US-China Law Review, June 2025, Vol. 22, No. 6, 259-277
doi:10.17265/1548-6605/2025.06.001

Does Competing on Privacy Terms Foster Competition? The Truth of Privacy Exploitation

HE Qing
Beijing University of Posts and Telecommunications, Beijing, China

Based on the proposition that platforms compete on privacy terms and thus prompt privacy-sensitive users to switch to competing platforms with better privacy policies and increase competition, this paper argues that firms compete on privacy terms to prevent consumers from switching by foreclosing competitors, e.g., denial of access to data, while increasing monopoly profits by privacy violation or shifting costs to consumers, which constitutes "privacy exploitation". Based on the "privacy-as-quality" theory, privacy is a substitute of quality as a measurement of consumer welfare in most antitrust cases, but the reduced privacy could be offset by other positive qualities. Thus, based on case studies and the concepts of the endowment effect and loss aversion from behavioral economics, this paper analyzes the positive effect of "anticipation for privacy" on buyers' demand to explain how the exploitation can exist on both the producer's side and the consumer's side, if we treat the transfer of personal data as a transfer of privacy risk. This paper contributes to the debate on the role of privacy in competition analysis, as well as to the theories of harm literature.

Keywords: competition, privacy, exploitation, exclusion, digital platform, theories of harm, behavioral economics

Introduction

With the increasing commercialization of personal data, data privacy is characterized as a parameter of non-price competition in the digital era (Esayas, 2019), and the negative effects on privacy, relating to excessive data extraction, personalized pricing, and unfair trading conditions, could be interpreted as a type of exploitative harm under competition law (Economides & Lianos, 2021; Condorelli & Padilla, 2021; Douglas, 2021). Large companies are accused of exploitative abuse of power in different forms, but the harm to consumers may be offset by positive effects (Graef & van der Sloot, 2022). The claims of exploitative harm are challenged, particularly in cases where the company raises the notice-and-choice defense, privacy-protection defense, high-quality services defense, or innovation defense.

In such settings, the U.S. House Judiciary Committee published a report (2022) on competition in the digital marketplace in July 2022, which proposed the notion of "privacy exploitation" by invoking an elaboration from Professor Howard Shelanski: "One measure of a platform's market power is the extent to which it can engage in [privacy exploitation] without some benefit to consumers that offsets their reduced privacy and still retain users".

HE Qing, Doctor, assistant professor, Law Faculty, School of Humanities, Beijing University of Posts and Telecommunications, Beijing, China.

However, without further exploration of this notion, it is difficult for the plaintiff to prove consumer harm.[1] For the companies that offer "free services", the plaintiff needs to find substitutes of higher price to establish a reduction in consumer welfare, such as reduced quality of services, including fewer privacy protections (e.g., FTC v. Facebook, 2020).

On the other hand, it is a challenge to prove that privacy violations give rise to relevant competitive damage. Unlike the justification of privacy protection for "walled gardens", which the platform can take advantage of, the causal relationship between privacy violation and anticompetitive effects is controversial. In 2019, Facebook was accused of excessive data collection without users' additional consent, which constituted an abuse of dominance in violation of the German Act against Restraints of Competition (GWB) (Facebook v. Bundeskartellamt). However, the causality between privacy violation and anticompetitive effects is not established *per se*, and it remains unclear whether the willful maintenance of market power, based on data advantage, can be determined by privacy intrusion or a shifting of costs in relation to privacy protection.

Nevertheless, improper use of personal data has raised concerns about restricting competition, even for those who are well known for their "privacy-preserving policies". For example, Google was alleged to illegally collect and use the user data to train AI (artificial intelligence) products in violation of privacy laws and the unfair competition law in a recent class action suit.[2] Google has not been sued for its privacy policy despite the controversies over its "sandbox proposal", until data training for AI models becomes a concern for law makers.

Therefore, this paper further explores how privacy exploitation is connected to a violation of antitrust in the digital era. The main contributions of this paper are:

First, this study collects 24 data-competition intersected cases against four major tech-companies—Facebook, Apple, Amazon, Google—all of which involve personal data collection or processing, removes the substantially replicated cases, for example, multiple Washington lawsuits were filed against Amazon for similar facts and grounds—excluding third-party sellers by self-preferencing strategies,[3] and removes the cases where the antitrust claims were dismissed by the courts or the authorities.[4] I generalize 15 types of conducts/strategies from these cases that may raise competition concerns, and I group them into three stages—data extraction, anticompetitive conducts toward trading partners, and exploitative conducts toward final consumers. Figure 1 shows that most cases put more emphasis on Stages 1 and 2, but the number of exploitative abuse cases (3rd step) is increasing recently.

---

[1] For example, the online ad industry in France had ever sought interim measures to stymie Apple's new App Tracking Transparency feature in 2021, by claiming it amounts to an antitrust violation to the prejudice of third-party advertisers, but the French Competition Authority rejected the requests (Meyer, 2021).

[2] J. L. et al. v. Alphabet Inc. et al., 3:23-cv-03440 (N.D. Cal. 2023).

[3] See, e.g., Joyce v. Amazon, Inc. et al., No. 2:22-cv-0617 (W.D. Wash. 2022); FTC v. Amazon.com, Inc., No. 2:23-cv-1495-JHC (W.D. Wash. 2023); In re Amazon.com S'holder Derivative Litig., No. C22-0559-JCC (W.D. Wash. 2024).

[4] See, e.g., CMA (UK), Case ME 7100/24 Amazon/Anthropic, decision of 27 September 2024; CMA (UK), Case ME/7012/22, Amazon/iRobot, decision of 24 July 2023; Roberta Ann K.W. Wong Leung Revocable Trust U/A Dated 03/09/2018 v. Amazon.Com, Inc., C.A. No. 2023-1251-BWD (Del. Ch. 2024).

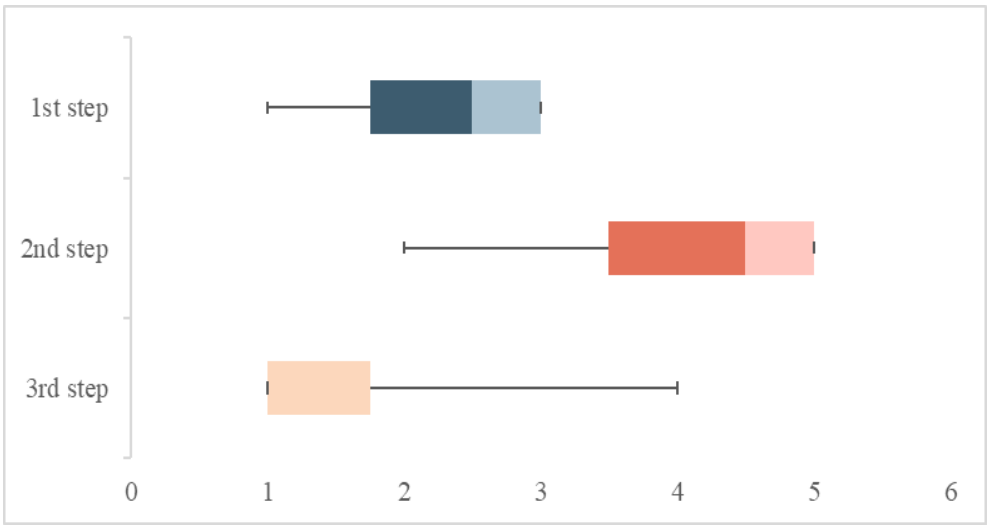


Figure 1. 24 data-competition intersected cases against Facebook, Apple, Amazon, Google.

