

NOT ALL E-COMMERCE BUSINESSES ARE BORN EQUAL: IMPLICATIONS FOR PRIVACY REGULATION



BY JORGE PADILLA, SALVATORE PICCOLO, ALBERT RIERA & HELDER VASCONCELOS¹



¹ The authors are economists at Compass Lexecon. The opinions in this paper are the authors' sole responsibility. Please send your comments to: jpadilla@compasslexecon.com.

CPI ANTITRUST CHRONICLE

February 2024

THEORIES OF HARM BECAUSE OF DATA

By Christian Rusche



DATA IN THE DIGITAL ECONOMY: THE “ANTI-HERO” OF ANTITRUST OR JUST “BAD REPUTATION?”

By Kristof Zetenyi & Dheeraj Chaudhary



FROM DATA MYTHS TO DATA REALITY: WHAT GENERATIVE AI CAN TELL US ABOUT COMPETITION POLICY (AND VICE VERSA)

By Geoffrey A. Manne & Dirk Auer



NOT ALL E-COMMERCE BUSINESSES ARE BORN EQUAL: IMPLICATIONS FOR PRIVACY REGULATION

By Jorge Padilla, Salvatore Piccolo, Albert Riera & Helder Vasconcelos



THE ECONOMICS OF THE DATA-DRIVEN ECONOMY AND THE DEMAND FOR ANTITRUST

By Dan Ciuriak



CAN DATA REGULATION RESHAPE THE SHORT-TERM RENTAL MARKET?

By Ginger Zhe Jin, Liad Wagman & Mengyi Zhong



DATA AT THE FRONTLINE: THE ECONOMIC THEORIES OF DATA-CENTRIC ANTITRUST ENFORCEMENT

By James Mellsop, Veronica Postal & John Scalf



Visit www.competitionpolicyinternational.com for access to these articles and more!

CPI Antitrust Chronicle February 2024

www.competitionpolicyinternational.com

NOT ALL E-COMMERCE BUSINESSES ARE BORN EQUAL: IMPLICATIONS FOR PRIVACY REGULATION

By Jorge Padilla, Salvatore Piccolo, Albert Riera & Helder Vasconcelos

This paper discusses privacy concerns and privacy regulation under two different e-commerce business models: a pure marketplace and a hybrid marketplace. In previous papers we have found that the nature of the business model has crucial implications for the scope of the private information collected and disclosed by the online company; e.g. hybrid marketplaces have fewer incentives to collect and disclose than pure marketplaces in many circumstances. In this paper we explore the implications of these findings for privacy regulation. Interventions that may be required for pure intermediation platforms may not be justified when applied to hybrid marketplaces.

Scan to Stay Connected!

Scan or click here to sign up for CPI's **FREE** daily newsletter.



I. INTRODUCTION

Digital e-commerce platforms have unambiguously contributed to spreading market coverage by reaching consumers that would otherwise not be served or, at best, would incur rather high search costs to make their purchases. Thanks to their digital and two-sided nature, those platforms have privileged access to a massive amount of user data and often track their users' online behavior (e.g. browsing patterns, shopping preferences, and even, sometimes, social interactions). The collection and subsequent management of this data is justified by the need to build users' profiles and efficiently deliver ads to the relevant user segments (a process which has been termed targeting advertising) or to identify missing varieties that consumers would likely value.

Apart from making own use of the collected data, some online platforms may profit by reselling their users' individual data to third parties, which may then use this information for commercial, marketing, or, in the worst cases, illegal purposes. This naturally gives rise to privacy concerns. Consumers are more likely to express concern about the nature and amount of data a given e-commerce business extracts if they anticipate that such information may be transmitted to third parties, especially if they believe that their information may land in the wrong hands.

Because the success of e-commerce platforms depends on their ability to attract users so that they can then recruit third-party sellers, e-commerce platforms have an incentive to mitigate their users' privacy concerns by limiting the amount of user information that they acquire and disclose. That user-friendly motivation is in part offset by the platforms' incentive to monetize their customer bases, which induces them to collect and disclose more information than their users would find optimal. Sellers in a platform will make more money, and the platform will thus obtain higher access fee revenues, if they can price discriminate and/or target their marketing efforts more effectively. That in turn will be easier when the platform collects and discloses more information about its users.

The balance of those two incentives determines the amount of information collected and disclosed. In two recent economic theory papers we find that the precise business organization of an e-commerce platform impacts on its incentives to acquire, process and resell consumer data to third parties.² We distinguish two different online business models: the "marketplace model," where the platform intermediates between sellers and buyers, and charges sellers an access fee; and the "hybrid model," where the platform acts both as a marketplace and as a retailer operating in that marketplace. The marketplace model is, therefore, a pure intermediation model, whereas in the hybrid model the platform is both an intermediary and a seller.

We find that the platform's decision to gather and disclose consumers' information in the two business models crucially depends on (a) the level of intra-platform competition (as measured by the degree of substitutability between the platform's own private label and the remaining products sold by third-party sellers present in its marketplace), and (b) the platform's bargaining position vis-à-vis the independent sellers. When intra-platform competition is intense and the platform has significant bargaining power, then it acquires and disseminates less accurate information when operating as a hybrid marketplace.

In this paper we consider the regulatory implications of these findings. More specifically, we assess their implications for the design and implementation of privacy policy. Interventions that may be required for pure intermediation platforms may not be justified when applied to hybrid marketplaces. Because not all multi-sided online businesses are born equal, public policy cannot treat them equally either. Policymakers, both regulators and antitrust authorities, must be aware of these differences and factor them in when designing their policies. Thus, for example, while hybrid marketplaces can be trusted to limit the collection and sharing of end-users' information in circumstances where that business has significant bargaining power (and may even play a gatekeeper role) and can choose how close its own branded products are to those sold by third-party sellers in the marketplace, this is not the case of pure marketplace platforms.

We also extend the analysis in previous papers to consider the incentives of online ad-platforms to gather and disclose user information; we find that those are necessarily more likely to give rise to privacy concerns. Marketplaces make money from sellers and buyers and their incentives regarding the buyers' data collection and dissemination reflect both the preferences of sellers and buyers. Instead, online ad-platforms only raise revenue from sellers and, therefore, their incentives are to extract as much data as possible and sell it at the highest possible price without as much monitoring of its use.

In sum, our analysis suggests that the only sensible way of approaching privacy regulation in digital markets is a case-by-case approach, which takes account of the business model at stake, the bargaining power of the platform and the strength of competition at that platform.

