Effect of consumer's biases on infringements to competition law by social media platforms' algorithms

Introduction

The literature on the articulation of public and private action in competition law insists on the benefits to introducing private action by consumers because of an informational advantage held by the latter: they would receive the signal of the infringement more quickly than the authorities (McAfee, Mialon, 2008).

It is easy to imagine this informational advantage in the context of a cartel: consumers are subject to a monetary overcharge that they identify immediately. Therefore, they are the first to receive the signal of the infringement by consuming the cartelised product.

However, in the context of a digital economy, it would seem that the characteristics of online platforms mean that consumers lose their informational advantage in the event of an infringement of competition law. Indeed, in the digital market, consumers have a free access to services, in exchange for their data. So, if a infringement to competition occurs in the form of an excessive data collection, they won't receive the signal of the infringement, because they don't bear a monetary cost that would vary and are not in a position to estimate a change in the collection of their data.

This, combined with a lack of incentives for the online platforms to behave competitively: there are no disciplinary mechanisms inside the social media market that would prevent an excessive collection of consumer data.

On the contrary, social media platforms are incentivized to collect as much consumer data as possible, to have performant algorithms, with this personalised data then sold for targeted advertising. And even if a platform in a dominant market excessively collect data from its consumers, they bear no costs because these consumers are unaware of the practice and wouldn't be able to quantify the damages which are future, diffuse, and hardly attributable if the data are sold to a third party.

The lack of transparency on algorithms processing of consumers data, with all the biases consumers are subject to when accessing these digital services negatively impact consumers' ability to incentivize platforms of behaviours, by the mean of threat to ligitate.

Finally, despite all the advantages that the consumers benefits from the artifical intelligence, it is also a damage aggravators. The data collected by the social media platforms, sold to the adverstisers, limit consumers choice and autonomy, which are turned into algorithmics consumers (Gal, Elkin-Koren, (2017)).

In the first section, the article briefly provides an overview of the type of competition infringements that may arise from social media platforms and highlight the difficulties to assess consumers' harms to damages quantification in this specific market. Section 2 reviews the consumers' biases when using social media platforms. Section 3 discusses the importance of raising consumer awareness on their data with the goal of design a tool improving algorithms transparency.

I. A non-quantifiable damage from algorithms in social media platforms

The digital market economy has three characteristics: extreme return to scale, network externalities, and the role of data[1]. These characteristics combined, for instance network effects associated with barriers to entry, lead the path for highly concentrated markets. With very few key players in the digital market, especially for this paper, in the social media market, they might be tempted to abuse from their high market power. For these reasons, the digital economy is under scrutiny by competition authorities and regulators all around the world.

Relating to competition law, abuse of dominance are mostly fears from social media platforms. However, with consumers accessing services without a monetary cost, if an infringement occurs, users would face difficulties in order to quantify their infringement. Knowing that in EU Competition law, the only tool available for the private enforcements are the claims for monetary damages, for which the defendant must demonstrate the harm suffered. It means that we need to set aside potentially effective remedies in the digital markets (Petit Gal, (2020)) and all the solutions to overcome the issue of damages evaluation, like the disengorgement remedy, in the US context (Newman, 2015).

Then, how can the algorithms on social media platform harms consumers through a competition law infringement, and how would a defendant quantify the resulting damage?

Nazzini (2019) recalls that competition law can only address the harm to “competition”, and to introduce privacy considerations into the scope of competition law it should be by « developing a privacy-quality theory of harm ». To sum up, the goal of Article 102 TFUE is to deter and sanction abuse of dominance, and privacy issues can only be addressed if they constitute an exclusionary theory of harm (abuses which exclude competitors frm the market) or an exploitative abuse (where the dominant company exploit its market power). Regarding consumer harm, we should focus on

[1] EU Commission, Competition Policy for the digital era, 2019, p.7.

exploitative abuses. The zero-priced of online platforms creates strong incentives to collect data on consumers, more users' data the online platform collects, the better drives its algorithms.

Botta and Wiedemann (2019) identified three potential categories of exploitative abuses by data-driven dominant platforms:

- excessing pricing, taking the form in data markets of an excessive amount of personal data that online platforms request final consumers to provide in exchange for 'free' access to an online platform.
- Discriminatory pricing: with algorithms facilitating price discrimination among consumers via an analysis of personal data and by means of predictive modelling.
- Unfair trading conditions: when conditions imposed by a dominant platform to get users' consent to the processing of their personal data may be considered as 'unfair trading' under Art 102.

