A Critical Discussion on Privacy Concerns in EU Antitrust Enforcement

Xinpeng Liu*

University of Galway, Galway, Ireland

*X.Liu12@universityofgalway.ie

Abstract. The topic of antitrust and privacy has been widespread for many years. It deals with the integration of privacy in competition law. In this topic, the German Facebook case is a hot-debated case. In this case, the Federal Cartel Office (FCO) explicitly takes privacy into antitrust concerns, promoting the topic to a wider discussion. Opinions diverge greatly in FCO's approach. As a result, there is a need to determine whether the EU antitrust enforcement should take privacy into account. In this essay, I analyse first the conflicting views about privacy concerns in antitrust. Then, I argue that privacy should be an EU antitrust concern from three perspectives. Firstly, privacy harm can lead to consumer welfare degradation. To solve the degradation, the intervention of competition law is necessary. Secondly, with the users' privacy data collection, the dominant companies have the incentive to implement price discrimination to exploit consumer surplus. Thirdly, the data protection law alone is unable to address the antitrust privacy issue because the data protection law and competition law are interactive in the digital economy.

Keywords: Antitrust, Privacy, Data, Consumer Welfare

1 Introduction

Considering privacy as an antitrust concern helps to protect end users' privacy. The EU recognises privacy as a fundamental human right, as considered in the Charter of Fundamental Rights of the European Union. Thus, the protection of privacy should be strict. Consumers may not like privacy collections. A survey in 2021 shows that up to 46% of consumers do not like their data being collected.[1] It is a violation of privacy for many companies not to leave users the right to refuse privacy data collection. Therefore, to solve the problem, privacy can be an antitrust concern.

However, it has been argued that privacy should not be an antitrust concern.[2] Firstly, there is a trade-off between the user's data collection and free services. It is unreasonable to expect unlimited free services and consumers actually "pay" for companies' free services with their data. Secondly, the mere possession of monopoly power is not unlawful in many jurisdictions (eg. the US). Therefore, mere big data collection does not mean compromising privacy. There is a need to prove an incentive for the firm to harm privacy or it will fall into the trap of "big is bad". Actually, instead of harming privacy,

D. Rad et al. (eds.), *Proceedings of the 2024 5th International Conference on Mental Health, Education and Human Development (MHEHD 2024)*, Advances in Social Science, Education and Humanities Research 857,
https://doi.org/10.2991/978-2-38476-271-2_33

companies are incentivized to improve product quality with the data collected.[3] For example, Amazon can make better recommendations according to users' preferences. Thirdly, the EU data protection law (GDPR), not competition law, should deal with privacy concerns in antitrust enforcement.[4] The clarity of competition law would be compromised if it takes privacy into antitrust concern.

As a result, there is a necessity to judge whether privacy should be an antitrust concern. I argue that privacy should be an antitrust concern. The reasons will be discussed in the following sections.

2 Consumer Welfare Degradation and Data Market

The first reason is excessive data collection can degrade consumer welfare. Privacy data collection can be considered a parameter of service quality.[5] Thus, privacy can be a part of consumer welfare.[6] Firstly, data collection can put privacy at risk.[7] User data will allow companies to grasp users' behavioural habits. More targeted business practices can therefore be implemented accordingly. The user may then be vulnerable to price discrimination, target fraud and etc. Additionally, the information asymmetry that the consumer is ignorant about future risks when they provide their data is making matters worse. Secondly, data collection can compromise consumers' privacy preferences. Different consumers have different ideas about whether and to what extent they reveal data. Some users are not willing to provide data but to pay for services. However, due to the power imbalance between consumers and dominant firms, consumers have no other choice but to give out all of their privacy. The take-it-or-leave-it service ignores users' privacy preferences, thus degrading consumer welfare.

These issues can be solved by establishing a market for personal data.[8] The market is distinct from the markets of service fueled by data.[9] This market can take two forms. In the first form, users who provide information can use the service for free, while those who do not have to pay for the service. The second form is that privacy "opt-out" is the default model and customers get compensation for choosing "opt-in" to provide data. Which market form will emerge depends on various factors such as how much users value privacy, and the company's market position. However, the common premise of their appearance is that companies (eg. Google, Facebook) provide more data collection options and information disclosure. Consumers should have the choice to "opt-out" of data collection and be informed of the purpose of the data. In this way, consumers will then be able to assess the benefits and costs of data provision and decide whether and to what extent to reveal their data.