² See Padilla, J., Piccolo, S., Riera, A. & Vasconcelos, H. (2020a), "Alternative Business Models, Information Design and Privacy Concerns," mimeo, University of Bergamo. See Padilla, J., Piccolo, S., Riera, A. & H. Vasconcelos (2020b) "On the Social Value of Consumer Data in Hybrid Marketplaces," mimeo, University of Bergamo.

The remainder of this paper is organized as follows. In Section II we discuss the pros and cons of data collection from the viewpoint of consumers. In Section III we discuss arguments in favor and against the strict protection of privacy by restricting the amount of user information that platforms can collect and disclose. We explain why the so-called privacy paradox does not justify a complete *laissez faire* approach to data collection and disclosure, and conclude that such regulations need to be content dependent and conditional on the business organization of the platforms under scrutiny. In Section IV we discuss their differential incentives to collect and disclose users' private information for pure and hybrid marketplaces. In Section V we extend the previous discussion to assess the incentives of online advertising platforms. Section VI presents the implications for privacy regulation and Section VII concludes.

II. PROS AND CONS OF DATA COLLECTION AND DISCLOSURE

The cost of storing, processing and transmitting data has experienced an exponential decline over the last few years. Currently, the most valuable companies in the world, Google, Apple, Facebook, Amazon, and Microsoft rely on business models for which data is an important driver of their value propositions. Firms like Google or Facebook collect data about their users in order to sell targeted advertising space to their clients. Online retailers, such as Amazon, collect data about their customers in order to learn about their preferences and enhance their product offering. Azure, Microsoft's cloud division, is nowadays the firm's fastest growing revenue source offering data analysis, data storage or cloud computing.³ Data is not only valuable to the Big Tech giants, there is a broad range of companies of all sizes whose business models rely on the collection, processing and/or dissemination of data: e.g. data brokers, app developers, data security and data visualization providers. It is estimated that at the end of 2020 in Europe the data industry will be worth around €740 billion and will employ 10.4 million workers.⁴

A. Consumer Benefits

Undoubtedly, consumers have obtained a share of the value generated through their data in several ways. Firstly, a myriad of valuable services such as search engines, instant messaging or online video services are available for free to anyone with internet access, which is nearly 60% of the world population in 2020.⁵ Secondly, by gathering information from consumers, firms can learn about their preferences and therefore offer to them, or even develop for them, better (targeted) products and services. Thirdly, in some markets, such as the credit market or the job market, access to personal data can reduce market frictions to the benefit of consumers. For instance, empirical studies in the US credit market demonstrate that the use of consumer financial data facilitates the screening of borrowers, leading to lower prices for mortgages.⁶ As a final example, sharing personal data can allow society to solve coordination problems, such as improving traffic congestion or helping health authorities managing diseases outbreaks, such as the Covid-19 pandemic.

B. Privacy Concerns

However, the growth of the digital economy has been accompanied by increasing privacy concerns. Although these are varied, most can be grouped into four types. Firstly, internet users worry about data breaches and misuses of their personal data. Certainly, well-known hacking episodes such as the Ashley Madison case, where hackers stole the financial and sexual data of 32 million users have not contributed positively to the users' perception of security, nor the fact that 22 percent of online users have been subject to some form of credit fraud.⁷

Secondly, harnessing personal data may allow firms to learn about the willingness to pay of their customers and engage in first-degree price discrimination, whereby different customers are charged different prices for the same product or service according to their individual valuations. Firms may thus use customer data to extract all the economic rents generated by their customers' transactions. Price discrimination will reduce consumer welfare when consumers are captive due to, for example, switching or searching costs and, more generally, in the presence of market power.

3 In 2019 Azure's revenue growth was 72%, according to Microsoft's *Annual Report* (2019), available at <https://www.microsoft.com/investor/reports/ar19/index.html>, last accessed on April 29, 2020.

4 European Commission (2017), *The European Data Market Study: Final Report*, available at <http://datalandscape.eu/study-reports/european-data-market-study-final-report>, last accessed on April 29, 2020.

5 See <https://www.statista.com/statistics/617136/digital-population-worldwide/>, last accessed on April 29, 2020.

6 Kim, J. & Wagman, L., (2015), "Screening Incentives and Privacy Protection in Financial Markets: A Theoretical and Empirical Analysis," *RAND Journal of Economics*, Vol. 46.1, pp. 1-22.

7 See e.g. Brooke, S. & Véliz, C. (2020), "Views on Privacy: A Survey," Research Project on Data, Privacy, and the Individual, Center for the Governance of Change, IE University, 2019, available at www.ie.edu/cgc/research/data-privacy-individual, last accessed on April 29, 2020, for an online survey about individuals view on privacy where it is concluded that privacy-related negative experiences online are extremely common (e.g. the average respondent had more than one bad privacy-related experience, 23 percent reported having had experienced an unauthorized access to their online account, and 22 percent have had their credit card number stolen or have experienced bank fraud or unauthorized purchases from their account.)

Finally, while in some cases access to data can eliminate information asymmetries and result in enhanced consumer welfare, as in the credit market, information asymmetries can sometimes be desirable. An example is genetic data. Access to an individual's genetic data can be beneficial to society, as it may drive breakthroughs in medical research. However, it may also allow health insurance companies or employers to discriminate against individuals with a high risk of developing a genetic disorder. Such discrimination might not only be unacceptable from a moral perspective, but can also be economically inefficient.⁸ Traditionally, this problem has been resolved through strict privacy laws regarding access to patients' medical records. Currently however, there is the risk that individual's private health information might be inferred from what users type on search engines, what they buy from online marketplaces, or what they post on social networks.

III. PRIVACY PROTECTION IN PLATFORMS

The increasing importance of data as a key input, which empowers online platforms to extract valuable insights and knowledge from their consumers, and the legitimate concerns of some consumers, who see their privacy comprised, has given rise to an intense debate about the adoption of instruments and policies aiming at defending consumer trust and privacy. At the European level, it is important to highlight the introduction of the General Data Protection Regulation (henceforth, "GDPR"),⁹ which sets rules protecting citizens in what concerns the processing and the free movement of their personal data. These rules aim at guaranteeing that firms collect and process personal data in a way that protects consumers privacy appropriately (e.g. by keeping the data encrypted or by anonymizing it).¹⁰ The debate is, however, ongoing, as some stakeholders push for further privacy protection measures, while others defend a non-interventionist approach.