However, questions such as whether it is a concern for competition law if the reductions in the privacy of consumers are compensated by benefits to producers remain unanswered. This study fills this gap and reveals that firms compete on privacy terms to prevent consumers from switching by foreclosing competitors (e.g., denial of access to data), while increasing monopoly profits through privacy violations or shifting costs to consumers in a deceptive or coercive manner, without compensation to producers.

Second, this study develops the theory of harm based on privacy exploitation by invoking the concepts of the endowment effect and loss aversion from behavioral economics, to explain why platforms tend to collect user data by endorsing privacy-friendly policies—the positive effect of privacy expectations on users' demand.

Third, this paper groups privacy exploitation into three types in Section 7, and demonstrates how privacy exploitation is implemented in practice.

The paper is structured as follows. Section 2 briefly reviews the development of the theory of harm based on privacy exploitation. Section 3 discusses the controversies over the transfer of personal data and suggests that we can treat the transfer of personal data as a transfer of privacy risk, and that the data subject retains control over his/her data even if it is transferred. Section 4 describes the research gap—how we can prove the harm of privacy exploitation to consumers by using the idea of risk-transfer. Section 5 presents the proof methods; Section 6 presents the findings.

Theory of Harm Based on Privacy Exploitation

This paper explores whether and to what extent privacy concerns can stand alone as an independent antitrust standard of review—by linking to traditional competition law theories of harm, such as leveraging and monopoly maintenance—willful maintenance of market power through improper data processing may motivate competition law intervention.

EU competition law focuses on distributive justice, particularly emphasizing the position of "consumers" (Economides & Lianos, 2021), but how can we determine the "justice" when a group of people are worse off and the others are better off? For example, the controversies over the harms of price discrimination to consumers

have often focused on the market expansion effect on consumers with a low willingness to pay, which is weighted against the welfare losses for consumers with high willingness to pay.

However, in the digital era, technological development, such as accurate algorithms and AI assistants (e.g., Apple's Siri), has increased the risk of "digital" consumer manipulation, and can adapt to market changes more quickly and accurately. Thus, the profits gained through price discrimination may no longer be redistributed to consumers, whereas the implementation of such "AI-enabled" price discrimination is costly for data controllers (Li et al., 2023), which may prompt them to "shift risk and costs to weaker parties".[5] In this respect, it is doubtful that consumers can still be protected "just by stopping powerful companies from driving their rivals out of the market" (Vestager, 2016).

In accordance with the changing times, the traditional theories of harm for competition law have been challenged for the first time since the 1970s (Graef & van der Sloot, 2022); claims of exploitative abuse in digital markets, relating to excessive data extraction, personalized pricing and excessive pricing have, albeit controversially, started to predominate over exclusionary concerns in antitrust cases (Economides & Lianos, 2021; Condorelli & Padilla, 2021; Douglas, 2021), and the exploitative theories of harm have even expanded to include the exploitation of businesses that are customers of online platforms, not final consumers (OECD, 2020).

Compared with exclusionary effects of privacy-related restrictions, the assessment of exploitative effects also requires the performance of a balance of interests, except for two differences:

(1) Technological advancement has strengthened the adverse impact of exploitative conduct (e.g., AI-enabled price discrimination) in contrast with its positive impact;

(2) Access to personal data with commercial value is essential for competition, which contributes to a direct impact of data processing on consumers' interests (including privacy interests).

As a result, the grounds for finding an abuse have shifted from economic dependence and asymmetrical bargaining power between market players, to economic dependence (lock-in effect) and asymmetrical bargaining power between the dominant digital platforms and the users.

Controversies Over the Transfer of Personal Data

The Legal Foundation for the Alienability of Personal Data

Privacy exploitation is related to, but more than an invasion of, privacy. The theories of harm for privacy law are moving from torts that require proof of privacy harm toward exante regulation. Some privacy statutes, such as the California Consumer Privacy Act of 2018 (CCPA) and the General Data Protection Regulation (GDPR), to a large extent, identify harm through unlawful conduct regardless of whether the data subject is harmed (Cofone, 2021).

Such privacy concerns may motivate competition law intervention due to the harvesting of personal data. Professor Howard Shelanski interpreted privacy exploitation as a behavior of a platform that might invest little in data protection and use the information in ways that benefit the firm but that consumers do not like, and the

[5] European Commission, "Staff working document, impact assessment, initiative to improve the food supply chain (unfair trading practices), accompanying the document, proposal for a directive on unfair trading practices in business-to-business relationships in the food supply chain" SWD (2018) 92 final, at 11.

extent to which the platform engages in such behavior and still retains users indicates the platform's market power (Shelanski, 2013). To explore this notion further, the paper interprets privacy exploitation as an abuse of market power via data extraction and unfair contract terms.

However, it is doubtful that antitrust law is the best legal instrument for addressing exploitative practices harming consumers in the form of data extraction and unfair contract terms (Economides & Lianos, 2021; Graef & van der Sloot, 2022; Morozovaite, 2023). First, there is controversy over whether such practices as excessive data collection and personalized pricing should be subject to antitrust liability for an abuse of dominance. For example, by implementing price discrimination, firms can charge those consumers who can afford to pay higher prices and can thus serve consumers who cannot afford by charging them a lower price, and the output is expanded accordingly (OECD, 2018; Steinberg, 2019).

Second, an individual may benefit from higher-quality services (e.g., better-targeted advertising) on the basis of the data harvested (OECD, 2015; Economides & Lianos, 2021; Graef & van der Sloot, 2022). Individual privacy here is incorporated into longstanding antitrust analytical frameworks, which recognize quality as a basic parameter for competition, i.e., the "privacy-as-quality" theory (Stucke, 2018; Douglas, 2021). Accordingly, a reduction in privacy would account for a decline in the quality of products or services, which is inevitably weighted against the positive effects on other aspects of quality or innovation in the market.

The balance of hardships is essentially dependent on the nature of the alienable personal data. Are personal data transferred as a non-material interest, such as an object of fundamental right (e.g., the right to informational self-determination), or as a material interest, such as property interest?

If we take the former perspective, we need to attach importance to the consent mechanism and its potential effects on data-driven competition; if we take the latter perspective, we need to justify the grant of access to user data in favor of competitors, which concerns how we deal with trade secrets (legitimate proprietary interest in a broader sense[6]) pertaining to personal data. This section elaborates on these questions.

Transferred as a non-material interest.

(1) Personal data as an object of fundamental right. In Europe, the concept of the right to data protection under data protection laws focuses on "informational self-determination", namely, the individual is able to freely decide how to live his (her) life. The GDPR, for example, develops the individual right to data protection for the purpose of preventing potential harm to the essence of a fundamental right or of the constitutional order.[7] In accordance with legislation, some commentators state that the right to data protection aims to safeguard the personalities of data subjects, not their property (Rodotà, 2009; Purtova, 2017).

Therefore, if personal data are transferred as an object of fundamental right, we need to assess how the validity of a user's consent might affect data-driven competition. Taking the German Facebook case[8] as an example. The German Competition Authority (FCO) prohibited Facebook (Meta) from processing data on the

[6] In the employment sector, the courts in some jurisdictions have held that trade secrets, confidential information, and customer lists are employer's *legitimate proprietary interests*, which include *contact information, the clients' needs or preferences and the rates the clients are willing to pay* (Pulver Crawford Munroe LLP, 2022).

