of the past decade's academic literature on the role of data in digital markets has focused on the intersection of what had been previously thought of as the separate domains of privacy and antitrust. Given that data serves as a significant input for many of the major online platforms' services and products, digital firms are eager to collect and process as much of it as possible. Such firms also use data-sharing agreements to obtain further data (*i.e.*, information collected and provided by external suppliers) in order to improve their products and services. This is particularly true for those platforms whose business models rely on monetizing consumer information by selling targeted advertising and personalized sponsored content. In a market where platforms' data-acquisition strategies are driven by the objective of granting sellers preferential access to consumer attention, personal data can represent an especially valuable portion of platforms' information assets.[1] Moreover, given the social dimension of personal data, one user's choice to share personal information with an online platform may generate externalities on other non-disclosing users (or non-users) by revealing information about them. Recent advances in machine learning may magnify the extent of these externalities, and raise questions about the effectiveness of data-protection regulations more generally.[2]

These dynamics have moved policymakers to take a greater interest in the degree to which data-accumulation strategies undermine individual privacy and entrench platforms' market power. Some contend that the peculiar features of digital markets and the potential adverse uses of data in the digital economy require a regulatory approach that integrates privacy into antitrust enforcement and ensures close cooperation between antitrust authorities and data-protection regulators.[3]

---

[1] *See* Jacques Crémer, Yves-Alexander de Montjoye, & Heike Schweitzer, *Competition Policy for the Digital Era*, (2019) Report for the European Commission, 4, *available at* https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf (referring to the possibility that a dominant platform could have incentives to sell "monopoly positions" to sellers by showing buyers alternatives that do not meet their needs).

[2] *See* Alessandro Bonatti, *The Platform Dimension of Digital Privacy*, forthcoming in THE ECONOMICS OF PRIVACY, (AVI GOLDFARD & CATHERINE TUCKER, eds.), University of Chicago Press; Daron Acemoglu, Ali Makhdoumi, Azarakhsh Malekian, & Asu Ozdaglar, *Too Much Data: Prices and Inefficiencies in Data Markets*, 14 AM ECON J MICROECON 218 (2022); Shota Ichihashi, *The Economics of Data Externalities*, 196 J. ECON. THEORY 105316 (2021); Omri Ben-Shahar, *Data Pollution*, 11 J. LEG. ANAL. 104 (2019); Jay Pil Choi, Doh-Shin Jeon, & Byung-Cheol Kim, *Privacy and Personal Data Collection with Information Externalities*, 173 J. PUBLIC ECON. 113 (2019); *see also* Jeanine Miklós-Thal, Avi Goldfarb, Avery M. Haviv, & Catherine Tucker, *Digital Hermits*, NBER Working Paper No. 30920 (2023), (arguing that, as advances in machine learning allow firms to infer more accurately sensitive data from data that appears otherwise innocuous, users' data-sharing decisions polarize between a group of users choosing to share no data and another group choosing to share all their data (sensitive or not sensitive)).

[3] *See, e.g.*, *Competition and Data Protection in Digital Markets: A Joint Statement Between the CMA and the ICO*, UK COMPETITION AND MARKETS AUTHORITY AND INFORMATION COMMISSIONER'S OFFICE, (2021) 5, https://www.gov.uk/government/publications/cma-ico-joint-statement-on-competition-and-data-protection-law [hereinafter "CMA-ICO Joint Statement"]; *Privacy and Competitiveness in the Age of Big Data: The Interplay Between Data Protection, Competition Law and Consumer Protection in the Digital Economy*, EUROPEAN DATA PROTECTION SUPERVISOR (2014) https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-and-competitiveness-age-big-data_en.

According to this account, as network effects strengthen online firms' market power, it becomes progressively more difficult to structure incentives for firms to compete on offering privacy-friendly products and services.[4] Conversely, these advocates claim, more competition in digital markets would lead to more privacy.[5]

Particular scrutiny is directed toward advertising-funded platforms that offer free services to attract users and thereby feed users' data to the other side of the platform (*i.e.*, advertisers), whose willingness to pay is strictly dependent on being able to deliver effective marketing through granular targeting or personalization. For their part, however, end users may not be aware of the value of their own data or may be induced to disclose private information. This could happen because users are attracted by zero-price services' offers or, given the lack of available and comparable alternatives, in order to remain connected to their social, family, or work networks, users may feel compelled to accept take-it-or-leave-it terms that include the unwanted collection and use of their data.[6]

Some suggest that privacy should be included in antitrust assessments because suboptimal privacy offerings may be the result of anti-competitive behavior leading to decreased quality of products and services.[7] In this sense, privacy would represent a particularly significant factor to be taken into account in the merger-review process, as market concentration

---

[4] *See, e.g.*, *Investigation of Competition in Digital Markets', Majority Staff Reports and Recommendations*, U.S. HOUSE ENERGY AND COMMERCE SUBCOMMITTEE ON ANTITRUST, COMMERCIAL, AND ADMINISTRATIVE LAW (2020), 28, *available at* https://www.govinfo.gov/content/pkg/CPRT-117HPRT47832/pdf/CPRT-117HPRT47832.pdf [hereinafter, "Antitrust Subcommittee Report"]; Frank Pasquale, *Privacy, Antitrust, and Power,* 20 GEORGE MASON LAW REV. 1009 (2013); Pamela J. Harbour & Tara I. Koslov, *Section 2 in a Web 2.0 World: An Expanded Vision of Relevant Product Markets*, 76 ANTITRUST LAW J. 769 (2010).

[5] *See, e.g.*, Antitrust Subcommittee Report, *supra* note 4, 39, citing Howard A. Shelanski, *Information, Innovation, and Competition Policy for the Internet*, 161 U. PA. L. REV. 1663 (2013), to argue that "[t]he persistent collection and misuse of consumer data is an indicator of market power in the digital economy"; European Data Protection Supervisor, *supra* note 3, 35, stating that, where there are a limited number of operators or when one operator is dominant, "the concept of consent becomes more and more illusory;" *see also*, *Online Platforms and Digital Advertising*, UK COMPETITION AND MARKETS AUTHORITY (2020) para. 6.26, *available at* https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf, stating that "[i]n a more competitive market, we would expect that it would be clear to consumers what data is collected about them and how it is used and, crucially, the consumer would have more control. We would then expect platforms to compete with one another to persuade consumers of the benefits of sharing their data or adopt different business models for more privacy-conscious consumers." However, *see also* James C. Cooper & John M. Yun, *Antitrust & Privacy: It's Complicated,* J. LAW TECHNOL. POLICY 343 (2022), finding no systematic relationship between privacy ratings and market concentration.

[6] *See, e.g.*, *Report on Social Media Services,* AUSTRALIAN COMPETITION & CONSUMER COMMISSION (2023), 128, https://www.accc.gov.au/media-release/accc-report-on-social-media-reinforces-the-need-for-more-protections-for-consumers-and-small-business; Rebecca Kelly Slaughter, *The FTC's Approach to Consumer Privacy*, FEDERAL TRADE COMMISSION (2019) 3, *available at* https://www.ftc.gov/system/files/documents/public_statements/1513009/slaughter_remarks_at_ftc_approach_to_consumer_privacy_hearing_4-10-19.pdf.

[7] Antitrust Subcommittee Report, *supra* note 4, 28; Maurice E. Stucke & Ariel Ezrachi, *When Competition Fails to Optimise Quality: A Look at Search Engines*, 18 YALE J. LAW TECHNOL. 70 (2016).

among companies that hold big data could further expand the merging firms' tools to profile consumers and potentially invade their privacy.[8]

Finally, some advocates propose commingling antitrust and privacy regulation as part of a broader agenda to realign competition policy away from pure efficiency-oriented antitrust enforcement and instead toward a holistic approach that combines competition law with other fields of law, in order to take account of a broader swath of social interests.[9] In essence, privacy and antitrust would each help to cover the other's purported Achilles heel.[10] While end users' privacy interests would become relevant in investigating data-accumulation strategies that antitrust might otherwise fail to tackle, antitrust authorities would be more effective in ensuring data protection.[11]

Against the integrationist perspective, however, some scholars warn of risks that would attend transforming privacy infringements into *per se* antitrust violations.[12] Indeed, competition law and privacy regulation pursue different aims and deploy different tools. While privacy is not irrelevant to competition law and may constitute an important component of nonprice competition, the goals of competition and privacy are often at odds. Pushing these regulatory regimes to converge threatens to confuse, rather than strengthen, the enforcement of either.[13]

---

[8] Pamela J. Harbour, *Dissenting Statement in the Matter of Google/DoubleClick,* FEDERAL TRADE COMMISSION (2007), 4, *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/statement-matter-google/doubleclick/071220harbour_0.pdf.

[9] For a critical perspective, *see* Giuseppe Colangelo, *In Fairness We (Should Not) Trust: The Duplicity of the EU Competition Policy Mantra in Digital Markets,* ANTITRUST BULLETIN (forthcoming).

[10] *See* Cristina Caffarra & Johnny Ryan, *Why Privacy Experts Need a Place at the Antitrust Table*, PROMARKET (2021) https://www.promarket.org/2021/07/28/privacy-experts-antitrust-data-harms-digital-platforms, arguing that "[t]here is a market power crisis and a privacy crisis, and they compound each other."

[11] *See, e.g.*, Wolfgang Kerber & Karsten K. Zolna, *The German Facebook Case: The Law and Economics of the Relationship Between Competition and Data Protection Law*, 54 EUR. J. LAW ECON. 217 (2022), arguing that digital markets exhibit two types of market failure (*i.e.*, competition problems on the one hand, and information and behavioral problems on the other) and suggesting that the effectiveness of enforcement should also be an important criterion for determining which policy should deal with a case if both laws can be applied. Accordingly, if data-protection law is uncapable of dealing effectively with privacy issues and competition law appears better able to overcome this challenge, then the competition authority should step in as the lead enforcer. On the enforcement failure of old and new data-protection regimes, see Filippo Lancieri, *Narrowing Data Protection's Enforcement Gap*, 74 MAINE LAW REV. 15 (2022).

[12] For an overview of various theories that have emerged in the literature, see Erika M. Douglas, *The New Antitrust/Data Privacy Law Interface*, YALE L.J. F. 647 (2021); Giuseppe Colangelo & Mariateresa Maggiolino, *Data Protection in Attention Markets: Protecting Privacy Through Competition?* 8 J. EUR. COMPET. LAW PRACT. 363 (2017). *See also, Consumer Data Rights and Competition Background: Note by the Secretariat*, OECD (2020), *available at* https://one.oecd.org/document/DAF/COMP(2020)1/en/pdf, and Geoffrey A. Manne & Ben Sperry, *The Problems and Perils of Bootstrapping Privacy and Data into an Antitrust Framework*, CPI ANTITRUST CHRONICLE 2 (2015), exploring the difficulties associated with incorporating consumer-data considerations into competition policy and enforcement.

[13] *See* Noah Joshua Phillips, *Remarks at the Mentor Group Paris Forum*, Federal Trade Commission (2019), 13-15, https://www.ftc.gov/news-events/news/speeches/remarks-commissioner-noah-joshua-phillips-mentor-group-paris-forum; and Maureen K. Ohlhausen & Ben Rossen, *Privacy and Competition: Discord or Harmony?* 67 ANTITRUST BULLETIN 552 (2022).