A. Arguments Against Privacy Regulation

Academic research has found what it appears to be an inconsistency between individuals' valuation of privacy and their observed behavior regarding the dissemination of their personal data.¹¹ When asked about how much they care about protecting their privacy, responses tend to put a high value in the protection of personal data, yet, arguably, observed behavior indicates otherwise, as many people seem willing to trade their personal data for very little in exchange, and seem unwilling to employ available technology capable to protect their privacy.¹²

This so-called privacy paradox has been rationalized in different ways (see below). Some argue that people's actions (or revealed preferences) provide more accurate information about their true regard for privacy than their responses (or declared preferences) to surveys. The claim is that their true regard for privacy is low: while they express concern to survey takers, their observed behavior reveals that their concerns must be low compared to the benefits that they obtain from sharing their data. In this connection, it is often noted that when surveys ask about the willingness seem willing to pay to preserve it.¹³

This interpretation of the evidence is then used to claim that consumers adhering to online platforms value (at least implicitly) the benefits obtained by sharing their data with those platforms (e.g. gaining access to free services) more any potential privacy costs they may suffer.

Those costs, mostly non-pecuniary, need not be negligible, of course. Consumers lose control of their personal data when adhering to, or using the services of, an online platform, as they do not know how the data will be used and/or by whom.¹⁴ They may also be confronted with

8 Consider a group of risk averse individuals that are about to take a genetic test that will predict whether they will develop an illness that will require expensive medical treatment. As they are risk averse, *ex ante* (i.e. before the genetic test is performed) it would be welfare maximizing for all of them to buy medical insurance and share the risk. *Ex post*, however, only the individuals that tested positive would be willing to buy insurance. However, insurance would not be available as those individuals that tested negative would no longer be interested in purchasing medical insurance for a disease that they know will not develop. Thus, access to information (i.e. the genetic test) eliminates the possibility of medical insurance, which is inefficient from an *ex ante* perspective.

9 Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

10 Another example of a regulatory intervention to protect privacy is the California Consumer Privacy Act (CCPA) of 2018, a state statute intended to enhance privacy rights and consumer protection for residents of California.

11 Acquisti, A., Taylor, C. & Wagman, L., (2016), "The Economics of Privacy," *Journal of Economic Literature*, Vol. 54(2), pp. 442—492 and references therein.

12 Grunes, A.P. & Stucke, M., (2015), "No Mistake About It: The Important Role of Antitrust in the Era of Big Data," *Antitrust Source*, pp. 1-14, available at <https://pdfs.semanticscholar.org/e867/9a20c3d5f316fdfaf4b94d43390b4c5dd71.pdf>, last accessed April 29, 2020.

13 Strahilevitz, L. J. & Kugler, M. B., (2016), "Is Privacy Policy Language Irrelevant to Consumers?," *Journal of Legal Studies*, Vol. 45(S2), pp. S69-S95.

14 See e.g. OECD. (2016), "Big data: Bringing competition policy to the digital era – Background Note by the Secretariat," OECD Competition Roundtables; and also OECD (2019a), "Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies," OECD Publishing, Paris.

large amounts of intrusive advertising and/or subject to behavioral-based price discrimination.¹⁵ Further, and very importantly, due to the growth in use and value of data, personal data breaches and other privacy violations have become more common.

Yet, it is argued, data is the new currency on the internet,¹⁶ and consumers appear to be willing to trade their data for free online services for free (e.g. social networks and search engines). Their choices are a clear signal that the exchange rate between the intrinsic value attributed by consumers to those services, on the one hand, and the data they share with service providers, on the other, is fair.

Another argument used against the adoption of strict privacy protection rules is that the market regulates itself. Consumers wishing to protect their privacy have access to, and can make use of, a wide range of instruments and privacy enhancing technologies (e.g. anonymous browsing, more secure payment tools, cookie deletion software, etc.). They may also embark on and reward online platforms that offer greater privacy protection.¹⁷ In response, some online platforms may choose to compete by offering enhanced privacy protection, thereby introducing a quality dimension within inter-platform competition.¹⁸

This competition process explains, according to the advocates of self-regulation arguments, why for example Microsoft announced in 2013 that it would not use the content of Outlook messages to show targeted ads as a strategy to compete with Gmail and its practices of scanning through private emails for keywords that can be used to sell personalized ads. It may also explain why online businesses, such as Amazon,¹⁹ refrain from using personalized price-discrimination strategies, since they are likely to antagonize customers and result in high reputational costs. A platform's incentive to use personal information for price discrimination purposes will be reduced by the anticipated loss of business if consumers detect and punish that discriminatory behavior. Indeed, there is evidence that this retaliatory mechanism operates in practice.²⁰ Knowing this, the platform's reaction will likely be to restrict the volume of information collected from its end-users, as well as its scope, limiting or even terminating price discrimination strategies, with positive side implications on the protection of consumers' privacy.

A recurrent argument against the strict regulation of privacy protection is that the costs of such regulations may outweigh their potential benefits if, for example, enhancing privacy protection may increase market frictions. Regulations like GDPR are a case in point. Even though its Article 20 on the "right of data portability" grants individuals the right to receive the personal data provided to a given data controller (say, an online platform) and transmit those data to another controller without hindrance, some have argued that the expected competition enhancing effects, resulting from lower switching costs and lock-in effects, may not materialize. Since this regulation applies broadly to all types of firms, therefore not being restricted to those enjoying a dominant position, small and medium enterprises ("SMEs"), and even start-ups, must also incur the costs of the investment needed to ensure that the data in their possession can be ported, if requested.

15 As argued by Stucke, M.E. & A. Ezrachi (2016), *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy*, Harvard University Press, United States, "Companies are increasingly adopting business models that rely on personal data as a key input. (...) companies offer individuals free services with the aim of acquiring valuable personal data to assist advertisers to better target them with behavioural advertising." (p. 20) Along related lines, at OECD (2016), *op. cit.*, it is highlighted that online platforms, "such as search engines or social networks, typically provide a set of 'free' services that are subsidised by advertising sold on a 'per-click' basis. (...) [In addition, a]rguably, consumers also pay by submitting their data, either indirectly – through the website recording clicks for online searches or shopping – or directly – through entering personal data into an online form," (p. 12.)

16 As the EU Competition Commissioner emphasized: "These incredibly powerful tools, like search engines and social media, are available for free. In many cases, that's because we as consumers have a new currency that we can use to pay for them – our data." (See Vestager, M. (2016), "Competition in a big data world," *Speech at the DLD 16*, Munich, 17 January 2016).