However, the establishment of this market needs competition law intervention. Dominant firms have no incentives to establish a market when they can collect all user data with a take-it-or-leave-it offer. Even when data markets are established, companies can use their dominant position to exploit consumers. For example, due to an imbalance bargain power, consumers may be overcharged if they choose not to provide data, or get paid an overly low price for their data. One possible solution is to break up dominant firms structurally. However, its effect on the data market is limited. The network effects make the "winners take all" phenomenon more prominent. After breaking up, new

dominant firms will grow up and the market structure will be the same as before. Another solution can be the application of Article 102 of TFEU if the price of data can be considered an "unfair price". The EU competition authorities should compare the price charged and the cost of providing services to determine whether the price charged is excessive. In addition, the EU competition authorities can also "facilitate consumers' collective bargaining power" to increase the data price sold to dominant firms. Regardless of whichever approach is finally taken, the intervention of competition law is necessary.

To sum up, privacy degradation can lead to reduced consumer welfare. To solve the problem, the intervention of competition law to establish data markets is necessary.

3 Price Discrimination and Consumer Surplus Exploitation

The second reason is dominant firms have an incentive to harm users' privacy with data collection because they can practice price discrimination. Data brings market power.[10] With a large amount of power collected, dominant firms may exploit consumer welfare surplus by pricing consumers unequally. With price discrimination, many consumers may pay more than what they should pay. In online transactions, firms can implement price discrimination more easily because customers' price preferences can be found out through customers' data (eg. search history).

Despite the risk of consumer surplus loss, it has been held that price discrimination is not necessarily an antitrust consideration. This is because price discrimination can be beneficial and considering data collection and price discrimination in antitrust enforcement is time-consuming and costly. Firstly, price discrimination may increase net consumer welfare. It can be seen as simply a way to charge customers according to their willingness to pay through technological means. There are many consumers who pay lower than the otherwise uniform price. The influence on net consumer welfare will be uncertain if the group of such consumers is larger than that of consumers paying more than a uniform price. Secondly, price discrimination can increase competition efficiency. Regarding static efficiency, rich consumers and poor consumers should have been in different markets. Due to price discrimination, both rich and poor consumers can afford services, and thus competition increases in the market for both poor and rich consumers. Regarding dynamic efficiency, price discrimination may generate more revenue for companies. Companies can then invest more in innovation, increasing their product range, and also in research. Therefore, considering the uncertainty of the impact on consumer welfare and competition, privacy collection and price discrimination are not necessarily considered in antitrust enforcement.

However, I argue that privacy collection and price discrimination should be considered in antitrust though they can sometimes be beneficial. In the digital era, everyone uses online services. When price discrimination is harmful, its impact will be very widespread. With the assistance of machine learning and AI, the risk of consumer welfare loss from price discrimination is getting greater. In addition, the negative effects of price discrimination are not limited to consumers paying more than otherwise

uniform prices.[11] For example, many consumers are not informed of price discrimination. This lack of transparency undermines the consumer's right to know. Price discrimination can also lead to negative externalities by making consumers spend more time trying to avoid it. Therefore, antitrust investigations into data collection and price discrimination are worthwhile even if they can be costly.

In summary, with a large amount of users' data collected, dominant firms have the incentive to harm users' privacy through price discrimination. In the digital economy, price discrimination can have a widespread negative effect on consumers. Thus, antitrust needs to take privacy data collection and price discrimination into consideration.

4 An Integrated Approach to Competition and Data Protection Law

The third reason is that competition law and data protection law are highly interactive in the digital economy. The idea that it is the role of data protection law to solve antitrust privacy concerns is untenable because data protection laws alone cannot solve the privacy issues in antitrust due to this interaction.

Competition law and data protection law have a strong interaction in antitrust privacy concerns. Under the traditional legal approach, different laws address different issues. Thus, privacy concerns in antitrust (eg, Facebook case) should rely alone on GDPR in the EU. A famous example is the EU Commission assumes that there is no need to consider the effects on privacy in data mergers because privacy concerns should rely on EU data protection rules. However, the traditional legal approach is based on a few assumptions. One of the important ones is the effects of different laws are independent of each other. In the antitrust privacy concerns, it means competition law and GDPR do not affect each other's effectiveness. However, the presumption is contrary to the facts. GDPR influences competition law effects with its high requirements on consumer consent. Dominant companies have more resources to meet this requirement than smaller companies. This increases entry barriers and puts more data in the hands of dominant companies, increasing privacy risks for users. Additionally, it can also promote competition law enforcement through the facilitation of data market establishment. This is because the data portability right (GDPR Article 20) can reduce the switching cost of data. By contrast, competition problems can also impact GDPR enforcement. The extent to which data is collected varies from company to company. When there is less competition in the market, the fewer choices consumers have about data collection degrees. Consumers will then be less incentivised to read companies' privacy policies, leading to a greater privacy crisis. The dominant firms can also be motivated to use misleading and less transparent practices to collect users' privacy because users have few alternative service options. Therefore, the traditional separation of law application approach ignores the strong interaction between competition law and data protection law and is unable to fit into the digital economy.