Further, the widely recognized "privacy paradox" illustrates that assessments of privacy are extremely subjective. Different consumers in differing contexts often express starkly different sensitivities about the protection of their personal data, rendering it challenging to provide accurate quality-driven assessments or even to set broadly acceptable baseline rules and policies.[14] More generally, an expansive approach that would treat privacy violations as sources of competitive harm potentially implies the need for antitrust investigations whenever dominant firms potentially violate any law, as they would acquire an advantage by saving costs or raising rivals' costs.[15] Antitrust authorities would therefore become economy-wide regulators.

While some recent cases brought by U.S. antitrust authorities have also placed privacy concerns in a prominent position,[16] there are two reasons that Europe appears to represent the primary testing ground for an integrated approach for privacy and antitrust. First, European policymakers long have prided themselves as leaders in regulating digital markets, notably for a broad array of heterogeneous legislative initiatives that have in common their strenuous efforts to foster data sharing and their sponsors' belief that the emergence of large technology platforms requires a bespoke approach.[17] In this sense, the initiative that blazed the path for the emerging integrationist perspective was the EU's General Data Protection Regulation (GDPR), which assigned control rights over data to individuals and, in light of the emerging regulatory convergence of privacy and antitrust, introduced a

[14] *See, e.g.*, Susan Athey, Christian Catalini, & Catherine E. Tucker, *The Digital Privacy Paradox: Small Money, Small Costs, Small Talk*, NBER Working Paper No. 23488 (2017); Alessandro Acquisti, Curtis Taylor, & Liad Wagman, *The Economics of Privacy*, 54 *J Econ Lit* 442 (2016). *See also*, Avi Goldfarb & Catherine Tucker, *Shifts in Privacy Concerns*, 102 AM ECON REV: PAPERS AND PROCEEDINGS 349 (2012), noting that individuals' privacy preferences evolve over time; notably, as people grow older. they get more privacy-conscious. *See also* Jeffrey T. Prince & Scott Wallsten, *How Much Is Privacy Worth Around the World and Across Platforms?*, 31 J ECON MANAG STRATEGY. 841 (2022), estimating individuals' valuation of online privacy across countries (United States, Mexico, Brazil, Colombia, Argentina, and Germany) and data types (personal information on finances, biometrics, location, networks, communications, and web browsing), and finding that Germans value privacy more than people in the United States and Latin American countries do and that, across countries, people most value privacy for financial and biometric information.

[15] Giuseppe Colangelo & Mariateresa Maggiolino, *Antitrust Über Alles. Whither Competition Law After Facebook?*, 42 WORLD COMPETITION LAW AND ECONOMICS REVIEW 355 (2019).

[16] *See, e.g.*, *Federal Trade Commission v. Facebook*, Case No. 1:20-cv-03590 (D.D.C. 2021), para. 163, arguing that "[t]he benefits to users of additional competition include some or all of the following: … variety of data protection privacy options for users, including, but not limited to, options regarding data gathering and data usage practices"; and *U.S. et al. v. Google*, No. 1:20-cv-03010 (D.D.C. 2020), para. 167, arguing that "[b]y restricting competition in general search services, Google's conduct has harmed consumers by reducing the quality of general search services (including dimensions such as privacy, data protection, and use of consumer data), lessening choice in general search services, and impeding innovation." *See also*, *Executive Order on Promoting Competition in the American Economy*, THE WHITE HOUSE (2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/07/09/executive-order-on-promoting-competition-in-the-american-economy, urging federal agencies to pay closer attention to "unfair data collection and surveillance practices that may damage competition, consumer autonomy, and consumer privacy."

[17] *See* Margrethe Vestager, *Tearing Down Big Tech's Walls*, PROJECT SYNDICATE (2023) https://www.project-syndicate.org/commentary/eu-big-tech-legislation-digital-services-markets-by-margrethe-vestager-2023-03, stating that "[w]e are proud that Europe has become the cradle of tech regulation globally."

general data-portability right for individuals, the rationale of which was inherently pro-competitive.[18]

Second, on the antitrust side of the ledger, the decision handed down by the German competition authority in the *Facebook* case was the first (and remains the primary) example of the trend toward enforcers asserting that competition law should be informed by data-protection principles and that data protection should enforced outside its usual legal context, with the goal of remedying the shortcomings of privacy law.[19]

Despite the purported synergies underpinning the respective policy goals of competition and data-protection law, however, their interests and objectives are not necessarily aligned.[20] In particular, there are signs that some major digital firms may interpret data-protection requirements in ways that risk distorting competition.[21] Namely, once privacy harms are included among the interests ostensibly protected in antitrust proceedings, platforms may have incentive to adjust their strategies to invoke data protection as a business justification for allegedly anticompetitive conduct.[22]

For example, some platforms justify their decisions to deny rivals access to their facilities on grounds that doing so would risk violating their users' privacy.[23] App-store providers in particular have described some restrictions that may be interpreted as anticompetitive self-preferencing (*e.g.*, requiring in-app purchases to be routed through their own in-app payment processor, limiting sideloading, and limiting app developers' ability to communicate with end users about the availability of alternative payment options) as necessary to guarantee users' security and privacy.[24]

---

[18] 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, [2016] OJ L 119/1, Article 20. See Bert-Jaap Koops, *The Trouble with European Data Protection Law*, 4 INT. DATA PRIV. LAW 4, 44 (2014), arguing that "[b]y its nature, data portability would be more at home in the regulation of unfair business practices or electronic commerce, or perhaps competition law—all domains that regulate abuse of power by commercial providers to lock-in consumers."

[19] Bundeskartellamt, 7 February 2019, Case B6-22/16.

[20] CMA-ICO Joint Statement, *supra* note 3, 18-19.

[21] *Ibid.*, 23.

[22] Douglas, *supra* note 12.

[23] *See, e.g.*, *hiQ Labs v. LinkedIn*, 938 F.3d 985 (9th Cir. 2019), affirmed 31 F.4th 1180 (9th Cir. 2022), allowing hiQ continued access to LinkedIn users' profile information in the name of competition. Notably, the court pointed out that hiQ's entire business depends on being able to access public LinkedIn member profiles and that, at the same time, there is little evidence that LinkedIn users who choose to make their profiles public actually maintain an expectation of privacy with respect to the information that they post publicly. Therefore, "even if some users retain some privacy interests in their information notwithstanding their decision to make their profiles public, we cannot, on the record before us, conclude that those interests—or more specifically, LinkedIn's interest in preventing hiQ from scraping those profiles—are significant enough to outweigh hiQ's interest in continuing its business, which depends on accessing, analyzing, and communicating information derived from public LinkedIn profiles."

[24] *See, e.g.*, *Epic Games v. Apple*, 559 F. Supp. 3d 898, 922–23 (N.D. Cal. 2021), affirmed in part and reversed in part 2023 U.S. App. LEXIS 9775 (9th Cir. 2023), finding that Apple's restrictions are designed to improve device security and user privacy; and District Court (Rechtbank) of Rotterdam, 24 December 2021, Case No. ROT

The most debated example illustrating the growing tension between data protection and antitrust is Apple's adoption of its "app tracking transparency" (ATT) policy, which creates new consent and notification requirements that change the way app developers can collect and use consumer data for mobile advertising on iOS. There very well could be privacy benefits associated with the new Apple framework, as it may enhance users' privacy and control over their personal data. But ATT also would now differentiate between a user's consent for Apple's advertising services and consent for third-party advertising services. The ATT policy might therefore represent a form of discrimination that benefits Apple's own advertising services and reinforces its position in app distribution to the detriment of rivals. For these reasons, the ATT policy is under investigation by several antitrust authorities.[25]

Given this backdrop, this paper seeks to investigate the intersection of privacy and competition law and to analyze how data-protection rules and principles have been applied in antitrust proceedings by the European Commission and by EU national competition authorities (NCAs). The analysis of the case law will illustrate how data protection has been progressively transformed from a weapon used by antitrust authorities to limit data accumulation to a shield exploited by digital platforms to justify potentially anticompetitive strategies and to game antitrust rules.

As a result, the paper aims to demonstrate the fallacy of the narrative that describes the relationship between privacy and antitrust in terms of synergy and complementarity. Such a paradigm, indeed, does not provide useful insights to solve the growing conflicts between the interests protected and the goals pursued by these different fields of law.

As has already happened with regard to the traditional intersection of intellectual-property protection and competition law, invoking a convergence of aims does not in itself sketch out a pragmatic solution. Notably, competition authorities' cooperation with data-protection regulators may help to ensure a coherent and uniform interpretation and application of the GDPR, it will not help antitrust authorities to strike the balance between privacy benefits and anticompetitive restrictions. In such a scenario, competition law enforcers risk being forced, like Buridan's Ass, to make a choice that cannot be made.[26]

---

21/4781 and ROT 21/4782, dismissing the arguments that Apple's in-app payment system is needed for security and privacy.

[25] *See, e.g.*, Autorità Garante della Concorrenza e del Mercato, 11 May 2023, Case A561; Press Release, *Bundeskartellamt Reviews Apple's Tracking Rules for Third-Party Apps*, BUNDESKARTELLAMT (2022), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2022/14_06_2022_Apple.html; Autorité de la Concurrence, 17 March 2021, Decision 21-D-07, *Apple*, https://www.autoritedelaconcurrence.fr/en/decision/regarding-request-interim-measures-submitted-associations-interactive-advertising-bureau; *Apple – The President of UOKiK Initiates an Investigation*, URZĄD OCHRONY KONKURENCJI I KONSUMENTÓW (2021), https://uokik.gov.pl/news.php?news_id=18092. *See also, Mobile Ecosystems: Market Study Final Report*, UK COMPETITION AND MARKETS AUTHORITY (2022) Chapter 6 and Appendix J, https://www.gov.uk/cma-cases/mobile-ecosystems-market-study.

[26] Phillips, *supra* note 13, 15.

The remainder of the paper is structured as follows. Section II examines the European cases in which privacy concerns have been addressed in antitrust proceedings to tackle data-accumulation strategies by large online platforms. Section III deals with the strategic use of privacy as a business justification for potential anticompetitive conduct, which emerges as a byproduct of promoting the integration of privacy and antitrust. Taking stock of the German *Facebook* case recently addressed by the Court of Justice of the European Union (CJEU),[27] Section IV illustrates how the intrinsic conflict between data-protection and competition law cannot be solved merely by invoking a purported synergy or complementarity. Section V concludes.

## II. Privacy as an Antitrust Sword Against Data-Accumulation Strategies

While data-protection and competition law serve different goals, it is commonly argued that the emergence of business models involving the collection and commercial use of personal data creates inevitable linkages between market power and data protection.[28] Notably, given that the key goal of the GDPR was to enable individuals to have control of their own personal data,[29] applying competition rules to digital markets could, it is asserted, promote precisely that control.[30] As a consequence, "previously separate policy areas become interlinked, and different regulatory authorities are increasingly required to consider a given set of issues from the perspective of contrasting policy aims and objectives."[31]

From this perspective, combining data-protection and competition law is justified on grounds that a common aim they share is to avoid exploitation of personal data and restrictions on consumers' privacy.[32] Since end users may experience less privacy and autonomy as a result of excessive data collection and use:

> Reductions in privacy could also be a matter of abuse control, if an incumbent collects data by clearly breaching data protection law and if there is a strong interplay between the data collection and the undertaking's market position.[33]

Indeed, from the standpoint of competition law, the idea has been advanced that the acquisition and exploitation of user information is itself the result of, or evidence of,

---

[27] CJEU (Grand Chamber), 4 July 2023, Case C-252/21, *Meta Platforms v. Bundeskartellamt*, EU:C:2023:537.