17 See Cooper, J. C. (2013), "Privacy and Antitrust: Underpants Gnomes, the First Amendment, and Subjectivity," *George Mason Law Review*, Vol. 20.4, pp. 1129 – 1146. Along related lines and while investigating how the trade-off between (targeting) advertising effectiveness and user privacy concerns affects competition between online advertising platforms, Gal-Or, E., Gal-Or, R., & Penmetsa, N., (2018), "The Role of User Privacy Concerns in Shaping Competition among Platforms," *Information Systems Research*, Vol. 29 (3), pp. 698-722, claim that consumers react differently to target ads: while some consumers are averse to targeted advertising and to share personal information, others prefer to see relevant (rather than random) ads even at the expense of the potential negative consequences resulting from sharing personal information (e.g. unforeseen risks such as data breaches or leakages).

18 In fact, privacy considerations can fall within the context of non-price quality competition. See e.g. Lande, R.H., (2008), "The Microsoft-Yahoo Merger: Yes, Privacy is an Antitrust Concern, 714 FTC WATCH 9, February 25, 2008 (available for download at: https://scholarworks.law.ubalt.edu/all_fac/718/); Kimmel, L. & Kestenbaum, K., (2014), "What's Up with WhatsApp?: A Transatlantic View on Privacy and Merger Enforcement in Digital Markets," *Antitrust Magazine*, Vol. 29.1; and also Stucke, M. E., & Grunes, A. P., (2016), *Big data and Competition Policy*, Oxford University Press, New York.

19 This then explains why in 2001 Jeff Bezos, Amazon's CEO, committed to never test prices based on customer demographics. No further evidence of Amazon engaging in price discrimination has been found ever since. See <https://www.bizjournals.com/seattle/stories/2000/09/25/daily21.html>. Last accessed on 29 April 2020.

20 Anderson, E.T. & Simester, D.I., (2008), "Price Stickiness and Customer Antagonism," *Quarterly Journal of Economics*, Vol. 125(2), pp. 729-765, use a 28-month randomized field experiment involving over 50,000 customers to investigate how customers react if they buy a product and later observe the same retailer selling it for less. They find that customers react by making fewer subsequent purchases from the firm. The effect is largest among the firm's most valuable customers: those whose prior purchases were most recent and at the highest prices.

SMEs and start-ups may thus see hurt their capacity to compete head-to-head with their larger rivals as well as their incentives to invest in data-driven innovations.²¹ Put it another way, there is the risk that the implementation of the specific provisions of GDPR may end up having perverse anti-competitive effects.²²

B. Arguments in Favor of Privacy Protection

Supporters of privacy public policy protection, on the other hand, deny the so-called privacy paradox, and point to the existence of several market failures that arise around data. These usually relate to imperfect information, externalities and market concentration issues.

1. The So-called Privacy Paradox

Several commentators have explained why the true valuation of privacy cannot be accurately inferred from individual's actions since those choices are driven by several behavioral biases. Many internet users do not fully understand how much data is being collected from them and for what purpose. And even those who are aware may not react to such understanding because of bounded rationality, such as hyperbolic discounting,²³ which causes them to procrastinate in the defense of their privacy. Or they may rationally choose not to pay attention, given the complexity of accurately assessing the costs and benefits of their actions.²⁴

Others maintain that there is no inconsistency behind the apparently contradictory statements on privacy made by individuals and their observed behavior. It is through the flawed generalization of findings from different specific contexts that the paradox emerges, when in fact the underlying factual evidence is consistent, once the different contexts in which it has been collected are considered. As Daniel Solove points,

*Often, stated preferences are not articulated to the same degree of specificity as people's observed behaviour. The behaviour might appear to be in conflict with a stated preference when, in fact, the inconsistency is due to the false assumption that the stated preference encompasses the risks undertaken by the behaviour. There are many privacy issues, and not all might trouble everyone.*²⁵

2. Market Failures

Some defend privacy protection and enforcement by reference to moral hazard arguments. When deciding on how much information to collect, share with or even sell to third parties, an online business may be willing to inefficiently risk exposing its consumers to eventual privacy violations, as it does not bear the full cost of that risk. Consumers may not be able to assess the magnitude of this risk due to the asymmetry of information between them and the platform: the online platform (the risk-taking party) knows more about the consequences of its intentions and decisions than its consumers (who are the ones exposed to privacy breaches and violations). Consumers excessive exposure to those risks then naturally gives rise to incidents of improper use of personal data, which have contributed to increasing calls for governments to protect consumers' data and privacy.²⁶

Relatedly, online platforms may end up collecting and sharing too much personal information if they do not fully internalize the harm that their decisions will have for their consumers. Likewise, an online platform might not invest enough in information security and safety, as it does not fully internalize the costs of potential data breaches or leakages. Moreover, evidence suggests that data breaches can cause company market valuations to drop on the period close to the announcement of the breach, but the negative shock on valuation disappears in a short period of time.²⁷

21 See OECD (2014), "Data-driven Innovation for Growth and Well-being," Interim Synthesis Report, OECD Publications, Paris.

22 See Section 4.1.3 in OECD. (2016), *op. cit.*, and the references cited therein.

23 Acquisti A., & Grossklags J., (2004), "Privacy Attitudes and Privacy Behaviour," in Camp L.J. & Lewis S. (eds.) *Economics of Information Security. Advances in Information Security*, Vol 12. Springer, Boston, MA

24 Marreirosa, H., Tonin, M., Vlassopoulos, M., & Schraefela, M.C., (2017), "Now that you mention it": A survey experiment on information, inattention and online privacy," *Journal of Economic Behaviour and Organization*, Vol. 140, pp. 1-17

25 Solove, D. J. (2020), "The Myth of the Privacy Paradox," GW Law School Public Law and Legal Theory Paper No. 2020-10.

26 See Winegar, A.G. & Sunstein, C.R., (2019), "How Much Is Data Privacy Worth? A Preliminary Investigation," *Journal of Consumer Policy*, vol. 42, 425-440.

27 See Acquisti, A., Friedman, A. & Telang, R., (2006), "Is There a Cost to Privacy Breaches? An event study," *Proceedings of the Twenty Seventh International Conference on Information Systems and Workshop on the Economics of Information Security 2006*.