However, if the authors demonstrated that it is theoretically possible to enforce exploitative abuses in data markets, they also stressed all the challenges that would face a Competition Authority. And it would fair to add that introducing a stand-alone private action would be even more complicated than a follow-on action. It might also worth noting here that, even before the rise of the digital economy, exploitative abuses were already neglected in the EU practice of Competition law.

On the private enforcement and quantification of the harm, the directive 2014/104/EU establishes a right to full compensation intending to "place a person who has suffered harm in the position in which that person would have been had the infringement of competition law not been committed. It shall therefore cover the right to compensation for actual loss and for loss of profit, plus the payment of interest."

The directive does not provide insights on the quantification of harm. However, a guidance document was released the EU Commission in 2013 on the quantification of harm in antitrust cases. If this practical guide is very helpful, it does not tackle all the issues raised by the digital market, starting with the zero-priced markets.

In other words, a defendant who would have suffered an exploitative abuse from a social media company, because of the excessive collection and use of his data by their algorithms, would need to demonstrate the situation that would have prevailed without the infringement (i.e. establishing the counterfactual). This would be already tricky, without any transparent information on its data and without the possibility to identify a modification of quality from the social media services.

If the defendant succeeds in this first step, he would need to establish loss, expressed in monetary provisions, to support his claim for damages, without any insights on the value of his data or privacy.

Finally, it is worth pointing out that the eco-systems of these social media platforms, and the high performance of their algorithms thanks to the huge amount of data collected, also lead to a lock-in effect of the consumers.

II. Consumers biases when using social media platforms

Consumers are not aware of the amount of their data being collected and how these are used. Morever if they claim to be very concerned with their privacy, most of them are using these data-driven platforms: this is the so-called the privacy paradox (Aquisti, 2010).

Pinar Akman (2021) led an empirical study, with over 11,000 consumers surveyed about their use, perceptions, and understand of online platform services. Among the many very interesting results, one statistic from the survey is striking to our research. When asked about the business model of Google or Facebook, how users can access their services free of charge, only 42% of the respondents were aware that advertisers pay the platform provider to target advertisements.

So many papers tried to survey consumers' biases, behaviours, and explain the privacy paradox, that one researcher did a review of all of them (Kokolakis, 2017). Specifically, he reviewed the interpretations of the privacy paradox by the literature. Some authors defend a privacy calculus, individuals would perform a calculus between the expected loss of privacy and the potential gain of disclosure. This rational behaviour from the consumers is challenged by the literature, highlighting cognitive biases and heuristics in privacy decision making. Moreover, most people lack of cognitive ability and information to calculate privacy risks and disclosure benefits. The information asymmetry, characteristic of the relationship between social media platforms and the consumers, enhances the inability of the consumers to perform a privacy calculus.

Consumers' attitudes toward social media platforms can also indicate some biases in their behaviour. While users should be worried about their private information being collected and distributed, without any control mechanism. Pinar Akman (2021) study found that "The majority of respondents thinks that the big tech are "the source of much innovation that improves lives and are mostly source of goods (54%)".

To solve the privacy paradox, Potzsch (2008) supports privacy awareness and discuss the requirement on tools to achieve it. This paper supports his argument, which is developed in the following section.

III. Raising consumer awareness and incentivizing algorithm transparency from social media platforms

Following what we have learned in the previous section, we could follow the assumption that increasing the available information to the consumers would help to raise its awareness, with the effect of incentivizing platforms to a proportionate use of consumer's data with a high level of privacy.

Even if platforms were to agree to disclose details of what data is being collected, for what purpose, to whom and how their algorithms are performing, we may face another difficulty: consumers are unlikely to read what would be hundreds or thousands of pages of information. So the disclosure of information may be unnecessary in itself.

To understand the extent of this potential issue, we can draw a comparative analysis with a research that was exploring the presence of an informed minority of users by studying the browsing and shopping behaviour of online consumers in standard-from contracts (Bakos, Marotta-Wurgler, Trossen (2014)). The study intended to observe whether consumers would be to be informed about the terms of two types of software. They found that the highest fraction of readers among retail shoppers was 0.65 percent, and even among these readers, the average length on time spend on reading the end-user license agreement was 62.7 seconds (while it should require 8 to 10 minutes).