[28] *See, e.g.*, European Data Protection Supervisor, *supra* note 3, 26, stating that "clearly power is achieved through control over massive volumes of data on service users."

[29] *See* GDPR, *supra* note 18, Recital 7.

[30] European Data Protection Supervisor, *supra* note 3, 26.

[31] CMA-ICO Joint Statement, *supra* note 3, 5.

[32] Nicholas Economides & Ioannis Lianos, *Restrictions on Privacy and Exploitation in the Digital Economy: A Market Failure Perspective,* 17 J. COMPETITION LAW ECON. 765 (2021).

[33] *Competition Law and Data*, AUTORITÉ DE LA CONCURRENCE AND BUNDESKARTELLAMT (2016), 25, *available at* https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf?__blob=publicationFile&v=2.

market failure.[34] In particular, users of dominant advertiser-based platforms are said to suffer both from significant information asymmetries as a result of opaque data policies, and from platform lock-in, with no choice other than to consent to the harvesting and use of their data because of the lack of viable alternatives.[35]

On the data-protection side of the ledger, it is bears noting that, according to the GDPR, consent means any "freely given, specific, informed and unambiguous" indication of a data subject's wishes—whether by statement or some other clear affirmative action—that signifies agreement to the processing of his or her personal data.[36] Further, the GDPR specifies the conditions for consent, which include that: the request for consent be presented in a manner clearly distinguishable from other matters; that it be in an intelligible and easily accessible form; that it use clear and plain language; that the data subject has the right to withdraw consent at any time; and that, when assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract—including the provision of a service—is conditional on consent to processing personal data not actually needed for the performance of that contract.[37]

### A. Privacy Harm as an Antitrust Abuse

As the French and German competition authorities have argued in a joint paper:

> [L]ooking at excessive trading conditions, especially terms and conditions which are imposed on consumers in order to use a service or product, data privacy regulations might be a useful benchmark to assess an exploitative conduct, especially in a context where most consumers do not read the conditions and terms of services and privacy policies of the various providers of the services that they use.[38]

From this perspective, privacy concerns support the use of antitrust intervention to limit data-accumulation strategies by treating the restriction on privacy as a form of exploitative abuse.

Another way that privacy interests can be leveraged by antitrust authorities to address competitive concerns about data accumulation is through the merger-review process. Indeed, "firms that gain a powerful position through a merger may be able to gain further market power through the collection of more consumer data and privacy degradation."[39]

---

[34] Economides & Lianos, *supra* note 32.

[35] *Ibid.*, 770-771.

[36] GDPR, *supra* note 18, Article 4(11).

[37] *Ibid.*, Article 7.

[38] Autorité de la Concurrence and Bundeskartellamt, *supra* note 33, 25. *See also* Australian Competition & Consumer Commission, *supra* note 6, 41, arguing that exploitative conduct involves the use of market power to "give less and charge more" and that, for consumers, this may involve lower-quality services or the excessive costs of providing personal data to access services.

[39] Autorité de la Concurrence and Bundeskartellamt, *supra* note 33, 24.

The use of merger review is expected to be more effective to achieve privacy-policy goals given that, while an antitrust abuse investigation may at best neutralize or alleviate exploitation of data gathered by a dominant player, merger proceedings would prevent data accumulation in the first place.

### *1. The German Facebook case: Users' privacy-exploitation claim*

The Bundeskartellamt's decision in *Facebook* undoubtedly represents the apex, to date, of enforcers' application of the integrationist perspective.[40] According to the German competition authority, Facebook unlawfully exploited its dominant position in the German market for social networks by making the use of its social-networking service conditional on users granting extensive permission to collect and process their personal data. Notably, Facebook failed to make its users fully aware of the fact that it collected their personal data from sources other than the Facebook platform and then merged those data with personal information gathered through its own platform.[41] Further, Facebook put its users in the difficult position of either accepting this data policy or refraining from use of the social network in its entirety.

Indeed, even well-informed users would have not been able to voluntarily consent to such data collection and combination, as they would fear the alternative of no longer being able to access the social network.[42] Therefore, according to the German competition authority, when the data controller is in a dominant position, its users' consent is insufficient under the GDPR, because the platform's market power always puts users in the position of having to either take or leave any offers made.

Considering these findings, the Bundeskartellamt established a link between market power and privacy concerns. In its view, Facebook's terms and conditions were neither justified under data-protection principles nor appropriate under competition-law standards. To comply with the GDPR, users should have been asked whether they voluntarily consent to the practice of combining data in their Facebook user accounts, which could not consist merely of ticking a box. Indeed, given Facebook's superior market power, the user's choice to either accept comprehensive data combination or to refrain from using the social

---

[40] *Facebook*, *supra* note 19. For a comment on the different episodes of the *Facebook* saga, see, e.g., Kerber and Zolna, *supra* note 11; Anne C. Witt, *Excessive Data Collection as a Form of Anticompetitive Conduct: The German Facebook Case*, 66 Antitrust Bulletin 276 (2021); Marco Botta and Klaus Wiedemann, *The interaction of EU competition, consumer, and data protection law in the digital economy: the regulatory dilemma in the Facebook odyssey*, 64 Antitrust Bulletin 428 (2019); Colangelo and Maggiolino, *supra* note 15.

[41] *Facebook, supra* note 19, paras. 778-780 and 792, stating that users could not have expected that the platform would analyse data emanating from other websites and, when they had the opportunity to read Facebook's terms of service, users could barely understand the reasons why Facebook was processing and combining their data since Facebook's terms of service were very complex, replete with links to other explanations, and significantly too opaque to allow ordinary users to understand its data policy.

[42] *Ibid.*, section B(II), stating that voluntary consent to users' information being processed cannot be assumed if their consent is a prerequisite for using the Facebook service in the first place.

network could not be regarded as voluntary consent.[43] The Bundeskartellamt therefore concluded that Facebook had infringed GDPR rules by depriving its users of the human right to control the processing of their personal data and of the constitutional right of informational self-determination.

This form of coercion is, however, also relevant to competition law, as it was the result of Facebook's dominant position. Hence, Facebook's conduct could be considered exploitative within the meaning of the general clause of Section 19(1) of the German Competition Act (GWB), according to which competition law applies in every case where one bargaining party is so powerful that it can dictate the terms of the contract, with the end result being the abolition of the contractual autonomy of the other bargaining party. From the Bundeskartellamt's standpoint, if a dominant firm collects and analyzes users' data pursuant to terms and conditions that do not comply with EU data-protection rules, it also violates antitrust law by acquiring an unfair competitive advantage over firms that do adhere to the GDPR.

In summary, while the primary concern in the *Facebook* case was an antitrust issue (*i.e.*, the excessive quantity of data that Facebook accumulated in its unique dataset),[44] the Bundeskartellamt elaborated a theory of harm based primarily on protecting the constitutional right to informational self-determination. In other words, the competition authority invoked the right under which data-protection law affords individuals the power to decide freely and without coercion how their personal data is processed. Such reasoning is consistent with the case law of Section 19(1) GWB, which allows an antitrust authority to consider the protection of constitutional values and interests in assessing the practices of dominant firms. While the Bundeskartellamt contended that its proceedings against Facebook would also generally be possible under the EU's antitrust provision on

---

[43] *Ibid.*, para. 645, highlighting that GDPR's Recitals 42 and 43 state that consent is not freely given where consumers have no alternative options, or where there are clear power imbalances. *See also* Inge Graef & Sean Van Berlo, *Towards Smarter Regulation in the Areas of Competition, Data Protection and Consumer Law: Why Greater Power Should Come with Greater Responsibility*, 12 EUR. J. RISK REGUL. 674 (2021), arguing that, in formulating this two-way interaction between data-protection law and competition law, the Bundeskartellamt has not only incorporated data-protection principles into its competition analysis, but similarly transferred elements of competition law into data protection; and Orla Lynskey, *Grappling With 'Data Power': Normative Nudges From Data Protection and Privacy*, 20 THEOR. INQ. LAW 189 (2019), supporting the view that the GDPR provides a normative foundation for imposing a special responsibility on controllers holding data power, analogous to the special responsibility that competition law imposes on dominant firms.

[44] *See* Press Release, *Bundeskartellamt Prohibits Facebook From Combining User Data From Different Sources*, BUNDESKARTELLAMT (2019), https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html;jsessionid=8A581062B36687451A3D1E7A5C256390.2_cid378?nn=3600108, arguing that "[t]he combination of data sources substantially contributed to the fact that Facebook was able to build a unique database for each individual user and thus to gain market power."

exploitative abuses (Article 102(a) TFEU),[45] Section 19 GWB offered a broader (and, hence, more legally convenient) general clause.[46]

This privacy-focused approach also manifested in the remedy that Meta presented, and which the Bundeskartellamt welcomed. To implement the German antitrust authority's decision, Meta proposed several changes to the accounts center that would allow customers to decide whether they wanted to use all services separately, each with their own circumscribed functions, or to use additional functions across accounts, which would require sharing more personal data.[47] In the Bundeskartellamt's view, this solution would allow Meta's customers to make a largely free and informed decision.

The Bundeskartellamt's approach in the Facebook case therefore appears quite distinctive and essentially German-specific, as well as particularly controversial with respect to the scope and boundaries of competition and data-protection enforcement.[48] Indeed, in ascertaining a privacy violation previously undetected by any data-protection authority, the Bundeskartellamt acted as a self-appointed enforcer of data-protection rules.

It also interpreted data-protection rules in ways that far exceed the limits of its legal competence, given that there is nothing in the GDPR that makes the quality of a user's consent agreement contingent on the data controller's market power. Indeed, the GDPR makes no distinction at all on the basis of a firm's market power. Size does not matter when it comes to data-protection law; a dominant firm is just as bound by privacy rules as its smaller rivals. At the same time, from the perspective of competition law, following the Bundeskartellamt's expansive stance, virtually every legal infringement by a dominant firm could amount to an antitrust violation.

Because of the thorny implications for the interface between antitrust and data-protection law, the *Facebook* decision unsurprisingly sparked a heated debate not only in the literature, but also between German courts.

The Higher Regional Court (Oberlandesgericht, or OLG) of Düsseldorf suspended the landmark decision, expressing serious doubts about its legal basis and complaining that the Bundeskartellamt was "merely discussing a data protection issue, and not a competition problem."[49] Pursuant to both European and German antitrust provisions, a charge of abuse of market power by a dominant undertaking requires a finding of anticompetitive conduct

---

[45] *Facebook FAQs*, BUNDESKARTELLAMT (2019), 6, https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook_FAQs.pdf?__blob=publicationFile&v=6.