This may reflect the fact that consumers might have very limited and imprecise information on the data security record of competing businesses, which limits their ability to reward data secure platforms while punishing insecure ones. Consumers might not be aware that data is collected from them. Even if they are, they might not understand which data is precisely being collected and thus may be providing more data than they intend to.²⁸ They may also ignore the purpose for which that data are being collected, as data might be used in ways not anticipated at the time of collection.²⁹ Consumers are rarely informed in all detail about how their data might be used or shared with third-parties.³⁰

Further, there is evidence that most customers do not read privacy policies. And if they do, they do not fully understand them.³¹ In addition, there is evidence of high dispersion in consumers' valuation of data privacy as well as of the fact that consumers typically have poor understanding about the likelihood of privacy violations due to information misuse. This asymmetry of information between consumers and online platforms regarding data collection, usage, transmission and privacy policies then enables the online platforms to invest less in privacy than what would be socially optimal.

Data externalities also justify the public regulation of privacy protection. Data about an individual are not only informative about that specific individual, but also about other individuals who are like her in some relevant dimension. Hence, when consumers provide data about themselves, they might generate positive or negative externalities on other consumers. For example, this informational externality is when data provided by some consumers unconcerned about their privacy is used to infer information about other consumers who are concerned about privacy and would not have disclosed such information about themselves. Each consumer's decision to provide information reflects the balancing of her private benefits and costs, and naturally does not factor in the implications of such a choice on the welfare of others. So even when an individual may be satisfied with the compensation received for the data surrendered (e.g. the quality of the free services obtained), such a compensation is insufficient from a social viewpoint. Because individual data are therefore too cheap, online companies may end up gathering excessive amounts of information.³²

Furthermore, because some firms, due to their peculiar business models, hold far more data and have greater ability to analyze and use such data than others, there is a risk that they can leverage such data advantages anticompetitively to monopolize adjacent markets and entrench their quasi-monopoly positions in the market where the data was originally collected.³³ Such strategies are possible because dominant firms may coerce their customers into accepting policy terms that allow them to use their data across different markets and for purposes other than the provision of those services which motivated the exchange of data in the first place.³⁴ In that case, it may prove socially optimal to limit the ability of online firms to extract such concessions from their customers, which can be achieved by regulating their privacy policies so that data cannot be used across markets.

28 For example, location tracking coordinates provided by cell phones or IP addresses used when browsing the internet might be collected (and used) without the consumer being aware of it.

29 See OECD (2019b), "Data in the Digital Age," OECD Going Digital Policy Note, March 2019, OECD, Paris. See also Winegar & Sunstein, (2019), *op. cit.*, for a survey involving 2,416 Americans, where it is found that the consumers lack a clear knowledge of how their data is collected, secured, and used online.

30 See e.g. Véliz, C., (2020), "Data, Privacy and the Individual: Privacy Matters," IE University – Centre for the Governance of Change, where it is pointed out that with the 2018 Cambridge Analytica scandal it has become clear that personal data is often shared without individuals' knowledge and consent, and many times for unacceptable purposes, such as influencing elections. Along related lines, Brooke, S. & Véliz, C. (2020), *op. cit.*, stress that respondents to their online survey think that the most unacceptable uses of personal data by companies are thought to be selling it to third parties, influencing voting, and engaging in price discrimination.

31 See e.g. McDonald, A. M. & Crano, L. F., (2008), "The Cost of Reading Privacy Policies," *Journal of Law and Policy for the Information Society*, vol. 4, no. 3, 543-568, 543-897; and Anton, A. I., Earp, J.B, He, Q., Stuebeam, W. H., Bolchini, D. & Jensen, C., (2004), "Financial Privacy Policies And The Need For Standardization," *IEEE Security and Privacy*, vol. 2 (2), 36-45.

32 See Bergemann, D. & Bonatti, A. (2019), "The Economics of Social Data: An Introduction," (March 26, 2019), Cowles Foundation Discussion Paper No. 2171, available at SSRN: <https://ssrn.com/abstract=3360352>. See also Acemoglu, D. Makhdoumi, A. Malekian, A. & Ozdaglar, A. (2019), "Too Much Data: Prices and Inefficiencies in Data Markets," September 10, 2019, available at <https://economics.mit.edu/files/17760>.

33 See OECD (2019b), *op. cit.*, where it is noted, in particular, that "Data savvy firms may have a comparative advantage enabling and inducing them to broaden their scope and expand to additional sectors either as new entrants or through acquisitions of existing firms."

34 See Condorelli, D. & Padilla, J., (2020), "Harnessing Platform Envelopment through Privacy Policy Tying," *Journal of Competition Law and Economics*, forthcoming. See also Portuguese Competition Authority (2019), "Digital ecosystems, Big Data and Algorithms," Issues Paper, July 2019, where it is defended that: "It is important to consider the specificities of platforms when assessing the impact of certain strategies on competition. In the context of digital ecosystems, for example, bundling and tying strategies may have an amplified negative effect on the ability and incentives of new competitors to enter and innovate in the market. These strategies may aim to reduce potential competition and leverage market power." (p. 26).

3. One Size Does Not Fit All

Consistently with our findings above, Acquisti et. al. (2016), in a remarkably exhaustive literature survey on the economics of privacy,³⁵ conclude that:

Both economic theory and empirical analysis of privacy expose varying scenarios. In some, privacy protection can decrease individual and societal welfare; in others, privacy protection enhances them. Thus, it is not possible to conclude unambiguously whether privacy protection entails a net “positive” or “negative” change in purely economic terms: its impact is context specific.

The right choice regarding the enforcement of privacy protection will ultimately depend on the balancing the costs and benefits of such a policy. The outcome of such an exercise will likely depend on the specific features of the market in question. As recently emphasized by the OECD (2019c),³⁶

Policy makers should avoid the ‘data policy pitfall’ of seeking one-size-fits-all solutions; data should not be treated as a monolithic entity. The value of data access and sharing depends on the type of data and the context in which they are re-used, including the social, economic, and cultural environment in which activities take place.

Our companion paper Padilla et. al. (2020) contributes to this precisely by discussing how the economic context in which online platforms operate affects their data collection and dissemination strategies, in a setting where consumers care about the privacy implications of such activities.³⁷ By so doing, we show that privacy concerns are context dependent: the precise business organization of an e-commerce platform crucially impacts on its incentives to acquire, process and share consumer data with third parties.