[7] Art. 7 of the Charter of Fundamental Rights of the European Union (EUCFR) provides that everyone has "right to respect for his private and family life, his home and his correspondence"; Art. 8 EUCFR provides that everyone has "the right to the protection of personal data concerning him or her".

[8] Case C-252/21, Facebook Inc. and Others v. Bundeskartellamt OJ C 320, 09.08.2021.

grounds that the data processing in question did not comply with the GDPR, and constituted an abuse of dominance in the social media market in Germany. However, it is controversial whether national competition authorities are entitled to assess compliance with the GDPR. In response to this question, the Advocate General at the Court of Justice of the European Union (CJEU) issued his opinion that the compliance or non-compliance of the conduct at issue with the provisions of the GDPR may be a vital clue as to whether it amounts to a breach of competition rules, particularly whether users have given *free and effective consent* to the processing of their personal data.

(2) "Privacy-as-quality" theory. In addition to the fundamental right perspective, privacy is also recognized as a quality parameter of *non-price* competition according to "privacy-as-quality" theory and in some cases (e.g., the Facebook/WhatsApp merger[9]). Concerning the relationship between privacy degradation and negative effects on parameters other than the price of products, I take the perspective of deprivation of free choice (Swire, 2007), which cannot be converted into a price that a user pays in return for receiving free online services. Without unjustified practices to maintain a data advantage and eliminate consumer choice, merely privacy degradation will not suffice to find exploitative harm under competition law.[10] The question of whether consent is freely given on the basis of free choice matters in this regard.

Transferred as a material interest. The material interest attribute of personal data has been described in some privacy laws. For example, the California Privacy Rights Act of 2020 (CPRA) SEC.2.I states as follows: "Some companies that do not charge consumers a fee subsidize these services by *monetizing consumers' personal information*. Consumers should have the information and tools necessary to limit the use of their information to non-invasive, pro-privacy advertising…"

It follows that we may alternatively introduce some property rights, such as data ownership and trade secrets, to protect data subjects' rights as well as the legitimate private interest of data controllers. The economic value embedded in personal data can thus be monetized.

However, from the competition law perspective, the direct analogy of excessive data-collection with excessive prices is difficult to make. The exploitation effects that data extraction exerts on consumers do not lead to loss of money/wealth (including personal data) once they have been exploited, whereas excessive pricing cases do (Haucap, 2019; Kerber & Zolna, 2022).

Hence, we need to reconsider if we obtain the wrong idea about "paying" with personal data in exchange for services, and the rationale behind the trade secret mechanism designed for data protection.

(1) Personal data as a price paid for services. Given the ever-changing scenarios where personal data are used, measuring and estimating the value being generated is difficult (OECD, 2013). However, it does not seem to be a major concern for "monetizing" consumers' personal data. Tech companies have valued personal data in real-world dollars. For example, Meta (referred to as "Facebook") has offered to pay individuals for their voice recordings (Peters, 2020).

On the one hand, from the competition law perspective, the act of data collection might amount to an exploitative abuse where "producers take valuable consumer information without payment or without payment

[9] Case COMP/M.7217, Facebook/WhatsApp decision of 3 Oct. 2014.

[10] Some commentators argue that more data about users mean better targeted ads; the reductions in privacy of consumers are thus compensated by benefits to advertisers, which is not a concern for competition law (Manne & Sperry, 2015).

at a competitive price" (Patterson, 2017). However, if the company offers its services ("paying" with services) on the condition of obtaining personal data ("bundling of consent" requirement), it is difficult to determine what constitutes "excessive" for excessive data collection and therefore exploitative.

On the other hand, from the economics perspective, users have the possibility to share their own data with third parties by exercising data portability rights, for instance, and would be in favor of suppressing data output, unless the controller holds an exclusive right or license to the user data. In this case, monopsony may not reduce welfare (Haucap, 2019; Economides & Lianos, 2021).

Based on the considerations above, I present two arguments concerning why trading personal data for platform services should be seen as a problematic way to "monetize" personal data:

Unlike the property interest contained in intellectual property rights, the rule of fair use is not applicable in this case, as data subjects retain rights, for example, "ownership-similar rights", which allows for ongoing use restrictions as opposed to permanent transfers, over that information under the purpose limitation principle (Cofone, 2021). However, the data protection obligation will probably provide data controllers with objective ground for justifying the denial of granting access to a potential competitor, that is, the privacy-protection defense.[11]

With regard to the platform's "bundling of consent" requirement, some regulations have granted consumers a minimum standard of choice over the use of their personal data (e.g., German competition law, the EU Digital Markets Act). Commentators also argue that gatekeepers should offer consumers a choice that they can pay for services with a monetary fee in place of personal data (Kerber & Zolna, 2022). However, the idea of "trading personal data for services" will nevertheless lead people into a trap—the core service of a platform, such as online search of a search engine, is paid for by personal data, and then the techniques applied to individual privacy protection are an added value to its core service, which may constitute an "increased" quality that could be balanced against the loss of profit of some downstream competitors (e.g., adtech vendors).

(2) Personal data as a trade secret controlled by a platform. The personal data may fall within the scope of the private interest of controllers in cases where it is a part of protected trade secrets or intellectual property rights. According to the right of access under the GDPR, a data subject's right to obtain a copy is restricted only if such a right adversely affects the rights and freedoms of others (Article 15(4) GDPR), namely, if providing a copy of the data would harm *trade secrets* or intellectual property rights (Recital 63 GDPR).

The EU's Trade Secrets Directive[12] contains an expansive notion of trade secrets (Article 2(1)):

> "Trade secret" means information which meets all of the following requirements:
>
> 1. It is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
>
> 2. It has commercial value because it is secret;
>
> 3. It has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

[11] For example, in hiQ v. LinkedIn case, hiQ scrapes information that LinkedIn users have included on public LinkedIn profiles; LinkedIn employed blocking techniques to prevent hiQ's automated data collection methods, claiming that it has its members' privacy interests, in violation of California's Unfair Competition Law. See hiQ Labs, Inc. v. LinkedIn Corp., D.C. No.3:17-cv-03301-EMC (9th Cir. Apr. 18, 2022).

[12] Directive 2016/943 of the European Parliament and of the Council of 8 June 2016 on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use and Disclosure, OJ L [2016] 157/1.

Among others, the interpretation of "commercial value" focuses on the damage caused to the holder with regard to its scientific and technical potential, business or financial interests, strategic positions or *ability to compete*.

It has been widely accepted that data advantages could be essential for competition (Condorelli & Padilla, 2021). However, when consumers contribute to this advantage through their own data, it is supposed to entitle them to the economic value that comes out of their own "raw materials", compared with those data harvesters. Thus, when the trade secret embraces personal data, just as some commentators have argued, the balancing always concerns the freedom (data protection) and the obligations that the controller fulfills to protect it (Gellert & Gutwirth, 2013). On this ground, I present two arguments concerning why the notion of a "secret" should be distinguished from the traditional view of a trade secret when interfacing personal data:

(1) The secrecy embedded in a trade secret originates from "privacy", a private interest of the individual, rather than the controller's property interest, as long as the secret is associated with personal information. Secrecy can be interpreted as an obligation of privacy protection that the controller should fulfill, and its legitimate private interest based on such a trade secret manifests itself by incorporating such an obligation.

(2) Given the significance of privacy for competition, the "newcomer" may prevail for its "privacy flag". Facebook, for example, put forward its "superior" privacy-centered offer, as it initially entered the social media market in 2007, and users have the opt-out option to curb user tracking, as opposed to the "bundling of consent" requirement a decade later. The announcement of "keeping user data secret" did work—the incumbents at the time, such as Yahoo and MySpace, were forced out of the market (Srinivasan, 2019). Thus, the platform operator should show respect for consumers who have privacy preferences; the trade secret in relation to privacy, which serves as a competitive advantage, should be protected on a privacy-preserving premise.