Only an integrated approach of competition law and data protection law can solve antitrust privacy concerns. Data protection law alone is incapable of solving privacy concerns in antitrust. In the EU, GDPR can not analyse competition problems. It only

establishes a minimum privacy standard and a higher protection level may be expected in markets. For example, different firms have different impacts on privacy. Regulation of data collection from dominant companies may need to be stricter. However, GDPR treats firms equally and can not distinguish dominant firms from others. Therefore, GDPR should combine with competition law to solve antitrust privacy concerns. By contrast, an integrated approach can address privacy concerns in antitrust effectively. The "Digital Market Act" (DMA) is a good example. Article 5 and Recital 36 of DMA place many obligations on the core online service provider (gatekeeper) to protect the user's privacy (eg. not to process the user's data for advertisement purposes without users' free consent). This limits anti-competitive behaviour through ex-ante provisions and offers consumers a minimum degree of control over their data. It considers the interaction of competition and privacy, leading to optimal decisions in antitrust enforcement.

To conclude, data protection law alone is unable to solve antirust privacy concerns due to the interaction of data protection law and competition law. Therefore, competition law should combine with data protection law to solve antitrust privacy concerns.

5 Conclusion

Whether privacy should be an antitrust concern is a controversial issue. Many consumers are unwilling to provide their privacy data but the use of many companies' services is premised on consumers providing data. This forces many consumers to provide their data for free and their privacy is thus harmed. Therefore, taking privacy into antitrust consideration can better protect consumers' privacy. However, the counterarguments hold that privacy is not an antitrust concern for the following reasons: (1) consumers are actually trading their data for free services; (2) a mere collection of data does not mean privacy harm; (3) there is already data protection law dealing with privacy issues. Through analysis and comparison, I argue that privacy should be an antitrust concern. Firstly, privacy is a part of consumer welfare and excessive data collection can put their privacy at risk and compromise consumers' privacy preferences, leading to consumer welfare degradation. Empowering consumers with control over their private data and establishing a data market could solve this problem but the market establishment would require competition law to intervene. Secondly, companies have the incentive to exploit consumer surplus with price discrimination, though price discrimination can be beneficial sometimes. Price discrimination is common in the data economy, and privacy data collection makes companies easy to implement price discrimination. Once price discrimination is harmful, its negative effects can be very widespread. Therefore, data collection and price discrimination should be an antitrust concern, despite the increased cost of antitrust enforcement. Thirdly, data protection law alone is incapable of addressing antitrust privacy concerns. Competition law and data protection law are highly interactive in the digital economy. Only an integrated approach of competition law and data protection law can address antitrust privacy concerns. As a result, taking privacy concerns into antitrust enforcement, both user privacy and market competition will be well protected.

Reference

1. Akman P, (2021) 'A Web of Paradoxes: Empirical Evidence on Online Platform Users and Implications for Competition and Regulation in Digital Markets' SSRN Electronic Journal <https://www.ssrn.com/abstract=3835280> accessed 3 May 2023.
2. Manne GA and Sperry B, (2014) 'The Law and Economics of Data and Privacy in Antitrust Analysis' SSRN Electronic Journal <http://www.ssrn.com/abstract=2418779>.
3. Stucke M, (2016) Big Data and Competition Policy. Oxford University Press. Oxford.
4. Buiten MC, (2021) 'Exploitative Abuses in Digital Markets: Between Competition Law and Data Protection Law' 9 Journal of Antitrust Enforcement 270
5. Witt AC, (2021) 'Excessive Data Collection as a Form of Anticompetitive Conduct: The German Facebook Case' 66 The Antitrust Bulletin 276.
6. Esayas SY, (2017) 'Privacy-As-A-Quality Parameter: Some Reflections on the Scepticism' SSRN Electronic Journal <https://www.ssrn.com/abstract=3075239>.
7. Kerber W and Zolna KK, (2020) 'The German Facebook Case: The Law and Economics of the Relationship between Competition and Data Protection Law' SSRN Electronic Journal <https://www.ssrn.com/abstract=3719098>.
8. Economides N and Lianos I, (2021) 'Restrictions on Privacy and Exploitation In The Digital Economy: A Market Failure Perspective' 17 Journal of Competition Law & Economics 765.
9. Harbour PJ and Koslov TI, (2010) 'Section 2 In A Web 2.0 World: An Expanded Vision of Relevant Product Markets' 76 Antitrust law journal 769.
10. Carugati C, (2023) 'The Antitrust Privacy Dilemma' the European Competition Journal 1.
11. Wright JD, (2005) 'Missed Opportunities in Independent Ink' (2005-2006) Cato Sup Ct Rev 333.