[46] *See* Colangelo & Maggiolino, *supra* note 15.

[47] Press Release, *Meta (Facebook) Introduces New Accounts Center – An Important Step in the Implementation of the Bundeskartellamt's Decision*, BUNDESKARTELLAMT (2023), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2023/07_06_Meta_Daten.html.

[48] Colangelo & Maggiolino, *supra* note 15.

[49] *OLG Düsseldorf*, 26 August 2019, Case VI-Kart 1/19 (V), 10.

and, hence, damage to competition—namely, to the freedom of competition, that is "safeguarding competition and the openness of market access."[50] Therefore, dominant undertakings carry a special responsibility only in the domain of competition, rather than for compliance with the entire legal system by avoiding any violation of the law.[51] Further, in the appellate court's view, no influence was exerted on users, as Facebook's terms of service simply require them to weigh the benefits of using an ad-financed (and, therefore, free) social network against the consequences of Facebook's use of the additional data that it gathers.

However, the Federal Supreme Court (Bundesgerichtshof, or BGH) overturned the OLG's judgment and held that Facebook must comply with the Bundeskartellamt's decision.[52] The BGH's reasoning did, however, differ from the Bundeskartellamt's. According to the Federal Supreme Court, it is inconclusive whether Facebook's processing and use of personal data complied with the GDPR. The court's decision turned instead on Facebook's terms of service, which the BGH found are abusive if they deprive Facebook users of any choice in whether they wish to use the network in a more personalized manner (thus, linking their experience to Facebook's potentially unlimited access to characteristics that include their off-Facebook use of the internet more generally) or whether they wanted a level of personalization that was based solely on data that they themselves share on Facebook.[53]

Notably, the BGH found that Facebook's data processing constitutes an "imposed extension of services," as users receive an indispensable service only in combination with another undesired service.[54] Accordingly, such a practice was evaluated as both an exploitative and an exclusionary abuse. The lack of options available to users affects their personal autonomy and the exercise of their right to informational self-determination, as protected by the GDPR. Given lock-in effects that serve as barriers for network users who would otherwise like to switch providers, the BGH found that this lack of options exploits users in a manner relevant under competition law since, under effective competition, one would expect more diverse market offerings for social networks.[55] Further, the terms of service could also impede competition for online advertising, allowing Facebook to protect its dominant position against rivals, as they would be able to improve their offerings due to privileged access to a considerably larger database.[56]

---

[50] *Ibid.*, 11.

[51] *Ibid.*, 12.

[52] Bundesgerichtshof, 23 June 2020, Case KVR 69/19.

[53] *Ibid.*, para. 58.

[54] *Ibid.*.

[55] *Ibid.*, para. 86.

[56] *Ibid.*, para. 94.

As a result of this clash among the German courts, the Higher Regional Court of Düsseldorf decided to refer the case to the CJEU, adding a new twist to the *Facebook* saga.[57] In particular, the OLG of Düsseldorf raised seven questions about the interpretation of the GDPR, fundamentally asking the CJEU to untie the knot and clarify the competence of a competition authority to determine and penalize a GDPR breach; the prohibition on processing sensitive personal data and the conditions applicable to consenting to their use; the lawfulness of processing personal data in light of certain justification; and the validity of a user's consent to processing personal data given to an undertaking in a dominant position.[58]

It is also worth noting the different approaches taken by other authorities concerning the very same Facebook conduct. Notably, the Italian competition authority evaluated such practices as violations of the Consumer Code (instead of the competition law),[59] while in Belgium, the Court of First Instance of Brussels found a violation of privacy rules.[60]

### 2. *The Digital Markets Act: Rivals' exclusion and primacy of data-protection interests over competition-policy goals*

The *Facebook* case has already influenced the broader debate about the limits of competition law to address certain features of digital markets effectively. The EU's Digital Markets Act (DMA)—which was explicitly grounded in the assumption that competition law alone is unfit to tackle certain challenges and systemic problems posed by the platform economy—specifically prohibits combining personal data across a gatekeeper's services, a provision clearly inspired by the German investigation.[61]

Notably, pursuant to Article 5(2) DMA, a gatekeeper shall not: (a) process—for the purpose of providing online-advertising services—end users' personal data using third-party services that themselves make use of the gatekeeper's core platform services; (b) combine personal data from the relevant core platform service with personal data from any further core platform services, or from any other services provided by the gatekeeper, or with personal data from third-party services; (c) cross-use personal data from the relevant core platform service in other services provided separately by the gatekeeper, including other core platform services, and vice versa; and (d) sign end users into the gatekeeper's other services in order to combine personal data, "unless the end user has been presented with the specific choice and has given consent" within the meaning of the GDPR.

---

[57] OLG Düsseldorf, 24 March 2021, Case Kart 2/19 (V).

[58] *Meta*, *supra* note 27.

[59] Autorità Garante della Concorrenza e del Mercato, 10 December 2018, Case PS11112, *Facebook-Condivisione dati con terzi*.

[60] Nederlandstalige Rechtbank van Eerste Aanleg te Brussel, 16 February 2018.

[61] Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L 265/1, Article 5(2).

Further, according to Recital 36—given that gatekeepers process personal data from a significantly larger number of third parties than other undertakings—data processing for the purpose of providing online-advertising services gives gatekeeper platforms potential "advantages in terms of accumulation of data," thereby "raising barriers to entry." To ensure that gatekeepers do not unfairly undermine the "contestability" of core platform services, gatekeepers should enable end users to "freely choose to opt-in" to such data processing and sign-in practices. This may be accomplished by offering a less-personalized but equivalent alternative, and without making the use of (or certain functions of) the core platform service conditional on the end user's consent.[62]

Moreover, in light of Recital 37, when a gatekeeper does request consent, it should proactively present a "user-friendly solution" to the end user to provide, modify, or withdraw consent in an explicit, clear, and straightforward manner. In particular, consent should be given by a clear affirmative action or statement establishing a freely given, specific, informed and unambiguous indication of agreement by the end user, as defined in the GDPR.

Lastly, it should be as easy to withdraw consent as to give it. Gatekeepers should not design, organize, or operate their online interfaces in a way that deceives, manipulates, or otherwise materially distorts or impairs end users' ability to freely give or withdraw consent.[63] In particular, gatekeepers should not be allowed to prompt end users more than once a year to give consent for a data-processing purpose for which the user either did not initially give consent or actively withdrew consent.

The idea that only opt-in mechanisms can produce effective consent within the meaning of the GDPR is confirmed by the obligation under Article 6(10) DMA, which imposes on gatekeepers the duty to provide business users, or third parties authorized by a business user, access to aggregated and non-aggregated data (including personal data) generated in the context of using the relevant core platform services.[64]

---

[62] *Ibid.*, Recital 36.

[63] *Ibid.*, Recital 37.

[64] For critical analysis of this issue and more generally on the controversial relationship between the DMA and the GDPR, *see* Alba Ribera Martínez, *The Circularity of Consent in the DMA: A Close Look into the Prejudiced Substance of Articles 5(2) and 6(10)*, CONCORRENZA E MERCATO (forthcoming). *See also* Marco Botta & Danielle Da Costa Leite Borges, *User's Consent Under Art. 5(2) Digital Markets Act (DMA): Exploring the Complex Relationship Between the DMA and the GDPR*, EUI RSC Working Paper (forthcoming), arguing that, while respecting the general criteria indicated by Art. 7 GDPR, the users' consent under Art. 5(2) DMA should be adjusted to the DMA peculiarity and that the DMA should be considered as a *lex specialis*, taking precedence over the GDPR in case of conflict. Previously, the revised e-Privacy Directive introduced an opt-in system for website cookies: *see* Directive 2009/136/EC amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, (2009) OJ L 337/11, Article 5(3).

The provision under Article 5(2) DMA provides interesting insights into the relationship between data-protection and competition law. By emphasizing that the primary concern is online gatekeepers' data-accumulation strategies, the DMA's approach differs from the one the Bundeskartellamt pursued in *Facebook*. Rather than focusing on potential harms to users' self-determination and digital identity, the DMA points to a pure antitrust harm related to market contestability. Therefore, even if "[t]he data protection and privacy interests of end users are relevant to any assessment of potential negative effects of the observed practice of gatekeepers to collect and accumulate large amounts of data from end users,"[65] the primary interest protected is a competitive one—namely to avoid foreclosure against rivals.

From this perspective, it may be argued that the DMA adopts an integrated approach that takes data-protection principles into account within a competitive assessment of gatekeepers' conduct. The very last part of the provision, however, demonstrates the opposite. By subordinating the prohibitions to respect the GDPR, European authorities arguably acknowledge the potential tensions between data-protection interests and competition-policy goals. Moreover, in the event of such a conflict, the DMA affirms the primacy of the former. Indeed, all the forms of conduct listed in Article 5(2) are forbidden "unless" the end user has been presented with a specific choice and given consent within the meaning of the GDPR.

### 3. *New German platform-specific antitrust rules and the Google case*

There is another interesting and ongoing German investigation regarding Google's data-processing terms. Notably, in January 2023, the Bundeskartellamt issued a statement of objections against Google claiming that, under the company's current terms, users are not given "sufficient choice" as to how their data are processed across services.[66]

The antitrust authority noted that Google's business model relies heavily on processing user data and that its current terms allow the company to combine various data from various services and use them, for example, to create very detailed user profiles that the company can exploit for advertising and other purposes, or to train functions provided by Google services. Google may, for various purposes, collect and process data across services, which include both its own widely used services (Google Search, YouTube, Google Play, Google Maps, and Google Assistant), as well as numerous third-party websites and apps. Bundeskartellamt President Andreas Mundt stated that this grants Google a "strategic advantage" over other companies.[67]

---

[65] DMA, *supra* note 61, Recital 72.

[66] Press Release, *Statement of Objections Issued Against Google's Data Processing Terms*, BUNDESKARTELLAMT (2023), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2023/11_01_2023_Google_Data_Processing_Terms.html.

[67] *Ibid.*

According to the Bundeskartellamt's preliminary assessment, the choices offered to users are too general and insufficiently transparent. The authority contends that sufficient choice would require that users be able to limit data processing to the specific service used. In addition, they also must be able to differentiate between the purposes for which the data are processed. Moreover, the choices must not be devised in a way that would make consenting to data processing across services easier than not consenting to it.

The framing of the Google investigation is similar to that of the *Facebook* case. The antitrust authority is fundamentally concerned with a data-accumulation strategy that it contends confers to Google a critical competitive advantage. And given that having access to more user data than rivals have cannot in itself be considered anticompetitive, privacy concerns are exploited to limit such a strategy.