IV. PRIVACY CONCERNS UNDER ALTERNATIVE BUSINESS MODELS: PURE V. HYBRID MARKETPLACES

Digital platforms have largely expanded the available sources, volume and usage of personal data. Their role as large data aggregators as well as data brokers is, therefore, assuming increasing relevance.³⁸ Of particular importance is then the understanding of the underlying incentives of digital platforms, including marketplaces, to engage in the collection of raw data provided by their consumers, and to process and possibly redistribute that data amongst third-party sellers active within their marketplaces.³⁹

In principle, the difference in business models may have important implications for (i) the amount and nature of the end-user information that is collected, (ii) the way in which that information is handled, and (iii) the amount and quality of the information disclosed. The context in which the online business operates may, for example, influence its decision on whether to degrade the information transmitted to third parties (e.g. by revealing only a portion of the collected information and/or a less precise version of it).⁴⁰

In what follows we consider the relative magnitude of users’ privacy concerns under the pure marketplace model and the hybrid marketplace model. We first discuss the logic and limits of each of these two business models, and then discuss their differential incentives to collect and disclose user information.

35 See Acquisti, A., C. Taylor, & Wagman, L., (2016), “The Economics of Privacy,” *Journal of Economic Literature*, 54, pp. 442-492.

36 See OECD (2019c), “Enhancing Access to and Sharing of Data Reconciling Risks and Benefits for Data Re-use across Societies,” OECD Publishing, November 2019, Paris.

37 See Padilla, J., Piccolo, S., Riera, A. & Vasconcelos, H. (2020), “Alternative Business Models, Information Design and Privacy Concerns,” *mimeo*, University of Bergamo.

38 For a comprehensive survey on information markets, highlighting the central role played by data intermediaries, see Bergemann, D., & Bonatti, A., (2019), “Markets for Information: An Introduction,” *Annual Review of Economics*, Vol. 11, pp. 85-107, and the references cited therein.

39 Bergemann, D., and Bonatti, A., (2018), “Markets for Information,” Discussion Paper, Yale University and MIT, identify under which informational environments the data intermediary has incentives to lower the informativeness of the transmitted data by adding an aggregate noise into it. Other contributions where the information seller can restrict access to the information possessed as well as sell noisier versions of that information, include Admati, A. R., & Pfleiderer, P., (1986), “A monopolistic market for information,” *Journal of Economic Theory*, 39(2), pp. 400-438, Admati, A. R., & Pfleiderer, P., (1990), “Direct and indirect sale of information,” *Econometrica*, 58(4), pp. 901-928, Bergemann, D., & S. Morris (2013), “Robust Predictions in Games with Incomplete Information,” *Econometrica*, 81, pp. 1251-1308, and Bimpikis, K., D. Cramis, & A. Tahbaz-Salehi (2019), “Information Sale and Competition,” *Management Science*, Vol. 65, Issue 6, pp. 2646-2664.

40 See Montes, R., Sand-Zantman, W., & Valletti, T., (2019), “The Value of Personal Information in Online Markets with Endogenous Privacy,” *Management Science*, Vol. 65, no. 3, pp.1342-1362.

A. Pure v. Hybrid Marketplaces

While there is an extensive literature focusing on the comparison between the “reseller” model, where a firm purchases different products from third-party sellers and resells them acting as a retailer, and the pure marketplace model,⁴¹ much less attention has been paid to the comparison between pure and hybrid marketplaces.

Increasing traffic within a marketplace is a key dimension for its sustainability and attractiveness vis-à-vis other distribution channels. The problem, however, is that the marketplace and the independent sellers using it generally have misaligned interests with regards to the spectrum of varieties that should be available within the platform’s marketplace. In particular, third-party sellers using the marketplace to distribute their products may not have the incentive to offer as many varieties through that platform as they do through other channels (e.g. their own direct distribution channels). In addition, when independent sellers have unilateral market power or when they engage in tacit coordinated behavior, the resulting higher prices create an environment of artificial scarcity within the marketplace that negatively affects the volume of traffic and will, therefore, hurt the platform not only in the segment of demand in which those sellers are active but also in other segments.

Marketplaces have thus clear incentives to monitor their competitors to quickly detect competitive threats to their ecosystem. These initiatives may then naturally trigger strategic defensive actions in order to avoid that unilateral or coordinated behavior by third-party sellers result in high prices, suboptimal levels of traffic from the platform’s viewpoint and/or limited variety offerings. In particular, the platform may decide to enter its marketplace by creating and sponsoring its own retail arm, thereby transforming its platform into a hybrid model.

Apart from disrupting lack of competition in relevant demand segments, the move towards a hybrid marketplace may also be due to the identification of missing varieties that consumers would likely value, or of a business opportunity for its retail arm resulting from its understanding that consumers are unsatisfied with existing varieties offered by third-party sellers (notice that the platform may have access to customers’ reviews and ratings on all products transacted at its marketplace). By entering as a retailer to attract volume and contribute to a more levelled playing field within the marketplace, the platform not only enhances intra-platform competition, but also, and ultimately, inter-platform competition. That is, the adoption of a hybrid business model can be interpreted as an effort to attract and retain more online customers.⁴²

It is true that in a hybrid business model, the intensified intra-platform competition that results from the presence of the platform’s own retailer will negatively affect the profits of third-party sellers. Therefore, there might be the risk that these third-party sellers delist by the platform, thereby reducing the platform’s appeal. In a recent paper, Hagiu et al. (2020) show,⁴³ however, that this need not be the case. In their model, the multi-product retailer has the incentive to transform itself into a marketplace by hosting rivals, since this reduces the additional shopping costs to consumers of buying products from the rivals’ versions of the retailer’s non-core products. While this makes those rivals closer competitors, it turns the competitor into a complementor, thus increasing demand for the retailer’s core products. It follows that this strategy can be both beneficial for the retailer and its hosts.

B. Data Sharing and Data Privacy Concerns

Consider, for example, the incentives of a pure marketplace which facilitates the interaction between buyers and third-party sellers. The disclosure of detailed information about preferences and willingness to pay of its potential consumers may be used by third-party sellers within a marketplace for marketing and commercial purposes. They may use that information to improve their offerings and target them more effectively, and/or to tailor prices to the level of market demand or to set different prices to different market segments, i.e. the information may ultimately be used for price discrimination purposes.⁴⁴

41 See e.g. Jerath, K & Z. Shang, (2010), “Store within a Store,” *Journal of Marketing Research*, 47(4), 743-763. Hagiu, A. & J. Wright (2015a) “Marketplace or Reseller?” *Management Science*, 61 (1), 184–203; Hagiu, A. & J. Wright (2015b) “Multi-sided Platforms?” *International Journal of Industrial Organization*, 43, 162-174; Abhishek, V., Jerath, K. & Z. Zhang (2016), “Agency Selling or Reselling? Channel Structures in Electronic Retailing,” *Management Science*, 27(8), 2259-2280; Tian, L. Vakharia, A.J., Tan Y., & Y. Xu, (2018), “Marketplace, Reseller or Hybrid: Strategic Analysis of an Emerging E-commerce Model,” *Production and Operations Management*, 27(8), 1595-1610.