A New Thought: Transfer of Privacy Risk and Related Costs

Consumers who provide their personal data expect performance of a data-protection obligation, rather than a refund. It is out of question that we pay a price for the "purchase" of personal data if we analogize the personal data to property. However, what if we treat the transfer of personal data as a transfer of privacy risk, and if the data subject retains control over his/her data even if it is transferred?[13]

The individual's privacy risk has largely increased in the digital age, and too much information about consumers, including information about other consumers, makes protecting one's privacy costly (Esayas, 2017) to the extent that even the data subject can hardly afford. Therefore, given the commercial value of personal data, we can consider the feasibility of entrusting others (e.g., platform operators) with the responsibility of preserving the data on their behalf, which can reduce the cost of privacy protection for the data subject by transferring the privacy risk and increase the profits from data processing for the controllers. However, it will incur a cost for holding the data, on the premise that the holder (controller) bears the privacy risk.

[13] As a general rule for the passing of risk in the international sale of goods, for example, the seller who has satisfied his obligation to deliver goods or documents will cease to bear the risk of loss or damage. This finds analogy in the transfer of personal data, but the difference is that the data subject's rights over his/her data, including property interest, are not transferred at the same time.

As a consequence, the privacy exploitation issue will arise if the controller passes the costs on to the consumer or does not actually fulfill the privacy-preserving obligation; the harms of privacy exploitation to the consumers are decided by the performance of the digital platform's privacy protection, which I will discuss in the following part.

How Privacy Exploitation Can Harm Consumers

Rationale: Compensation for Consumers' Loss of Benefit

It is costly to preserve a fair amount of personal data with desirable privacy safeguards. If we treat the transfer of personal data as a transfer of privacy risk, we also entail the controller bearing a privacy-preserving cost. As Professor Howard Shelanski noted, if data processing entails a cost, the firm's decision not to undertake beneficial processing reduces marginal costs, and theoretically, the consumer should be compensated for the reduced benefit (Shelanski, 2013).

However, such a loss cannot be simply offset by a lower priced service because the firm is obligated to preserve the data on the consumers' behalf, although the compensation required for the loss can be converted into an estimated monetary value to explain that the exploitation effects of data extraction do lead to consumers' loss of wealth. Put simply, consumers' loss of benefit and the required compensation provide a legal foundation for recognizing exploitative harm.

Therefore, the harms of privacy exploitation to consumers are determined by the performance of the digital platform's privacy protection, and whether a digital platform has fulfilled the privacy protection obligation can be converted into an inquiry about whether the platform has borne the costs in relation to privacy protection, or whether the platform has passed them to consumers.

Research Gaps

In essence, the challenges of applying exploitative abuse provisions to privacy-related unfair practices originate from the controversy over privacy harm and more data collection; data extraction leads to a reduction in privacy (by introducing targeted ads), and thus prompts privacy-sensitive users to switch to competing platforms, and prevents controllers from collecting more data (Manne & Sperry, 2015), increasing interbrand competition, based on a similar rationale in comparison with the privacy-protection defense raised in the Epic Games v. Apple case (2023)—users' switching behavior pressures firms to compete on better privacy terms.

My argument is that firms compete on privacy terms to prevent consumers from switching by foreclosing competitors while increasing monopoly profits through privacy violation or shifting costs to consumers, even though the service is available free of charge for consumers.

In practice, competition authorities and courts have never overlooked the exclusionary nature of platform data accumulation but have difficulties finding antitrust violations even when recognizing unfairness. In the German Facebook case, the court confirmed that considerable barriers exist for network users who would like to switch providers, and such a data advantage is financed by advertising and thus secures Facebook's market position. However, as mentioned above, the harm to consumers could be offset by positive effects; defenses, including privacy-protection defenses and high-quality service defenses, make it easy for the platform to win the case. Hence, further research on how we can prove the harm of privacy exploitation to consumers is needed.

Method

Case Studies

Facebook: Representative of "free services".

Data have been identified as a major contributor to market entry in the digital era. The "privacy flag" helped Facebook squeeze out its rivals at an early stage, as previously discussed, and the merger for growing a user base contributed to its data accumulation. The Facebook/WhatsApp merger (2014)[14] in the EU suggests that such a merger, a data concentration strategy, is a "designed" monopolization by virtue of misleading privacy exploitation; Facebook established an automated match between Facebook users' accounts and WhatsApp users' accounts, against its assurance to the Commission.[15] Facebook centralizes user data in a deceptive and misleading manner to enhance ad targeting and thus strengthen its position in the online advertising market while requiring counterparties (publishers) to submit data on their readership, which can help Facebook gain a competitive advantage over publishers to compete for advertisers' purchases.[16]

In 2019, the Bundeskartellamt prohibited Facebook from combining user data from different sources, and the Federal Court of Justice confirmed its decision in 2020, finding that Facebook processed user data that were collected online outside the Facebook platform without users' consent, which constituted an abuse of dominance (Bundeskartellamt, 2020).

In 2020, Facebook was accused of monopolizing the personal social networking (PSN) market in the U.S. (FTC v. Facebook, 2020). Notably, the court accepted the FTC's allegations in its repleaded complaint that a lack of quality, privacy, or other non-price features that result from Facebook's acquisitions of Instagram (in 2012) and WhatsApp (in 2014) could qualify as a type of consumer harm and constitute unlawful monopoly maintenance under Section 2 of the Sherman Act, but did not permit the allegation of "conditional dealing practices" with regard to Facebook's interoperability policies—denial of granting application programming interface (API) access to its competitors—to move forward.[17] Put simply, the practice that should be subject to antitrust liability is Facebook's willful maintenance of market power via anticompetitive acquisitions, rather than excessive/exploitative practices, or refusal-to-deal practices.[18]

Concerning the legality of the contested acquisitions, the court confirmed that Facebook tends to destroy competition via means other than competition—the acquisitions can constitute one such "means", and the consequence is decreased service quality and privacy protection. The assessments focused on the acquisitions and their effects on quality and privacy, rather than their contribution to excessive data extraction.

Apple: Representative of "privacy-friendly services".

Apple started an ad campaign in 2019, purportedly reiterating the company's stance on user privacy protection. The App Tracking Transparency feature (hereinafter "ATT"), in particular, requires third-party apps

---

[14] Case COMP/M.7217, Facebook/WhatsApp decision of 3 Oct. 2014.

[15] Case COMP/M.8228, Facebook/WhatsApp decision of 17 May 2017, http://ec.europa.eu/competition/mergers/cases/decisions/m8228_493_3.pdf (accessed on 27 January 2025).

[16] The platforms have also imposed oppressive contractual terms, such as forced arbitration clauses and class action waivers that provide the trading partners with fewer procedural rights (Khan, 2020).

[17] FTC v. Facebook (Meta), Doc.90 Case 1:20-cv-03590-JEB (D.D.C. 2022).