There is, however, a significant difference worth highlighting. In the Google case, the Bundeskartellamt's position benefits from a new provision of Section 19a GWB,[68] which empowers national competition authorities to tackle platform-specific practices that are similar and functionally equivalent to those prohibited under the DMA.[69] Notably, since January 2021, the Bundeskartellamt has had the power to designate undertakings of "paramount significance for competition across markets." The factors relevant to this designation include a platform's dominant position in one or more markets; financial strength or access to other resources; vertical integration and activities in otherwise related markets; access to data relevant for competition; and the importance of the activities for third parties' access to supply and sales markets and related influence on third parties' business activities. Google has been the first platform to be designated as of paramount significance for competition across markets.[70]

Once the designation is completed, the Bundeskartellamt can prohibit such undertakings from engaging in anticompetitive practices. In particular, the new provision introduces a list of seven types of abusive practices that are prohibited, unless the undertaking is able to demonstrate that the conduct at issue is objectively justified. While the targeted practices are similar to those captured by the DMA, the main differences are that the German list is considered exhaustive and the practices at issue are not prohibited *per se*. Instead, it introduces a reversal of the burden of proof, allowing firms to provide objective justifications for their conduct, which is not allowed under the DMA.

---

[68] *Entwurf Eines Gesetzes zur Änderung des Gesetzes Gegen Wettbewerbsbeschränkungen für ein Fokussiertes, Proaktives und Digitales Wettbewerbsrecht 4.0 und Anderer Wettbewerbsrechtlicher Bestimmungen*, BUNDESTAG (2020), *available at* https://dserver.bundestag.de/btd/19/234/1923492.pdf.

[69] *See* Giuseppe Colangelo, *The European Digital Markets Act and Antitrust Enforcement: A Liaison Dangereuse*, 47 EUR. LAW REV. 597 (2022).

[70] Bundeskartellamt, 30 December 2021, Case B7-61/21, https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2022/B7-61-22.html.

For the sake of this analysis, pursuant to paragraph 4 of Section 19a GWB, the Bundeskartellamt may prohibit an undertaking of paramount significance for competition across markets from creating or appreciably raising barriers to market entry (or otherwise impeding other undertakings) by processing data relevant for competition that have been collected by the undertaking, or demanding terms and conditions that permit such processing—in particular, making the use of its services conditional on a user agreeing to data processing by the undertaking's other services or by a third-party provider without "sufficient choice" as to whether, how, and for what purpose such data are processed.

As mentioned, while the *Google* investigation resembles the background of the *Facebook* decision, the introduction of Section 19a(4) GWB has relevant implications. The new provision is clearly inspired by the strategy investigated in *Facebook* and, as already enshrined in the DMA, essentially aims to ease enforcement, avoiding the hurdles and burdens of standard antitrust analysis. Practically speaking, the Bundeskartellamt therefore does not need to struggle to find a proper theory of harm and can easily avoid the odyssey it experienced in *Facebook*. Moreover, the new provision's wording changes the legal landscape, distinguishing the *Google* investigation from both the parallel DMA provision and the *Facebook* decision. Indeed, by relying on the lack of "sufficient choice" for users, Section 19a(4) GWB does not include any reference to the GDPR, thus allowing the Bundeskartellamt to provide an autonomous interpretation. With regard to the comparison with *Facebook*, on the other hand, Section 19a(4) GWB—just like the DMA—aims to promote contestability in the market ("creating or appreciably raising barriers to market entry"). Hence, data accumulation is prohibited to the extent that it excludes rivals, rather than whether it exploits users' privacy.

That the German provision is effective has been confirmed by Google's decision to end the proceeding by submitting commitments.[71] Under those commitments, Google will give its users the option to grant free, specific, informed, and unambiguous consent to have their data processed across services.[72] Google will also offer corresponding choice options for particular combinations of data and services, and will design selection dialogues to avoid dark patterns, thus not guiding users manipulatively towards cross-service data processing.

It is worth noting that Google's commitments involve more than 25 services, with only those services that the European Commission has since designated as core platform services

[71] Bundeskartellamt, 5 October 2023, Case B7-70/21.

[72] The Bundeskartellamt identified four main deficiencies to support its prohibition of Google's data-processing terms (*ibid.*, paras. 50-54). Namely, because of a lack of sufficient granularity in the settings options, users could not opt out of cross-service data processing or limit data processing to the Google service in which the data were generated. End users could only choose between accepting personalization across all services or opting out of personalization altogether. Further, users were not given sufficient choice within the meaning of Section 19a GWB, as in some cases, Google offers users no choice at all as to data-processing options. Furthermore, the settings options that Google offered lacked sufficient transparency—*i.e.*, sufficiently concise and comprehensible indications providing users with sufficient information as to whether, how, and for what purpose Google processes data across services. Finally, when creating a Google account, a user's options consent or reject consent were not equivalent.

under the DMA (*i.e.*, Google Shopping, Google Play, Google Maps, Google Search, YouTube, Google Android, Google Chrome and Google's online-advertising services) excluded from the list. While this was intended to avoid practical conflicts with application of the DMA, it also represents an acknowledgment that the DMA and German antitrust law pursue the very same goals. Indeed, as stated in the decision, Google's commitments "are intended to correspond in substance to an extension of Google's obligations under Article 5(2) DMA" to further services and, therefore, "in case of doubt, the terms used in the Commitments are to be interpreted in accordance with their meaning in the DMA."[73]

### B. Privacy Harm in Merger Analysis: The European Commission's Case Law

Given this broad consensus regarding synergies between data-protection and competition law in digital markets, it is somewhat surprising how reluctant the European Commission has been to implement this integrated approach in the context of merger analysis.[74] Indeed, while acknowledging privacy's role as a parameter of competition between online platforms, the Commission has to date not blocked any merger on the grounds of protecting individuals' control over personal data, and it has nearly always approved unconditionally those mergers that raised privacy concerns.

Notably, in the days before the GDPR, the Commission authorized the Google/DoubleClick merger, in the process affirming that antitrust and data-protection rules had wholly separate scopes.[75] While it could have determined that the combined data-collection activities of two players active in the online-advertising industry raised concentration concerns and a possible unfair advantage in producing targeted advertising, the Commission's assessment, under pure antitrust criteria, was that it was unlikely that the new entity would obtain a competitive advantage unmatchable by its rivals.[76] Further, the Commission underlined that its decision exclusively concerned an appraisal of the operation under competition rules, without prejudice to other obligations imposed on the parties by data-protection and privacy laws.[77]

This stance of maintaining separate regulatory spheres of inquiry was even more clearcut in the 2014 Facebook/WhatsApp merger.[78] Assessing the potential edge the combined

---

[73] *Ibid.*, para. 78.

[74] *See, e.g.*, Inge Graef, Damian Clifford, & Peggy Valcke, *Fairness and Enforcement: Bridging Competition, Data Protection, and Consumer Law*, 8 INT. DATA PRIV. LAW 200, 219-220 (2018).

[75] European Commission, 11 March 2008, Case COMP/M.4731. Previously, in a different setting (*i.e.*, discussing an exchange-of-information case), the CJEU (23 November 2006, Case C-238/05, *Asnef-Equifax*, EU:C:2006:734, para. 63) affirmed that "any possible issues relating to the sensitivity of personal data are not, as such, a matter for competition law, they may be resolved on the basis of the relevant provisions governing data protection."

[76] *Google/DoubleClick*, *supra* note 75, para. 364. See also para. 365, where the Commission noted that "that the combination of data about searches with data about users' web surfing behaviour [wa]s already available to a number of Google's competitors."

[77] *Ibid.*, para. 368.

[78] European Commission, 3 October 2014, Case COMP/M.7217.

entity might derive from controlling huge amounts of data, the Commission found that, regardless whether the merged entity would start using WhatsApp user data to improve targeted advertising on Facebook, there continued to be large troves of valuable internet user data that were not within Facebook's exclusive control.[79] More importantly, the Commission stated that:

> Any privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the Transaction do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules.[80]

The outcome and reasoning were the same in *Microsoft/LinkedIn*.[81] Consistent with the findings in *Facebook/WhatsApp,* the results of the Commission's market investigation revealed that privacy is an important parameter of competition and a driver of customer choice.[82] But not only did the transaction not raise serious antitrust concerns in online advertising, given that combining the firms' respective datasets did not appear to result in raising rivals' barriers to entry or expansion,[83] but also:

> [S]uch data combination could only be implemented by the merged entity to the extent it is allowed by applicable data protection rules. … Microsoft and LinkedIn are subject to relevant national data protection rules with respect to the collection, processing, storage and usage of personal data, which, subject to certain exceptions, limit their ability to process the dataset they maintain.[84]

Moreover, the Commission noted that the GDPR "may further limit Microsoft's ability to have access to, and process, its users' personal data in the future since the new rules will strengthen the existing rights and empower individuals with more control over their personal data."[85]

In a nutshell, the Commission again chose to defer to privacy rules for protecting individuals' personal data and analyzed the transaction's antitrust issues while "[a]ssuming such data combination [was] allowed under the applicable data protection legislation."[86] The Commission did not discuss whether the relevant markets under consideration were sufficiently competitive to provide users with the optimal level of privacy-friendly options. It didn't establish any link between the merging firms' market power and the variety of privacy-friendly tools and services they provided. Nor did it find any connection between

---

[79] *Ibid.*, para. 189.

[80] *Ibid.*, para. 164.

[81] European Commission, 6 December 2016, Case COMP/M.8124.

[82] *Ibid.*, fn 330.

[83] *Ibid.*, para. 180.

[84] *Ibid.*, para. 177.

[85] *Ibid.*, para. 178.

[86] *Ibid.*, para. 179.

such market power and the optimal quantity of personal data that the firms under scrutiny should have collected.

In *Apple/Shazam*, despite some concern that the acquisition would grant Apple access to commercially sensitive information about competitors of its Apple Music service, the Commission regarded it as unclear whether the merged entity would be able to put competing providers of digital-music streaming apps at a competitive disadvantage. And they again stressed that personal-data processing remained subject to the GDPR.[87]

The recent Google/Fitbit merger offered the Commission another opportunity to interrogate overlaps among data protection and antitrust. Ultimately, the Commission's analysis focused on the data collected via Fitbit's wearable devices and the interoperability of wearable devices with Google's Android operating system for smartphones.[88] While some market participants complained that, in combining those databases, Google could obtain a competitive advantage in the digital health-care sector that would leave competitors unable to compete, others (including the European Data Protection Board) raised privacy concerns on grounds that the merger would make it increasingly difficult for users to track the purposes for which their health data would be used.[89]

To address such issues, Google offered (and the Commission accepted) commitments to maintain a technical separation of Fitbit user data by storing them in a data silo separate from any Google data used for advertising; that it will not use the health and wellness data collected from users' wrist-worn wearable devices and other Fitbit devices for Google Ads; and it will ensure that users have an effective choice to grant or deny the use of health and wellness data stored in their Google Account or Fitbit Account by other Google services.

With regard to privacy concerns, the Commission reminded those involved that the parties are held accountable to implement appropriate technical and organizational measures to ensure that data processing is performed in accordance with the GDPR.[90] More specifically, the Commission noted that the GDPR is designed to enhance transparency over data processing, accountability by data controllers and, ultimately, users' control over their data.[91] The Commission found no evidence that privacy was an important parameter of competition in wearables and underlined that any privacy or data-protection decision or

---

[87] European Commission, 6 September 2018, Case COMP/M.8788, paras. 221 and 314.

[88] European Commission, 17 December 2020, Case COMP/M.9660.

[89] *See*, *Statement on Privacy Implications of Mergers*, EUROPEAN DATA PROTECTION BOARD (2020), *available at* https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_2020_privacyimplicationsofmergers_en.pdf, arguing that "(t)here are concerns that the possible further combination and accumulation of sensitive personal data regarding people in Europe by a major tech company could entail a high level of risk to the fundamental rights to privacy and to the protection of personal data."