42 See Jiang, B., Jerath, K. & Srinivasan, K., (2011), “Firm Strategies in the “Mid Tail” of Platform-Based Retailing,” *Marketing Science*, Vol. 30, No. 5, pp. 757–775.

43 Hagiu, A., Jullien, B. & Wright, J. (2020) “Creating Platforms by Hosting Rivals,” *Management Science*, forthcoming.

44 See e.g. Thisse J. & Vives, X. (1988), “On the strategic choice of spatial price policy,” *American Economic Review*, Vol. 78(1), pp. 122–137 for a discussion of the different effects resulting from price discrimination following information disclosure.

If consumers realize that the information collected is not used to improve sellers' offerings but rather for price discrimination purposes,⁴⁵ they may switch to other distribution channels or even to competing marketplaces or retailing platforms. The more information is extracted from them, the more likely it is that they will try to figure out what that information is used for, and to find out that it may be used to exploit them, if that is what the sellers within the marketplace do.

Thus, anticipating this, a marketplace may strategically decide to restrict both the volume and the type of information it collects from consumers doing business within its marketplace. Furthermore, it may focus on collecting and resharing with the sellers in its marketplace only information that is useful to improve product offerings (aggregate information) as opposed to information that is meant to facilitate price discrimination (personal information).

Allowing firms to recognize and collect information about customers raises not only the question of what can firms do with such information, but also the question of what are the privacy implications of consumer data collection.⁴⁶ Consumers typically anticipate that they might be hurt by any misuse of the information that is collected when they make deals within a given platform. Hence, the expected misuse of the information influences consumers' willingness to reveal information through their actions and transactions at a given platform. In addition, users are more likely to express concern about the nature and amount of data the online platform extracts from them if they anticipate that such information may be transmitted to third-parties or if they believe that their information may more likely land in the wrong hands.

Compared to a pure marketplace, a hybrid one will most likely restrict the information it collects and the fraction of that information that it shares with other sellers operating in the platform's marketplace in order to protect its own retailer. It may have to share information with third-party sellers to induce them to participate in the platform, since the more information it shares the more levelled is the playing field between them and the platform's own retailer. But the platform is likely to restrict the information shared to limit the cannibalization of its retailing and platform businesses and, also, because third-party sellers will not internalize the negative impact on the platform's business and reputation of "misusing" the information received.

As noted in the Introduction, in two recent economic theory papers,⁴⁷ we have formally investigated the incentives to collect and disclose private information under two business models: the pure marketplace model and the hybrid marketplace model. In our models, irrespective of the business model used, the platform commits to disclose the collected information to all the sellers distributing through its marketplace (including, obviously, its retail arm whenever present). All active sellers then use such information for target advertising purposes as well as to price discriminate between users. A key assumption of our analysis is that consumers anticipate that they might be hurt by any misuse of accurate individual information about themselves that is collected by the platform (and subsequently shared or resold) when they make deals at that marketplace. Hence, the expected misuse of their personal information (e.g. due to risks such as data breaches or leakages) directly affects their willingness to reveal information through their actions as well as, ultimately, their willingness to trade at the platform's marketplace.

We find that in the hybrid model the platform has a weaker incentive to engage in targeting advertising relative to third-party sellers. This is because the platform internalizes the negative effect that higher advertising efforts on its own (private label) brand would have on the demand addressed by third-party sellers distributing through it and, consequently, on the participation fee that it expects to extract from those independent sellers. Naturally, since the platform advertises less intensively, its own private label brand must also be sold at a lower price than the competing products traded through the platform's marketplace.

We also find that the platform's decision to gather and disclose consumers' information in the two business models crucially depends on the level of intra-platform competition and the platform's bargaining position vis-à-vis the independent sellers. When intra-platform competition is intense – i.e. when the platform's own private label and the products of third-party sellers are close substitutes – and the platform has significant bargaining power, then it acquires and disseminates less accurate information when operating as a hybrid marketplace.

45 There exists an extensive literature that assesses the impact of data pooling on firms' ability to engage in (third-degree) price discrimination and extract consumer surplus. Particularly relevant is the literature on behavior-based price discrimination, which occurs when firms have information about consumers' past behavior and use this information to offer different prices to consumers with different purchasing histories. For a prominent survey, see Fudenberg, D. & Villas-Boas, M., (2007), "Behavior-Based Price Discrimination and Customer Recognition." In: *Handbook on Economics and Information Systems*, ed. by T. Hendershott. North-Holland, Amsterdam, according to whom "[t]his sort of 'behavior-based price discrimination' and use of 'customer recognition' occurs in several markets... [and] it may become increasingly prevalent with improvements in information technologies and the spread of e-commerce and digital rights management." (p. 2).

46 See Acquisti, Taylor & Wagman, (2016), *op.cit.*

47 See Padilla, Piccolo, Riera & Vasconcelos, (2020a,b), *op. cit.*

The intuition is simple. Gathering end-user's information, processing it and disclosing it to third-party sellers has two important effects on the platform's profitability. First, when better informed about the characteristics of the demand they address, sellers are able to make more accurate pricing and advertising decisions, thereby generating extra profits and, as a result, generating as well higher revenues for the platform owner in the form of higher access fees. Second, since consumers have concerns related to having their private and individual information disclosed and potentially misused, gathering information leads to a negative shock in demand because users tend to refrain from joining a platform whenever they anticipate that purchasing online at the platform's marketplace involves serious privacy risks.

While the first effect is present irrespective of the business model, the second effect leads to less information collection by the hybrid platform whenever: (i) the platform's private level is a close substitute of the products offered by third-party sellers within the platform's marketplace; and (ii) the platform has significant bargaining power vis-à-vis the independent sellers which are active in its marketplace. This is because, under those conditions, the negative demand effect will trigger a stronger reduction in revenues for the hybrid marketplace: First, its own retailer's platforms will fall; an effect which is not present in the case of the pure intermediary. Second, the reduction in third-party sellers' revenues will also be large, given that competition between them and the platform's retailer will be more intense in the hybrid model than in the pure intermediation model. And third, the reduction in third-party seller revenues will cause a further and significant reduction in the platform's revenues when its negotiated access fees are large.

Importantly, in those circumstances where the hybrid prefers to collect and disclose less information, consumers are better-off when patronizing a hybrid marketplace rather than a pure intermediary. When both conditions hold, the hybrid platform is able to appropriate a larger share of the incremental value generated by each consumer that joins the marketplace and, as a result, has a higher incentive to boost demand within the platform's marketplace by adopting strategies that consumers perceive as strategies that protect their privacy.