[18] The concept of exploitation does not even exist in US antitrust law, as laid down in the Sherman Act. Instead, Section 5 of the Federal Trade Commission Act is used to intervene against the "unfair methods of competition", which are a hybrid between unfair competition and consumer concerns (Graef & van der Sloot, 2022).

to obtain users' explicit consent to collect their advertising identifier data in response to the prejudices of independent advertisers (Meyer, 2021). However, New York citizen and iPhone 13 owner Elliot Libman recently filed a class action lawsuit (Libman v. Apple, 2023[19]), accusing Apple of collecting and monetizing their private information without their consent despite privacy promises, in violation of the California Invasion of Privacy Act, California's Unfair Competition Law, and so forth.[20]

While the lawsuit focuses on privacy violations, the "Apple One Bundles" plan launched by Apple in 2020 is popular among Apple users. The plan bundles the major Apple services, including iCloud, Apple Music, Apple Arcade, etc., into one monthly payment, which is cheaper than that of separate subscriptions. It appears to be lawful to implement the plan to the detriment of its downstream competitors (e.g., Spotify in the market of music streaming services) because, on the surface, it causes no direct damage to consumers because it is more convenient and cheaper than subscribing individually. However, consumers can use YouTube and Spotify for free, although it has ads and is limited to online streaming (Morales, 2023). The costs incurred as a result of privacy protection have been passed on to consumers, in ways not easily detectable, by data extraction in conjunction with the exclusion of competitors.

In addition to privacy violations and cost-shifting concerns, in 2020, the case of Epic Games v. Apple[21] placed Apple's App Store tax" in the spotlight. The Apple removed Fortnite, a video game developed by the complainant, from the App Store, as it refused to use Apple's in-app payment system and paid the 30% commission, barring developers from telling users about other payment methods (also known as the "anti-steering" policy[22]), and was therefore accused of monopolization and illegal tying. Thus, the exploitation issue is connected with exclusionary conduct in a way.

Amazon: Membership strategy that increases customer spending.

Platforms may use membership *under a lower-price appearance* to increase customer spending. Amazon was alleged to "trick" and "mislead" consumers into subscribing to Amazon Prime in a recent case brought by the U.S. FTC.[23] The commentator revealed that Amazon Prime members spend more on its platform than nonprime members do (Khan, 2017). Prime members who are supposed to benefit from discounted products and services are treated with personalized coupons (Khan, 2017) and increasingly expensive membership fees; however, the cancellation of the memberships is difficult—Amazon fails to *disclose material facts* when signing them up for prime-free trials (FTC v. Amazon, 2023).

The data at issue play a critical role in obtaining excessive profits for the company from both the consumer's side and the producer's side. On the one hand, Amazon's most lucrative advertisements are shown in connection

[19] In re Apple Data Privacy Litigation, 5:22-cv-07069-EJD (N.D. Cal. 2023).

[20] Before the lawsuit, an ad industry trade group that includes Meta and Google as members has accused Apple of "cynicism and hypocrisy" over its iPhone anti-tracking policy, alleging that Apple tracks its users without accountability while requiring third-party apps to ask users for permission (Fathi, 2023).

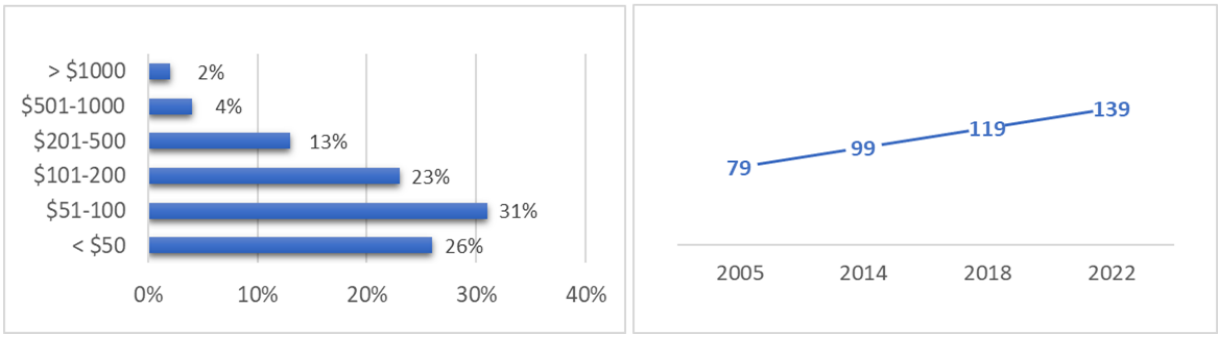
[21] Epic Games, Inc. v. Apple, Inc., No. 4:20-cv-05640-YGR (N.D. Cal. Aug. 13, 2020); Epic Games, Inc. v. Apple, Inc., No. 21-16506 (9th Cir. 2023).

[22] In June 2020, the EU Commission brought an antitrust investigation into Apple's rules, the anti-steering policy in particular, for app developers on the distribution of apps via the App Store. See https://ec.europa.eu/commission/presscorner/detail/en/ip_23_1217 (accessed on 30 June 2025). Recently, the Commission fined Apple over €1.8 billion over abusive App store rules for music streaming providers. See https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_24_1161/IP_24_1161_EN.pdf (accessed on 30 June 2025).

[23] FTC v. Amazon.com Inc., 2:23-cv-01495 (W.D. Wash. 2023).

with specific customer search queries that lead to Search Results Pages (FTC v. Amazon, 2023). On the other hand, Amazon was alleged to charge third-party sellers a non-negotiable 30% commission on every product sold on the site (Bira v. Amazon, 2024). However, Amazon misled users about their ability to delete their personal data, including voice recordings and geolocation information, in violation of privacy laws (United States v. Amazon, 2023).

Figure 2 presents (i) the average amount that Prime members spend per month on Amazon according to a 2021 survey and (ii) the change in its members' Prime cost. It has been reported that Amazon Prime members spend an average of $1,400 annually, whereas nonprime members spend $600 annually.



(a) (b)

Figure 2. Amazon's membership strategy. (a) Member spending (per month). Data retrieved from Statista: Average monthly spending of Prime members on Amazon in the U.S. in 2021, by spending range. (b) Prime cost (since 2005).

Behavioral Economics Perspective: The Impact of Anticipation for Privacy and Volumes of Data as an Advantage Indicator

This section further explains the interactions among the anticipation for privacy ("a^P"), buyers' demand ("D^B"), and volumes of data ("V_d"), by introducing cost of holding data ("c^H") and the concepts of the endowment effect and loss aversion from behavioral economics. Suppose that c^H increases with the "time" index σ: $c^H = c_0^H \sigma$ $(c_0^H > 0)$,[24] and there is a positive relationship between the anticipation for privacy and buyers' demand.

In alignment with the court's viewpoint that platforms compete on privacy terms, but different from the court's viewpoint that privacy is a substitute of price or quality as a measurement of consumer welfare, I hypothesize the following:

Hypothesis 1: Consumer's anticipation for privacy can result in positive effects on buyers' demand, even when the price is increased due to the announced privacy protection.

Hypothesis 2: The data holder will be motivated to shift the cost of holding data to buyers, or cut spending on privacy protections, when it surpasses the price of the service to buyers.

Following Hypothesis 1 that consumer's anticipation for privacy can result in positive effects on buyers' demand, there are two concerns: (i) can a^P reinforce the positive effect of D^B on V_d while increasing D^B (the positive effect of D^B on V_d can be proven by the merger case) (see Figure 3), and (ii) what are the differences between the "free services" strategy and the "higher-quality-but-higher-price" strategy with respect to the effect of p^B (price of the service to the buyers) on D^B and the shifting of c^H, when introducing a^P?

[24] As opposed to the marginal cost of online services, protecting one's privacy is costly to carry out, and the cost may increase as time goes on. For example, data controllers need to update their database and algorithms timely to maintain the accuracy of the estimate about how much each consumer is willing to pay, and even to predict the competitors' reactions (Graef, 2018).