[90] *Google/Fitbit*, *supra* note 84, para. 410.

[91] *Ibid.*, fn. 299.

initiative the parties might adopt would have to comply with the data-protection rules set out by the GDPR.[92]

The Commission addressed similar privacy issues arising from the combination of datasets in *Microsoft/Nuance*[93] and *Meta/Kustomer*,[94] each time noting that GDPR served as the appropriate safeguard.

Moreover, the Commission appears to retain this "separatist" stance, as confirmed recently by its unconditional approval of a joint venture among Deutsche Telekom, Orange, Telefónica, and Vodafone, which will offer a platform to support brands and publishers' digital-marketing and advertising activities in France, Germany, Italy, Spain, and the United Kingdom.[95] Subject to a user's consent (*i.e.*, on an opt-in basis only), the joint venture will generate a unique digital code derived from the user's mobile or fixed-network subscription that will allow brands and publishers to recognize users on their websites or applications on a pseudonymous basis, group them under various categories, and tailor their content to specific user groups.

Whatever privacy and security benefits or harms might arise from the operation, the Commission was ultimately guided in its decision by the lack of competition concerns. Moreover, the Commission declared that it has been in contact with data-protection authorities during its investigation and that data-protection rules are fully applicable, irrespective of the merger's clearance.

## III. Privacy as a Shield Against Antitrust Allegations

Amid these limited and somewhat confused attempts to address privacy concerns in digital markets by integrating data-protection rules and competition-law enforcement, a novel and challenging phenomenon has emerged. Taking stock of some authorities' willingness to grant primacy to data protection in the context of antitrust interventions, some platforms have implemented changes to their ecosystems with the declared aim of ensuring increased privacy to end users. For instance, Apple and Google have developed policies to restrict third parties from sharing user data through apps in the platforms' respective operating systems and websites in their respective browsers.[96] These policies include Apple's ATT, Intelligent Tracking Prevention, and iCloud Private Relay, and Google's Android Privacy Sandbox and Chrome Privacy Sandbox. To a certain extent, the DMA may have even

---

[92] *Ibid.*, fn. 300.

[93] European Commission, 21 December 2021, Case COMP/M.10290.

[94] European Commission, 27 January 2022, Case COMP/M.10262.

[95] Press Release, *Commission Clears Creation of a Joint Venture by Deutsche Telekom, Orange, Telefónica and Vodafone*, EUROPEAN COMMISSION (2023), https://ec.europa.eu/commission/presscorner/detail/en/IP_23_721. Previously, in a similar vein, *see* European Commission, 4 September 2012, Case COMP/M.6314, *Telefónica UK/Vodafone UK/ Everything Everywhere/ JV*.

[96] UK Competition and Markets Authority, *supra* note 25, Appendix J.

encouraged some of these design choices by apparently endorsing the view that only opt-in systems can ensure effective consent within the meaning of the GDPR.

The suspicion is that such facially noble intentions may actually conceal a goal of achieving anticompetitive advantages at the expense of rivals and business users. Therefore, it appears that a new form of regulatory gaming is on the horizon. Particularly in online-advertising markets, privacy may be weaponized as a business justification for potentially anticompetitive conduct and data-protection requirements may be leveraged to distort competition. The relevance and dangerousness of such hypotheses are confirmed by certain antitrust investigations launched recent years, which the following paragraphs will analyze.

### A. Apple's ATT Policy

As illustrated above, data represents a primary input for platforms whose business models rely on monetizing consumer information by selling targeted advertising and personalized sponsored content. In digital markets, advertisers benefit from access to detailed (and hence, highly valuable) user data, such as browsing behavior, profiles on company websites, demographic information, shopping habits, and past purchase history, especially given the potential to use that data across advertising platforms.[97] Therefore, the effectiveness of targeted advertising and the overall profitability of advertising-based business models rely on data tracking.

To enhance users' privacy protection, however, regulatory interventions like the GDPR aim to reduce data collection and mitigate platforms' tracking by requiring explicit consent for users' individual-behavior data to be used for targeted advertising.[98] In addition, some platforms have adopted (or announced) privacy-centric policies that would limit third parties' ability to track data, thus affecting the profitability and revenues of their advertising strategies.[99]

---

[97] *See, e.g.*, Nils Wernerfelt, Anna Tuchman, Bradley Shapiro, & Robert Moakler, *Estimating the Value of Offsite Data to Advertisers on Meta*, SSRN (2022) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4176208, finding that the costs to acquire new consumers through targeted advertisements increases tremendously without access to offsite data. On the value of external data and on the relevance (especially for small and medium-sized players) of gaining access to external data from large players in the marketplace, *see also* Xiaoxia Lei, Yixing Chen, & Ananya Sen, *The Value of External Data for Digital Platforms: Evidence from a Field Experiment on Search Suggestions*, SSRN (2023) https://ssrn.com/abstract=4452804.

[98] For a review of the economic literature on the GDPR and its unintended consequences on firms' performance, innovation, competition, and market concentration, as well as its impact on personalized marketing channels, *see* Garrett A. Johnson, *Economic Research on Privacy Regulation: Lessons from the GDPR and Beyond*, (forthcoming) in *The* ECONOMICS OF PRIVACY, *supra* note 2.

[99] *See* Reinhold Kesler, *Digital Platforms Implement Privacy-Centric Policies: What Does It Mean for Competition?*, CPI ANTITRUST CHRONICLE 1 (2022), and Daniel Sokol & Feng Zhu, *Harming Competition and Consumers Under the Guise of Protecting Privacy: Review of Empirical Evidence*, CPI ANTITRUST CHRONICLE 12 (2022), for a review of economic studies showing that advertising revenues decrease with limited tracking abilities and providing empirical evidence of reduced user tracking on Apple as a consequence of the ATT policy. *See also* Wernerfelt, Tuchman, Shapiro, & Moakler, *supra* note 97, finding that restrictions on offsite data particularly harms smaller advertisers.

Apple's ATT policy is a paramount example of such product changes. With the iOS 14.5 privacy update, Apple introduced an opt-in mechanism that imposes more restrictive rules on competing app developers than those the company applies to itself. The differential treatment mostly concerns features that prompt users to grant apps permission to track them. Without consumers opting into this prompt, developers cannot access their identifiers for advertisers (IDFA), which are used to monitor users' activity across apps.

The wording of the prompts ATT offers for user consent may unduly influence users to withhold consent from third-party apps. For apps developed by Apple itself, the consent prompt focuses on the positive aspects of personalized services, rather than the tracking of users' browsing activity. In contrast, the prompt for third-party app developers places greater emphasis on other companies' app and website tracking activities (without explaining the term "track") and does not provide information about the benefits that users could derive from personalized advertising. Moreover, even if the user gives consent to be tracked, third-party app developers remain unable to share the same data that would allow for the personalization of ads, and measure their effectiveness, on another app. Indeed, for third-party app developers, the ATT framework introduces a double opt-in, requiring the user to consent to being tracked for each access to different apps, even if these apps are linked.

This model illustrates an apparent tension between data-protection interests and antitrust goals. While the ATT policy has been framed as a privacy-protecting measure, it is not just the level of privacy chosen by Apple in its digital ecosystem that is at issue, but also the competitive implications that arise from the choice to adopt discriminatory privacy policies. Indeed, the differentiated treatment imposed on third-party app developers appears likely to reduce their advertising revenues, and hence their level of competitiveness vis-à-vis Apple, and could eventually enhance the dominance of the iOS ecosystem.

Notably, the ATT framework may hinder competitors' ability to sell advertising space, in ways that redound to Apple's own advantage—in particular, benefiting the company's own direct sales and advertising-intermediation platforms. Further, limiting third parties' ability to profile users may reduce business-model differentiation. The advertising-based monetization model used by free and freemium apps may be rendered less sustainable, causing these apps to exit the market or gradually shift to the fee-supported model. This would come at the expense of end consumers, for whom the possibility of choosing free or lower-priced apps could be reduced.[100]

---

[100] *See* Sokol & Zhu, *supra* note 99. *See also* Kesler, *Digital Platforms Implement Privacy-Centric Policies: What Does It Mean For Competition?*, *supra* note 99, suggesting that the ATT brings back paid apps and reinforces the industry trend toward more in-app payments. With regard to the possibility that the ATT framework may affect the developers' incentives in the Apple ecosystem, *see also* Cristobal Cheyre, Benjamin T. Leyden, Sagar Baviskar, & Alessandro Acquisti, *The Impact of Apple's App Tracking Transparency Framework on the App Ecosystem*, CESifo Working Paper No. 10456 (2023), https://www.cesifo.org/en/publications/2023/working-paper/impact-apples-app-tracking-transparency-framework-app-ecosystem, finding that developers did not withdraw from the market after ATT and instead adapted to operate under the new conditions. Further, *see* Ding Li & Hsin-Tien Tsai,

For these reasons, the ATT framework is currently under scrutiny by antitrust authorities in France,[101] Germany,[102] Italy,[103] and Poland,[104] who suspect that Apple is masking an anticompetitive strategy under the guise of privacy protection. Similar doubts have been raised by the UK Competition and Markets Authority in its market study on mobile ecosystems.[105]

Given these kinds of market responses, it is difficult to see how an integrated approach to data-protection and competition law could be implemented in practice. Contrasting the Italian and French investigations may provide useful insights into this conundrum. The Italian competition authority correctly stated that the case does not implicate the level of privacy chosen by Apple, but rather its decision to adopt a differentiated policy at the expense of its rivals.[106] Conversely, in evaluating whether to issue an interim measure against Apple, France's Autorité de la Concurrence solicited input from the domestic data-protection regulator (the Commission Nationale de L'Informatique et des Libertés, or CNIL), which *de facto* prevented the competition authority from ordering interim measures. Indeed, in the CNIL's view, the changes proposed by Apple could be of genuine benefit to both users and app publishers.[107] In particular, the ATT prompt would give users more control over their personal data by allowing them to make choices in a simple and informed manner,[108] and would allow app publishers to collect informed consent as required by the applicable regulation.

---

*Mobile Apps and Targeted Advertising: Competitive Effects of Data Exchange*, SSRN (2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4088166, finding that apps' inability to use tracking for advertising affects large apps to a greater degree, as they experience larger declines than smaller apps in download numbers and innovation.

[101] Autorité de la Concurrence, *supra* note 25.

[102] Bundeskartellamt, *supra* note 25.

[103] Autorità Garante della Concorrenza e del Mercato, *supra* note 25.

[104] Urząd Ochrony Konkurencji i Konsumentów, *supra* note 25.

[105] UK Competition and Markets Authority, *supra* note 25.

[106] Autorità Garante della Concorrenza e del Mercato, *supra* note 25, para. 47.