Following these results, they interpreted them on whether we could still observe an informed minority equilibrium. The informed minority equilibrium theory was developped by Schwartz and Wilde (1979). They show that if a sufficient amount of buyers are informed about the price and contract terms of a given product (the informed minority), sellers will offer the product at a competitive price to all buyers. In Bakos, Marotta-Wurgler, Trossen (2014) research, the authors found that there were too small amount of informed consumers to reach an equilibrium. These results have major consequences: because the buyers do not factor contract terms into their purchase decisions, sellers lack incentives to provide anything more than the minimally required legal protection.

The very little readership from consumers was also the core of a study from the EU Commission on terms and conditions when consumers buy products and services on the Internet (2016).

In the specific context of privacy policies and terms of service policies of social networking services, Obar and Oeldorf-Hirsch (2018), surveyed 543 participants (undergraduate students), which reveals that 74% of the participants skipped the privacy policies. They voluntarily inserted some shocking conditions, among which, the 93% of the participants who agreed to the terms of services also agreed to provide a first-born child as payment for the social networking access.

Now, back to our social media platforms users. They access these online services through the use of their data, also entering standard-form contracts. Very few consumers choose to be informed so the social media platforms have no incentive to provide a high level of privacy. Therefore, they can design algorithms with a maximum amount of consumer's data, damaging consumers privacy, this damage emphasized by the lock-in effect.

Online platforms behaviours towards data collection and use can be disciplined by either an informed minority equilibrium, reputational constraints or litigation threat. These three axes must be improved.

Fully aware of the consumers biases and behaviours on social media platforms, the next step of this paper would be to introduce an experiment that would help to design the best tool to inform the consumers on the use of their data by the algorithms. The optimal informational tool should be short enough and clear enough so that consumers would be incentivized to read it and be able to understand it. This tool should be accompanied by consequences inside the digital platform (the possibility to choose its own level of privacy without a loss of quality in the online services). In the eventuality of an abuse of dominance by the digital platforms, this informational tool should help quantifying the damage suffered by the users.

Bibliography:

AQUISTI, A., The Economics of Personal data and the economics of privacy, Background paper #3, OECD Conference center, 2010.

AKMAN, P., 2021. A Web Of Paradoxes: Empirical Evidence On Online Platform Users And Implications For Competition And Regulation In Digital Markets. *Available at SSRN 3835280.*

BAKOS, Y., MAROTTA-WURGLER, F. and TROSSEN, D.R., 2014. Does anyone read the fine print? Consumer attention to standard-form contracts. *The Journal of Legal Studies*, *43*(1), pp.1-35.

BOTTA, M. and WIEDEMANN, K., 2019. Exploitative conducts in digital markets: Time for a discussion after the Facebook Decision. *Journal of European Competition Law & Practice*, *10*(8), pp.465-478.

BOUGETTE, P., BUDZINSKI, O. and MARTY, F., 2019. Exploitative abuse and abuse of economic dependence: What can we learn from an industrial organization approach?. *Revue d'economie politique*, *129*(2), pp.261-286.

BUITEN, M.C., 2020. Exploitative abuses in digital markets: between competition law and data protection law. *Journal of Antitrust Enforcement*.

GAL, M.S. and ELKIN-KOREN, N., 2016. Algorithmic consumers. *Harv. JL & Tech.*, *30*, p.309.

GAL, M. and PETIT, N., 2020. Radical Restorative Remedies for Digital Markets. *Berkeley Technology Law Journal*, *37*(1), p.2021.

KOKOLAKIS, S., 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security*, *64*, pp.122-134.

MCAFEE, R.P., MIALON, H.M. and MIALON, S.H., 2008. Private v. public antitrust enforcement: A strategic analysis. *Journal of Public Economics*, *92*(10-11), pp.1863-1875.

NAZZINI, R. (2019), Privacy and Antitrust: Searching for the (Hopefully Not Yet Lost) Soul of Competition Law in the EU after the German *Facebook* Decision, edited by T. Schrepel, S. Sadden & J. Roth (CPI), 2019.

NEWMAN, J.M., 2015. Antitrust in zero-price markets: Foundations. *University of Pennsylvania Law Review*, pp.149-206.

NEWMAN, J.M., 2016. Antitrust in zero-price markets: applications. *Wash. UL Rev.*, *94*, p.49.

OBAR, J.A. and OELDORF-HIRSCH, A., 2020. The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, *23*(1), pp.128-147.

PÖTZSCH, S., 2008, September. Privacy awareness: A means to solve the privacy paradox?. In *IFIP Summer School on the Future of Identity in the Information Society* (pp. 226-236). Springer, Berlin, Heidelberg.