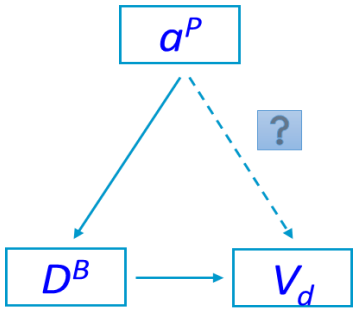


Figure 3. Relationship between a^P, D^B, and V_d.

First, in response to Question (i), we need to introduce the endowment effect and loss aversion—people tend to place more emphasis on a loss than a gain of equal magnitude (Camerer, 2005). If a platform discloses the costs in relation to privacy protection, which means the user has to spend "extra" money on the product (or service), it may push users who have less privacy preference/concern to a competing platform because such information emphasizes what you have to "lose"; otherwise, the "high-quality" information in a package emphasizes what you will "gain". It works especially when the user has not been "locked in" a certain platform, in which case, it will be difficult for the user to cease to use such a platform when he (she) has "owned" it (e.g., Facebook[25]). Thus, passing c^H to buyers without their knowledge under a quality-increased (privacy-friendly) appearance (a^P) will make the platform more attractive, thereby increasing the D^B. This is also the reason why data controllers tend to violate privacy laws in a deceptive manner.

However, to prove that an increase in a^P has a positive effect on D^B and has a positive effect on V_d through increased D^B, which is significant for increasing the platform's profit (Rochet & Tirole, 2003),[26] we need to explore, in the absence of increased D^B, e.g., the derivative of D^B, that is $\partial D^B / \partial a^P \leq 0$, whether the announced privacy-enhancing policy ($a^P > 0$) cannot impact V_d in any event (see Figure 3). The "first-party data" strategy, as an example, may still impact V_d without increasing D^B. Google launched a "privacy sandbox" proposal to curb user tracking by blocking the "traditional" way of tracking, third-party cookies (Geradin, Katsifis, & Karanikioti, 2021), and providing third parties with aggregate data instead, to the prejudice of downstream competitors, as such, the V_d of Google is larger than that of its competitors; thus, the V_d is an "advantage indicator"—a comparative value—that affects switching costs c^S for its trading partners.

However, such a direct impact of the a^P on V_d has a limitation that the users should singlehome—an analogy of a "walled garden"—otherwise, third parties can acquire user data through competing platforms or other means, such that its advantage in V_d may no longer exist.[27] Compared with the impact of a^P on V_d, the increase in (comparative) V_d relies primarily on the increase in D^B, regardless of whether users singlehome.[28]

---

[25] Users of Facebook are more willing to pay for Facebook rather than to be compensated to cease to use it (Sunstein, 2018).

[26] Rochet and Tirole (2003) invoked the formula, $\pi = (p^B + p^S - c)D^B(p^B)D^S(p^S)$, proposed by Schmalensee (2002), to express the total profit π in the case of private monopoly.

[27] This methodology to determine which variable (a^P, D^B) has greater impact on V_d is similar to the rationale behind sensitivity analysis. Sensitivity analysis is conducted for the purpose of investigating how important is each model input in determining its output (Iooss & Saltelli, 2015).

[28] In this case, the platform will have motivation to endorse privacy-friendly policies continuously for the purpose of increasing D^B, rather than to reduce the price to attract more buyers.

Second, in response to Question (ii), we may introduce the "within-group" network effect—a user's decision to participate in a market could also be influenced by the presence of other users in the same group (Belleflamme & Toulemonde, 2009). For example, users may opt for a search engine with a larger user base, as it appears to offer superior search quality (Decarolis & Li, 2023), and a relatively high price would be acceptable. Thus, to increase D^B, it does work to adopt an "appear-to-be-low" price (e.g., the Apple One bundles plan), but nevertheless, the data holder will be motivated to shift the cost of holding data c^H to the buyers when $c^H(\sigma) > p^B(a^P)$ or cut spending on privacy protections, e.g., selling personal profiles to advertisers for profit without consent (Facebook Internet Tracking case).

Therefore, according to the previous discussion, if we treat the transfer of personal data as a transfer of privacy risk, the controller is obligated to bear the privacy-preserving cost, and the consumers do not need to pay the bill for services with a higher level of privacy protection. It follows that, in addition to the exploitative effect on the producer's side (e.g., Apple's App Store tax), the exploitation occurs on the consumer's side at the same time.

Results and Discussion: The Evidence From 24 Cases

Based on 24 data-competition intersected cases and typical investigations against four major tech-companies, including cases where the company's data policy contributes to its position and profits on the advertising market (see Appendix A, data retrieved from competition-cases.ec.europa.eu, gov.uk, LexisNexis), Tables 1 and 2 display 15 types of conducts/strategies that show how privacy exploitation can establish a violation of antitrust. Digital platforms usually implement it through three strategies that follow one another:

(1) To adopt practices of data extraction:

- Set an expectation of privacy for the user via privacy policy.
- Obtain data from the users directly, or require trading partners to render their data (e.g., merger, use third-party seller data).
- Ensure exclusive access to the user data (e.g., a series of exclusive contracts).[29]

(2) To exclude or foreclose competitors:

- Ensure the data advantage.[30]
- Raise barriers to entry—for the purpose of preventing users from switching to other alternatives (e.g., self-preferencing, limitations on access to user data, anti-steering).
- Lock in the consumers.

(3) To shift the costs to individuals and businesses dependent on these platforms:

- Privacy violation (exploitation on the consumer's side by shifting costs, i.e., "$-c^H$"—the cost of holding data is deducted from the platform's marginal cost of a transaction).
- Raise the costs of counterparties (cost of switching, "c^S").
- Exploitation on the producer's side (e.g., Apple tax).

[29] According to Newman (2014), "Google built its dominant position in the search advertising market in part through a series of exclusive contracts that gave it access to an increasing amount of user data."

[30] It is said that the data derived from counterparties could be used in these platforms' algorithms to compete with their counterparties (Khan, 2020).

It follows that the illegality of privacy exploitation under antitrust law is preventing consumers from switching by foreclosing competitors while failing to bear the costs in relation to privacy protection despite privacy promises, or passing them to consumers under the cover of privacy protection or high-quality services, which can qualify as willful maintenance of market power (data advantage, Premise (1)) via anticompetitive conduct (by raising the cost of switching, "c^S"), and exclusionary practice contributes to the proof of such competitive harm of privacy intrusion ("$-c^H$").

Table 1

24 Data-Competition Intersected Cases Against Meta (Facebook), Apple, Amazon, Google, and 15 Types of Conducts/Strategies That May Raise Competition Concerns

Steps	Conduct	Meta	Apple	Amazon	Google	Total
Data extraction	Merger (WhatsApp, Buy Box, etc.)	[6] [7]	-	[14] [16]	[24]	5
	First-party data	-	[12]	-	[21] [23]	3
	Use third-party seller data	-	-	[13]	-	1
Controller ↔ trading partners	Refusal to grant access	[2] [5]	-	-	-	2
	Anti-steering policy	-	[8] [10]	-	-	2
	Self-preferencing	-	[12]	[13] [17]	[21] [22]	5
	Exclusive contract	-	-	-	[20]	1
	Apple/Google/Amazon tax	-	[10] [11]	[13]	[21] [22]	5
	Discounted wholesale price	-	-	[18]	-	1
Controller ↔ consumers	Collection without consent	[1] [2] [3] [4]	-	-	-	4
	Monetize user data against policy	-	[9]	-	-	1
	Prevent deletion requests	-	-	[15]	-	1
	Scrap user data to train AI models	-	-	-	[19]	1
	One bundles plan*					
	Personalized pricing/coupon*					

Note. * There is no case for these types yet.