[107] Autorité de la Concurrence, *supra* note 25. In a similar vein, *see* Anzo DeGiulio, Hanoom Lee, & Eleanor Birrell, *"Ask App not to Track": The Effect of Opt-In Tracking Authorization on Mobile Privacy*, in EMERGING TECHNOLOGIES FOR AUTHORIZATION AND AUTHENTICATION (ANDREA SARACINO AND PAOLO MORI, eds.), Springer Cham (2022), 152, finding that opt-in authorizations are effective at enhancing data privacy. Conversely, *see* Chongwoo Choe, Noriaki Matsushima, & Shiva Shekhar, *The Bright Side of the GDPR: Welfare-Improving Privacy Management*, CESifo Working Paper No. 10617 (2023) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4558426, distinguishing among platforms' business models and arguing that, if the firm's revenue is largely usage-based rather than data-based, then both the firm's profit and consumer surplus increase after the GDPR's opt-in requirement, while if the firm's revenue is largely from data monetization, then the opt-in can reduce the firm's profit and consumer surplus.

[108] *See also* Catherine Armitage, Nick Botton, Louis Dejeu-Castang, & Laureline Lemoine, *Study on the Impact of Recent Developments in Digital Advertising on Privacy, Publishers and Advertisers*, AWO BELGIUM (2023) Report for the European Commission, 227, https://op.europa.eu/en/publication-detail/-/publication/8b950a43-a141-11ed-b508-01aa75ed71a1/language-en, arguing that consent prompts under the ATT policy are user-friendly, easily accessible, comprehensible and actionable; and UK Competition and Markets Authority, *supra* note 25, para.

It is worth noting, however, that while all the other competition authorities are investigating Apple's policy as a potential form of discriminatory self-preferencing, the French authority has initially evaluated whether the introduction of the ATT prompt would result in imposing unfair trading conditions or a supplementary obligation, in breach of Article 102(a) and (d) TFEU. The complaint's investigation on the merits of the case will allow the French authority to assess whether ATT does or does not result in a form of discrimination.

### B. Google's Privacy Sandbox

Concerns regarding the potential impact of privacy policies on digital-advertising competition and publishers' ability to generate revenue have also been against Google's proposals to remove third-party cookies and other functionalities from its Chrome browser. In particular, Google's Privacy Sandbox project would disable third-party cookies on the Chrome browser and Chromium browser engine, with the stated goal of better protecting consumer privacy. The project would replace those cookies with a new set of tools for targeting advertising and other functionalities. Therefore, similar to Apple's ATT policy, Google's planned privacy changes raise concerns about anticompetitive discrimination against rivals.

Indeed, in 2021, the European Commission initiated antitrust proceedings to investigate the effects of Google's privacy policies on online display advertising and online display advertising-intermediation markets. The inquiry focused on whether Google had violated EU competition rules by favoring—through a broad range of practices—its own online display advertising-technology services in the ad tech supply chain, to the detriment of competing providers of advertising-technology services, advertisers, and online publishers.[109] Notably, the Commission also examined restrictions on third parties' ability to access data about user identity or user behavior, which remained available to Google's own advertising-intermediation services, as well as Google's announced plans to cease making advertising identifiers available to third parties on Android mobile devices whenever a user opts out of personalized advertising.

The Commission declared that it would "take into account the need to protect user privacy, in accordance with EU laws in this respect," underscoring that "[c]ompetition law and data protection laws must work hand in hand to ensure that display advertising markets operate on a level playing field in which all market participants protect user privacy in the same manner."[110]

---

6.163, acknowledging the privacy benefits associated with the introduction of ATT, as it enhances users' control over their personal data and significantly improves developers' compliance with data-protection law.

[109] Press Release, *Commission Opens Investigation into Possible Anticompetitive Conduct by Google in the Online Advertising Technology Sector*, EUROPEAN COMMISSION (2021), https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3143.

[110] *Ibid.*

A similar investigation was launched that same year by the UK Competition and Markets Authority (CMA).[111] The CMA subsequently accepted commitments from Google designed to ensure consistent use of data by both third parties and Google's own digital-advertising businesses through the use of safeguards to support privacy without self-preferencing.[112] In considering how best to address legitimate privacy concerns without distorting competition, the CMA highlighted the relevance of the close partnership with the UK Information Commissioner's Office (ICO), the public body tasked with the enforcement of the Data Protection Act 2018, which is the UK's implementation of the GDPR.[113]

## IV. The Failure of the Integrated Approach

The call for integrating privacy into antitrust enforcement reflects the policy goal of curbing ever-increasing personal-data collection and processing by a few large online platforms, who monetize such data by selling targeted advertising. Toward this aim, competition and data-protection laws are described as synergistic, as the economic features of digital markets generate connections between market power and data power. Against this background, rather than relying on the GDPR, scholars and policymakers ask competition law to step in to address the perceived problem of data-protection authorities lacking capacity to address privacy concerns effectively, as well as the extreme difficulty of forbidding data accumulation under antitrust provisions. Therefore, rather than reflecting a natural connection, data-protection and competition laws are fundamentally *obtorto collo* complementary, as each are considered weak in isolation.

Four primary theories of harm have been advanced to bring antitrust and privacy issues together.[114]

According to the first theory, there is a close relationship between (the lack of) competition in digital markets and privacy violations. In a competitive market, this theory asserts, firms would compete to offer privacy-friendly products and services, but the economic features of digital markets strengthen gatekeepers' power, regardless of their willingness to deliver privacy-enhancing solutions.[115]

---

[111] Press Release, *Investigation into Google's 'Privacy Sandbox' Browser Changes*, UK COMPETITION AND MARKETS AUTHORITY (2021), https://www.gov.uk/cma-cases/investigation-into-googles-privacy-sandbox-browser-changes.

[112] *Ibid.*

[113] *See also* UK Competition and Markets Authority, *supra* note 25, para. 10.19, stating that "[w]orking closely with the ICO, the CMA now has a role in overseeing the development of Google's proposals for replacements to third-party cookies, so that they protect privacy without unduly restricting competition and harming consumers."

[114] Colangelo & Maggiolino, *supra* note 12.

[115] *See, e.g.*, UK Competition and Markets Authority, *supra* note 5; Antitrust Subcommittee Report, *supra* note 4; Pasquale, *supra* note 4; Harbour & Koslov, *supra* note 4.

The second theory centers on risks arising from potential "databases of intentions" and primarily invokes the role of merger control.[116] Under this view, mergers among companies that hold significant data assets require more stringent scrutiny, as such mergers would grant the new entity tools to better profile individuals and invade their privacy.

A further attempt to justify commingling antitrust and privacy relies on assessing the quality of products and services as privacy-friendly.[117] As consumer welfare is not solely dependent on prices and output, products and services viewed as not privacy-friendly or that intrude into users' privacy may be considered low-quality and therefore harm consumer welfare.

Finally, it has been argued that privacy policies could be applied by antitrust enforcers when they are implemented by dominant players that rely on data as a primary input of their products and services—*e.g.*, by forcing individuals to accept take-it-or-leave-it terms involving the unwanted collection and use of their data.[118]

This overview of EU antitrust proceedings, however, demonstrates that none of these four theories of harm has been successful and that the much-invoked integrated approach is more proclaimed than adopted in practice. Indeed, neither other NCAs nor the European Commission have ever shared the Bundeskartellamt's stance of considering a GDPR violation as a benchmark for finding a dominant firm's practice to be abusive. Further, in the context of merger analysis, the Commission has systematically stated that any privacy-related concerns resulting from data collection and processing are within the scope of the GDPR enforcement.

Even in Germany, the Bundeskartellamt's approach has been sufficiently controversial to spark a clash among courts and a request for clarification from the CJEU. The recent update of the GWB seems to confirm the limits of such an approach, as the new Section 19a provides an antitrust authority with a convenient shortcut to target Facebook-like data-accumulation strategies on grounds of market contestability—namely, prohibiting rivals' foreclosure rather than users' privacy exploitation.

In addition, these EU antitrust proceedings demonstrate that twisting competition-law enforcement may be counterproductive. Indeed, the growing phenomenon of digital platforms adopting privacy policies as justification for potentially anticompetitive conduct does not fit the narrative of the complementarity of antitrust and privacy.[119] Emerging as a byproduct of the *Facebook* investigation, the *Apple ATT* case illustrates the intrinsic tension between these areas of law, highlighting the urgency of determining how to strike a balance between conflicting interests. From this perspective, the *Facebook* and *Apple ATT* cases are

[116] Harbour, *supra* note 8.

[117] Antitrust Subcommittee Report, *supra* note 4; Stucke & Ezrachi, *supra* note 7.

[118] *See* Autorité de la Concurrence and Bundeskartellamt, *supra* note 33. *See also* Australian Competition & Consumer Commission, *supra* note 6; Slaughter, *supra* note 6.

[119] Douglas, *supra* note 12, 667.

two faces of the same coin. Each results from the strategic use of privacy in antitrust proceedings by both competition authorities and digital platforms, respectively.

Moreover, the French episode of *Apple ATT* shows that proposing cooperation between authorities is just rhetoric unfit to resolve these tensions. It is regularly affirmed that any tension between competition and data protection law "can be reconciled through careful consideration of the issues on a case-by-case basis, with consistent and appropriate application of competition and data protection law, and through continued close cooperation" between the authorities.[120] Nonetheless, in the French *Apple ATT* case, the data-protection regulator's intervention actually jeopardized the antitrust investigation, demonstrating how the different goals pursued under antitrust and privacy provisions may be irreconcilable in practice.

Finally, the EU's solution to alleged failures by antitrust and privacy regulators in addressing data accumulation in digital markets has ultimately been crafted outside the traditional competition-law framework and according to a regulation that resolves any potential conflict between competition and data-protection policy goals once and for all. Even the DMA, however, does not fully square with any of the aforementioned theories of harm, as it introduces a pure privacy exception.[121] Indeed, tackling data collection and processing by digital gatekeepers, Article 5(2) DMA prohibits personal-data accumulation strategies unless they are compliant with the GDPR—namely, unless users have been presented with the specific choice and given consent according to data-protection rules. Therefore, rather than providing criteria to evaluate case by case how to strike a balance among the interests involved, the DMA establishes competition-policy deference to privacy, finding that, where personal-data collection and processing by large online platforms are involved, privacy is the greater good.

### A. The CJEU's Judgment in *Meta*

Given this background, the CJEU's July 2023 judgment in *Meta* was much-awaited, representing the season finale of the German *Facebook* saga.[122]

The decision is in line with the opinion delivered by the Advocate General (AG) Athanasios Rantos.[123] As Rantos had argued, "conduct relating to data processing may breach competition rules even if it complies with the GDPR; conversely, unlawful conduct under

---

[120] *See*, *e.g.*, CMA-ICO Joint Statement, *supra* note 3, 26.

[121] At best, it may be argued that the DMA, *supra* note 61, Recitals 36 and 72, supports the theory of harm that, because of network effects and other structural features of digital markets, the strengthening of gatekeepers' power lowers their incentives to compete through offering high levels of privacy. These Recitals consider that ensuring data protection facilitates contestability of core platform services by avoiding the risks that gatekeepers raise barriers to entry and allow other undertakings to differentiate themselves better through the use of superior privacy guarantees.

[122] *Meta*, *supra* note 27.

[123] Opinion of the Advocate General Athanasios Rantos, 20 September 2022, Case C-252/21, EU:C:2022:704.

the GDPR does not automatically mean that it breaches competition rules."[124] Therefore, the lawfulness of conduct under antitrust provisions "is not apparent from its compliance or lack of compliance with the GDPR or other legal rules."[125] Further, according to well-settled CJEU principles, the antitrust assessment requires demonstrating that a dominant undertaking used means other than those within the scope of competition on the merits and, toward this aim, the court must take account of the circumstances of the case, including the relevant legal and economic context.[126] "In that respect, the compliance or non-compliance of that conduct with the provisions of the GDPR, not taken in isolation but considering all the circumstances of the case, may be a vital clue as to whether that conduct entails resorting to methods prevailing under merit-based competition."[127] Indeed, "access to personal data and the fact that it is possible to process such data have become a significant parameter of competition between undertakings in the digital economy. Therefore, excluding the rules on the protection of personal data from the legal framework to be taken into consideration by the competition authorities when examining an abuse of a dominant position would disregard the reality of this economic development and would be liable to undermine the effectiveness of competition law."[128]

It follows that. "in the context of the examination of an abuse of a dominant position by an undertaking on a particular market, it may be necessary for the competition authority of the Member State concerned also to examine whether that undertaking's conduct complies with rules other than those relating to competition law, such as the rules on the protection of personal data laid down by the GDPR."[129]

Rantos more explicitly distinguished the hypothesis under which an antitrust authority, when prosecuting a breach of competition provisions, rules "primarily" on an infringement of the GDPR from cases in which such evaluations are merely "incidental":

> [T]he examination of an abuse of a dominant position on the market may justify the interpretation, by a competition authority, of rules other than those relating to competition law, such as those of the GDPR, while specifying that such an examination is carried out in an incidental manner and is without

---

[124] *Ibid.*, fn 18.

[125] *Ibid.*, para. 23.

[126] *See* CJEU, 17 February 2011, Case C-52/09, *Konkurrensverket v. TeliaSonera Sverige AB,* EU:C:2011:83; 27 March 2012, Case C-209/10, *Post Danmark A/S v. Konkurrencerådet*, EU:C:2012:172; 6 October 2015, Case C-23/14, *Post Danmark A/S v. Konkurrencerådet* (*Post Danmark II*) EU:C:2015:651; 6 September 2017, Case C-413/14 P, *Intel v. Commission,* EU:C:2017:632; 30 January 2020, Case C-307/18, *Generics (UK) and Others v. Competition and Markets Authority,* EU:C:2020:52; 25 March 2021, Case C-152/19 P, *Deutsche Telekom v. Commission* (*Deutsche Telekom II*), EU:C:2021:238; 12 May 2022, Case C-377/20, *Servizio Elettrico Nazionale SpA v. Autorità Garante della Concorrenza e del Mercato*, EU:C:2022:379.

[127] *Meta*, *supra* note 27, para. 47, quoting Rantos, *supra* note 123, para. 23.

[128] *Meta*, *supra* note 27, para. 51.

[129] *Ibid.*, para. 48.

> prejudice to the application of that regulation by the competent supervisory authorities.[130]

Given the differing objectives of competition and data-protection law, however, where an antitrust authority identifies an infringement of the GDPR in the context of finding of abuse of a dominant position, it does not replace the data-protection supervisory authorities.[131] Therefore, when examining whether an undertaking's conduct is consistent with the GDPR, competition authorities are required to consult and cooperate sincerely with the competent data-protection authority in order to ensure consistent application of that regulation.[132] In addition, where the data-protection authority has ruled on the application of certain provisions of the GDPR with respect to the same practice or similar practices, the competition authority cannot deviate from that interpretation, although it remains free to draw its own conclusions from the perspective of applying competition law.[133]

While these principles are compelling, they do not appear conclusive in addressing the issue, for two main reasons.

First, as competition authorities have significant leeway in framing their investigations, it will be extremely difficult in practice to demonstrate that they are primarily—rather than incidentally—tackling a data-protection breach. In this regard, the German *Facebook* investigation represents an illustrative example. In the press release announcing the launch of the proceedings, the Bundeskartellamt stated that Facebook's terms and conditions violated data-protection law and may "also" be regarded as abuses of a dominant position.[134] Later in the press release, however, in a section concerning the preliminary assessment, the authority changed that perspective, asserting that Facebook's contractual terms were unfair, quite apart from any privacy infringement, and that, in assessing the competitive impact of such a strategy, it was "also" applying data-protection principles. Further, the Bundeskartellamt ascertained a privacy violation previously undetected by any data-protection authority. If the *Facebook* case fulfills both requirements of an incidental assessment of a privacy breach and sincere cooperation with the data-protection authority, it will be difficult to imagine any antitrust investigation not passing the bar.[135]

Second, the judgment only examines a scenario in which a GDPR infringement may occur, while not being useful to unraveling the very different situation in which the adoption of

---

[130] Rantos, *supra* note 123, para. 24.

[131] *Meta*, *supra* note 27, para. 49.

[132] *Ibid.*, paras. 52 and 54.

[133] *Ibid.*, para. 56. *See also* Rantos, *supra* note 120, paras. 29-30.

[134] *See* Giuseppe Colangelo & Mariateresa Maggiolino, *Data Accumulation and the Privacy-Antitrust Interface: Insights from the Facebook Case*, 8 INT. DATA PRIV. LAW 224 (2018).

[135] *See also* Peter Georg Picht, *CJEU on Facebook: GDPR Processing Justifications and Application Competence*, SSRN (2023) 3, https://ssrn.com/abstract=4521320, arguing that it is doubtful whether informal communications, as apparently held by the Bundeskartellamt with one of the competent GDPR authorities, sufficiently protect party rights.

a privacy-enhancing solution is invoked as justification for anticompetitive conduct. In that case, cooperation between competition and data-protection authorities has thus far proven to be a harbinger of new issues and conflicts, rather than a panacea for all of the problems.

Finally, the CJEU also addressed another crucial topic of the integration between antitrust and privacy—that being the meaning of "consent" under the GDPR, and especially the requirement of freedom of consent. Supporters of an integrated approach find the legal basis of the privacy/antitrust marriage in the GDPR to be pivotally centered on the role assigned to freely given consent.[136] Notably, they imagine that the GDPR provides the legal basis for a link between data power and market power by stating that, among other things, there is no freely given consent to personal-data processing where there is a "clear imbalance" between the data subject and the controller.[137] In this respect, if the controller holds a dominant position on the market, it is argued that such market power could lead to a clear imbalance in the sense described in the GDPR.

According to the CJEU, however, while it may create such an imbalance, the existence of a dominant position alone cannot, in principle, render the consent invalid.[138] Notably, the fact that the operator of an online social network holds a dominant position on the social-network market does not, as such, prevent users of that social network from validly giving their consent, within the meaning of the GDPR, to the processing of their personal data by that operator. Consequently, the validity of consent should be examined on a case-by-case basis.

Moreover, as observed by Rantos, this does not imply that for market power to be relevant for GDPR enforcement, it needs to be regarded as a dominant position within the meaning of competition law.[139] Therefore, the relationship between data-protection and competition law is not one of mutual respect. While a competition authority is required to cooperate with a data-protection regulator in the case of a privacy breach, and is bound by the interpretation the latter gives of the GDPR, the converse does not apply with regard to the notion of "clear imbalance" under the GDPR. Data-protection authorities are granted significant leeway to establish market power under the GDPR.[140]

---

[136] *See, e.g.*, Klaus Wiedemann, *Data Protection and Competition Law Enforcement in the Digital Economy: Why a Coherent and Consistent Approach is Necessary*, 52 IIC 915 (2021), arguing that the regulation of consent to the processing of personal data under the GDPR serves as a dogmatic link between data-protection and competition law, as the freedom to choose granted by the GDPR to users whose personal data are monetized shares significant overlaps with the economic freedom acknowledged in competition-law jurisprudence.

[137] GDPR, *supra* note 18, para. 74.

[138] *Meta*, *supra* note 27, paras. 147 and 149. *See also* Rantos, *supra* note 123, para. 75.

[139] Rantos, *supra* note 123, para. 75.

[140] For an analysis of the critical implications, *see* Alessia Sophia D'Amico, *Market Power and the GDPR: Can Consent Given to Dominant Companies Ever Be Freely Given?*, SSRN (2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4492347. *See also* Peter Georg Picht & Cédric Akeret, *Back to Stage One? – AG Rantos' Opinion in the Meta (Facebook) Case*, SSRN (2023), 4, https://ssrn.com/abstract=4414591, considering the question of whether GDPR market power can be not only

## V. Conclusion

The features of digital markets and the emergence of a few large online gatekeepers whose business models revolve around collecting and processing large amounts of data may suggest a link between market power and data power. Accordingly, scholars and policymakers have supported regulatory measures intended to promote data sharing and to empower individuals with more control over their personal data. From a different perspective, this also has led to the idea that competition and data-protection are intertwined and therefore require an integrated approach where, despite holding different objectives, antitrust enforcement should also protect privacy interests.

The integrationist movement claims that unity makes strength. According to this view, while competition and data-protection laws are, in isolation, considered unfit to safeguard their respective interests, the inclusion of privacy harms into antitrust assessments would allow competition authorities to better tackle data-accumulation strategies, and that the enforcement of antitrust rules would be more effective in ensuring data protection.

The purported complementarity, or even synergy, between competition and data-protection law appears, however, difficult to detect in practice. The only case in which a GDPR breach has been considered a proper legal basis for an antitrust intervention is the rather controversial Bundeskartellamt *Facebook* decision. Further, recent legislative initiatives that have introduced provisions clearly inspired by *Facebook* and essentially motivated by the aim of bypassing the traditional antitrust analysis (*e.g.*, Article 5(2)DMA and Section 19a GWB) confirm the failure of the integrationist narrative and awareness that it would be impossible to endorse the Bundeskartellamt's stance. Moreover, whether or not one would argue that the DMA represents a concrete and advanced attempt at integrating data-protection concerns in competition policy, it is worth pointing out that Article 5(2)DMA actually establishes antitrust deference toward privacy.

As if this were not enough, the idea of commingling antitrust and privacy has generated a significant side effect. As a reaction to *Facebook* and the DMA, some platforms have, indeed, adopted policy changes to restrict user-data tracking on their ecosystems in ways that undermine the effectiveness of rivals' targeted advertising. The strategic use of privacy as a business justification to pursue anticompetitive advantages testifies once again to the tension between these fields of law. Further, as shown by the French *Apple ATT* investigation, the call for close cooperation between the authorities is often just a useless and rhetorical expedient.

The proposal to integrate competition and data-protection law in digital markets has been submitted as a much-needed boost to strengthen antitrust enforcement against gatekeepers and their data strategies. Moving away from pure efficiency-oriented assessments to embrace broader social interests, advocates claim, would help ensure more aggressive and

---

less than competition-law dominance but also of a different nature—*e.g.*, based on a set of parameters that would not suffice, as such, to establish market power in the competition-law sense.

effective antitrust enforcement. Including privacy harms in antitrust proceedings turns out, instead, to be a potential curse for competition authorities, providing the major digital players with an opportunity for regulatory gaming to undermine antitrust enforcement.

This should serve as a cautionary tale about the risks of twisting rules to achieve policy outcomes and the importance of respecting the principles and scope of different areas of law.