Table 2

Three Steps to Accomplish Exploitation

	(1) Data extraction	(2) Controller ↔ trading partners		(3) Controller ↔ consumers	
		Exclusionary conduct	Exploitative conduct	Privacy violation	Shifting of costs ("sales tax" mode)
Facebook	Merger (Instagram, WhatsApp)	Refusal to grant access		Collection without consent	
Apple	First-party data	Anti-steering policy	Taxing	Monetize user data against policy	One bundles plan
Amazon	Use of third-party seller data	Self-preferencing	Discounted wholesale price	Prevent deletion requests	Personalized pricing/coupon
Google	Merger (Doubleclick); first-party data	Exclusive contract	Taxing/paid-inclusion model	Scrap user data to train AI models	

1 2 3 4 5

Notes. (1) The deepest color indicates that the issue has been brought before the courts or authorities five times (five out of 24 cases), but the issue is not limited to one platform; e.g., self-preferencing is presented in (i) the investigation against Apple [12], (ii) Bira v. Amazon [13], (iii) FTC v. Amazon [17], the EU Google-Adtech case [21], and (iv) the Google shopping case [22].

(2) First-party data: Apple's new App Tracking Transparency feature ("ATT") does not prohibit Apps from collecting and using first-party data, which means that cross-site tracking would be allowed if those Apps are owned by the same company. See The Apple Company (2022). "User Privacy and Data Use". https://developer.apple.com/app-store/user-privacy-and-data-use.

(3) Discounted wholesale price: Publishers were opposed to Amazon's $9.99 pricing on new and bestselling e-books long ago; as opposed to selling books to retailers at a discounted wholesale price, Apple suggested a new "agency" mode—that made retailers the agents of publishers, giving the latter greater say on retail prices for books. See Raff & Zhang (2014). Amazon vs. Hachette: The Battle for the Future of Publishing. *Knowledge*. https://knowledge.wharton.upenn.edu/article/amazon-vs-hachette-battle-future-publishing.
(4) Paid inclusion model: According to the Google Shopping case (Google and Alphabet v. Commission), specialized search results were "natural" results, which are not paid for by the websites to which they link, in the times of "Froogle" and at the beginning of "Product Universal", then a paid inclusion model was introduced—the results pages additionally contain results that are paid for by the websites to which they link.
(5) Data scrapped for training AI: According to a recent lawsuit against Google, Google was alleged to revise its privacy policy in support of taking anything shared online to train and improve its AI products, including copyrighted information.

Conclusion

In the traditional view of antitrust law, competition authorities or courts are usually concerned with whether consumers suffer from higher prices or lower quality in a given market. With the increasing interplay between privacy law and competition law, new competition law concerns touch more on whether reduced privacy arising from data extraction, personalized pricing, invalid consent, etc., will lead to a substantial decline in consumer welfare or total welfare. However, none of these privacy intrusions can stand alone as an independent antitrust standard of review to establish a willful maintenance of market power. The major challenges for proof of competitive harm are as follows:

(1) The consumer surplus is accurately captured by AI-enabled price discrimination, in the form of higher prices for consumers with high willingness to pay and higher prices than for third-party sellers; however, it is difficult to determine whether the high price is a result of eliminated competition or increased quality of services, despite the recognition of unfairness.

(2) Privacy protection is a strong defense, as it is often acknowledged that firms will compete on better privacy terms to prevent users from switching; however, conversely, the privacy violation has to be converted into reduced quality to convince the court of the consumer harm that could support a monopolization case (or abuse of dominance in an EU context or other jurisdictions).

In response to these questions, the paper votes for ex ante regulation on problematic data processing. On the one hand, the exploitation can exist on both the producer's side and the consumer's side, rather than the mere single exploitative effect of single exploitative conduct; on the consumer's side, it takes the forms of privacy violation, or shifting of costs in a deceptive or coercive manner—the reduction in consumers' privacy cannot be compensated by benefits to producers.

On the other hand, the switching costs arising from data advantage, the lack of an individual's right to informational self-determination (i.e., freedom to choose), and the privacy violation against the data subject's expectation of privacy that the platform sets via privacy terms, from which the effects of both exclusionary and exploitative conduct accrue, will work to show that privacy concerns have independent significance to the proof of competitive harm other than being part of the quality. This study contributes to the debate on the role of privacy in competition analysis, as well as to the theories of harm literature.

References

Belleflamme, P., & Toulemonde, E. (2009). Negative intra-group externalities in two-sided markets. *Int. Econ. Rev. (Philadelphia), 50*(1), 245-272.

Caffarra, C. (2020, December 8). *Abuse of dominance in digital markets—Theories of harm in digital markets*. OECD DAF/COMP/GF(2020)8.

Camerer, C. (2005). Three cheers—psychological, theoretical, empirical—for loss aversion. *Journal of Marketing Research, 42*, 129-133.

Cofone, I. N. (2021). Beyond data ownership. *Cardozo Law Review, 43*(2), 553-556.

Condorelli, D., & Padilla, J. (2021). Data-driven envelopment with privacy-policy tying. *14th Digital Economics Conference*. Online.

Decarolis, F., & Li, M. (2023). Regulating online search in the EU: From the Android case to the digital markets act and digital services act. *International Journal of Industrial Organization, 90*, 1-15.

Douglas, E. M. (2021). The new antitrust/data privacy law interface. In *The Yale Law Journal Forum* (pp. 647-684). Retrieved from https://www.yalelawjournal.org/pdf/DouglasEssay_pv1pt6ak.pdf

Economides, N., & Lianos, L. (2021). Restrictions on privacy and exploitation in the digital economy: A market failure perspective. *Journal of Competition Law & Economics, 17*(4), 765-847.

Esayas, S. Y. (2017). Privacy-as-a-quality parameter: Some reflections on the scepticism (Stockholm Faculty of Law Research Paper No. 43). Stockholm University.

Esayas, S. Y. (2019). Privacy as a non-price competition parameter: Theories of harm in mergers. *European Competition Law Review, 40*(4), 166-181.

Fathi, S. (2023, January 24). Apple accused of "hypocrisy" by ad industry coalition over its anti-tracking policy. *MacRumors*. Retrieved from https://www.macrumors.com/2023/01/24/apple-ad-coalition-tracking-policy

Gellert, R., & Gutwirth, S. (2013). The legal construction of privacy and data protection. *Comput. Law Secur. Rev., 29*(5), 522-530.

Geradin, D., Katsifis, D., & Karanikioti, T. (2021). Google as a de facto privacy regulator: Analysing the privacy sandbox from an antitrust perspective. *European Competition Journal, 17*(3), 617-681.

Graef, I. (2018). Algorithms and fairness: What role for competition law in targeting price discrimination towards ends consumers. *Columbia J Eur Law, 24*(3), 541-560.

Graef, I., & van der Sloot, B. (2022). Collective data harms at the crossroads of data protection and competition law: Moving beyond individual empowerment. *European Business Law Review, 33*(4), 513-536.

Haucap, J. (2019). Data protection and antitrust: New types of abuse cases? An economist's view in light of the German Facebook decision. *CPI Antitrust Chronicle, 2*(2).

Iooss, B., & Saltelli, A. (2015). Introduction to sensitivity analysis. In R. Ghanem et al. (Eds.), *Handbook of uncertainty quantification* (pp. 1103-1122). New York: Springer.

Kerber, W., & Zolna, K. K. (2022). The German Facebook case: The law and economics of the relationship between competition and data protection law. *European Journal of Law and Economics, 54*, 217-250.

Khan, L. (2017). Amazon's antitrust paradox. *Yale Law Journal, 126*(3), 710-805.

Khan, L. (2020, December 8). *Abuse of dominance in digital markets—Theories of harm in digital markets*. OECD DAF/COMP/GF(2020)8.

Li, Q., Philipsen, N., & Cauffman, C. (2023). AI-enabled price discrimination as an abuse of dominance: A law and economics analysis. *China-EU Law Journal, 9*, 51-72.

Manne, G., & Sperry, B. (2015). The problems and perils of bootstrapping privacy and data into an antitrust framework. *CPI Antitrust Chronicle, 5*(2).

Meyer, D. (2021, March 17). France refuses to Block Apple's big privacy changes. *Fortune*. Retrieved from https://fortune.com/2021/03/17/apple-privacy-changes-app-tracking-antitrust-france

Morales, J. (2023, June 29). Apple one vs. third-party subscriptions: Which is better value for money? *MOU*. Retrieved from https://www.makeuseof.com/apple-one-vs-third-party-subscriptions

Morozovaite, V. (2023). The future of anticompetitive self-preferencing: Analysis of hypernudging by voice assistants under article 102 TFEU. *European Competition Journal, 19*(3), 410-448.

Newman, N. (2014). Search, antitrust and the economics of the control of user data. *Yale J. on Reg, 31*(2), 401-454.

OECD. (2013). Exploring the economics of personal data: A survey of methodologies for measuring monetary value (OECD Digital Economy Papers No. 220). Paris: OECD Publishing.

OECD. (2015). *Data-driven innovation: Big data for growth and well-being*. Paris: OECD Publishing.

OECD. (2018, November 28). Personalised pricing in the digital era—Note by the United States. DAF/COMP/WD(2018)140.

OECD. (2020, December 8). Abuse of dominance in digital markets. DAF/COMP/GF(2020)8.

Patterson, M. R. (2017). *Antitrust law in the new economy*. Cambridge: Harvard University Press.

Peters, J. (2020, February 20). Facebook will now pay you for your voice recordings. *The Verge*. Retrieved from https://www.theverge.com/2020/2/20/21145584/facebook-pay-record-voice-speech-recognitionviewpoints-prounciations-app

Pulver Crawford Munroe LLP. (2022). Restrictive covenants—detailed analysis—legitimate proprietary interest. *The Canadian Employee Competition Blog*.

Purtova, N. (2017). Do property rights in personal data make sense after the big data turn: Individual control and transparency. *Journal of Law and Economic Regulation, 10*(2), 64-78.

Rochet, J. C., & Tirole, J. (2003). Platform competition in two-sided markets. *Journal of the European Economic Association, 1*(4), 990-1029.

Rodotà, S. (2009). Data protection as a fundamental right. In S. Gutwirth et al. (Eds.), *Reinventing data protection?* (pp. 77-82). New York: Springer.

Shelanski, H. A. (2013). Information, innovation, and competition policy for the Internet. *University of Pennsylvania Law Review, 161*, 1663-1705.

Srinivasan, D. (2019). The antitrust case against Facebook: A monopolist's journey towards pervasive surveillance in spite of consumers' preference for privacy. *Berkeley Bus. L. J., 16*(1), 39-101.

Steinberg, E. (2019). Big data and personalized pricing. *Business Ethics Quarterly, 30*(1), 97-117.

Stucke, M. E. (2018). Should we be concerned about data-opolies? *Georgetown Law Technology Review, 2*(2), 275-324.

Sustein, C. (2018). How much would you pay to use Facebook? A behavioural perspective. Retrieved from https://hls.harvard.edu/bibliography/how-much-would-you-pay-to-use-facebook-a-behavioral-perspective/

Swire, P. (2007, October 18). Submitted testimony to the federal trade commission behavioral advertising town hall. Retrieved from https://www.americanprogress.org/article/protecting-consumers-privacy-matters-in-antitrust-analysis

US House Judiciary Committee. (2022, July 19). Judiciary Committee publishes final report on competition in the digital marketplace. Media Center.

Vestager, M. (2016). Protecting consumers from exploitation. *Chillin' Competition Conference*. Brussels.

Appendix A

Facebook

[1] Doe, et al. v. Meta Platforms, Inc., et al., 3:22-cv-03580WHO (N.D. Cal. 2023).

[2] FTC v. Facebook, Inc., 2021 WL 2643627, at 1-2 (D.D.C. June 28, 2021).

[3] Facebook, Inc. v. Bundeskartellamt, No. 080/2020 (BGH. Jun. 23, 2020).

[4] In re Facebook, Inc. Internet Tracking Litig., 956 F. 3d 589 (9th Cir. 2020).

[5] Stackla, Inc. v. Facebook Inc., 4:19-cv-05849, (N.D. Cal. 2019). (Refusal to grant access)

[6] EC, Case COMP/M.7217, Facebook/WhatsApp, decision of 3 Oct. 2014; Case COMP/M.8228, Facebook/WhatsApp, decision of 17 May 2017.

[7] FTC, File No. 121-0121, Facebook/Instagram decision of 22 Aug. 2012.

Apple

[8] EC, Case AT.40437, Apple—App Store Practices (music streaming), decision of 4 Mar. 2024.

[9] In re Apple Data Privacy Litigation, 5:22-cv-07069-EJD (N.D. Cal. 2023).

[10] Epic Games, Inc. v. Apple, Inc., No. 4:20-cv-05640-YGR (N.D. Cal. Aug. 13, 2020); Epic Games, Inc. v. Apple, Inc., No. 21-16506 (9th Cir. 2023).

[11] Jin Xin v. Apple, Inc., Civil Judgment of Shanghai Intellectual Property Court, Case No. (2021) Hu 73 Zhi Min Chu No. 220.

[12] Bundeskartellamt (German Federal Cartel Office), 2021. Investigation against Apple for its App Tracking Transparency Framework.

Amazon

[13] CAT (UK), Case No.1641/7/7/24, Bira v. Amazon, in progress.

[14] EC, Case COMP/M. 10920, Amazon/iRobot, decision of 29 Jan. 2024.

[15] United States v. Amazon.com, 2:23-cv-00811-TL (W.D. Wash. 2023).

[16] EC, Case COMP/M. 40703, Amazon/Buy Box, decision of 2 Mar. 2023.

[17] FTC v. Amazon.com Inc., 2:23-cv-01495 (W.D. Wash. 2023).

[18] Bookends & Beginnings LLC v. Amazon.com, Inc., 1:21-cv-02584 (S.D.N.Y. 2021).

Google

[19] J. L. et al. v. Alphabet Inc. et al., 3:23-cv-03440 (N.D. Cal. 2023).

[20] United States v. Google, LLC, No. 20-cv-3010, 2024 WL 3647498 (D.D.C. Aug. 5, 2024).

[21] EC, Case AT.40670, Google—Adtech and Data-related practices, in progress.

[22] Case T-612/17, Google and Alphabet v. Commission (Google Shopping) EU:T:2021:763.

[23] Competition and Markets Authority (CMA), 2020. Online Platforms and Digital Advertising market study—Appendix G: the role of tracking in digital advertising. (First-party data)

[24] EC, Case COMP/M.4731, Google/DoubleClick, decision of 11 Mar. 2008.