V. ONLINE ADVERTISING PLATFORMS

The incentives of an online ad-platform are very much different from those of pure and hybrid marketplaces. The online ad-platform does not sell any products itself. It sells eyeballs or ad space to advertisers. Importantly, the value it can extract depends on the amount and scope of the data it collects and transmits to advertisers. Those advertisers want as much data and as granular data as possible so that they can not only improve their offers but also price discriminate more effectively.

Analyzing the evolution of the online advertising ecosystem, Evans (2009) points out that by collecting detailed information on how people use their computers, online advertising methods raise difficult issues concerning the expectation of privacy and the regulation of the online advertising industry.⁴⁸ In particular, consumers may resist having advertising platforms collecting detailed data about their behavior and government regulation may be called for limiting the ability of advertising intermediaries to collect these data. As Evans (2009), highlights, (overly) lenient privacy regulations can harm consumers as they "could incur the costs of having private information disclosed and potentially misused, and incur the costs of reducing their use of the web because of concerns over privacy." Further, "[r] egardless of whether their private information is disclosed, consumers may dislike receiving ads that reflect too much knowledge about them" (p. 58).⁴⁹

Unlike (pure and hybrid) marketplaces, the online ad-platform's incentives are exclusively aligned with those of advertisers, since it has no other revenue stream than the sales made to advertisers. Furthermore, unless those operating other business models, the ad-platform is likely to be less concerned about potential retaliation by consumers, since the latter may find it more difficult to establish a link between the information collected by the platform and the use of that information made by advertisers when selling their products elsewhere. In addition, while ad-platforms have incentives to collect all sorts of information from consumers, as they have a diverse range of agents to whom this information can be provided (including even political parties), marketplaces are only interested in collecting a subset of that information, i.e. only collect information

48 See Evans, D., (2009), "The Online Advertising Industry, Economics, Evolution, and Privacy," *Journal of Economic Perspectives*, 23 (3): 37--60.

49 Along related lines, Gal-Or, E., Gal-Or, R., & Penmetsa, N., (2018), "The Role of User Privacy Concerns in Shaping Competition among Platforms," *Information Systems Research*, Vol. 29 (3), pp. 698-722, highlight the fact that even though users may benefit from being exposed to relevant ads, the associated loss of privacy may lead consumers to avoid ads that seem too intrusive and, ultimately, may also discourage them from adopting an online advertising platform. With this motivation in mind, the authors investigate how the trade-off between (targeting) advertising effectiveness and user privacy concerns affects competition between online advertising platforms. Further, following empirical studies claiming that platforms can profit by giving users more control over their personally identifiable information (e.g. Tucker, C.E., (2014), "Social networks, personalized advertising and privacy controls," *Journal of Marketing Research*, Vol. 51(5), pp. 546-562), the authors also investigate a scenario wherein platforms can reduce the privacy concerns of users by offering them greater control over their personal information. See also Zhao, X., & Xue, L., (2012), "Competitive Target Advertising and Consumer Data Sharing," *Journal of Management Information Systems*, Vol. 29, No. 3, pp. 189-221, for a study on the incentives of homogeneous product competing firms to directly trade consumer data with each other in a setting where: (i) there is advertising competition between two firms that target the same consumer; but (ii) firms are asymmetrically informed about the consumer value, i.e. about the revenue income the consumer can generate to the firm.

related to demand, and which is, thus, of interest to retailers. As a result, online ad-platforms will collect and disseminate much more information than (pure and hybrid) marketplaces.

The amount of data collected may also raise concerns regarding the likelihood of online platforms embarking on exclusionary strategies. A typical argument is that “the marginalization of smaller competitors due to differentiated data access might be self-reinforcing: access to a larger amount of data may support better services, which in turn attract more customers – and more data (“snowball effects”). By contrast, smaller companies might attract fewer consumers and as a result have less data. As the gap in market share increases, so might the gap in data collection, which could further increase the gap in the quality of services proposed to customers.”⁵⁰ In the case of on-line ad-platforms, the vast and large scope of data collected through time may indeed be self-reinforcing and give rise to the exclusion of other players or newcomers from competition. The same is not true, however, as far as marketplace platforms operating a hybrid business model are concerned. As explained above, by collecting only a limited set of information, on the one hand, and by sharing it with independent sellers, on the other, hybrid platforms, rather than embarking on exclusionary strategies, aim at inducing third-party sellers to attain a critical mass of consumers, thereby increasing traffic and promoting a more levelled playing field between all sellers within the platform’s marketplace.

VI. IMPLICATIONS FOR PRIVACY REGULATION

A first conclusion resulting from our previous analysis is that different business models have distinct implications for the amount and nature of the end-user information that is collected by different platforms, as well as for the way in which that information is handled or eventually shared with third parties.

When consumers care about their privacy, intra-platform competition is strong and the marketplace’s bargaining position vis-à-vis independent sellers is also strong, a hybrid marketplace will tend to collect and share less information about its end-users than a pure intermediary. In addition, and perhaps most importantly, in those circumstances where the hybrid platform prefers to collect and disclose less information, it is in the consumers’ interest to adhere to a hybrid platform rather than to a pure intermediary one.

This conclusion has significant policy implications, as some hybrid business models, such as Amazon’s dual business model, have been accused of making use of their strong bargaining power to engage in so-called private-label-copying strategies, which consist in entering as a retailer with close substitutes of the best-selling items of third-party sellers operating within their marketplaces.⁵¹ However, our analysis shows that it is precisely when the platform possesses bargaining power and its products are close competitors to those of third-party sellers in the platform that consumers should actually trust hybrid platforms more than pure intermediaries, as hybrid platforms will tend to collect and disclose less personal data from them, with natural positive implications on privacy protection.

Amazon’s dual business model has also been questioned because it allegedly causes Amazon to embark on information discrimination strategies that grant exclusive use of the collected information to its affiliated retailer. This question has been formally addressed in another recent companion paper of ours,⁵² where we conclude that, despite naturally hurting the profits of third-party independent sellers, such a strategy of asymmetric allocation of collected information between the platform’s retail arm and the independent sellers may, again, be consumer welfare enhancing.

As we show, to the extent that consumer data is used both for price discrimination and targeted advertising purposes, two fundamental features of e-commerce, the hybrid platform’s incentive to share information with independent sellers crucially depends on the degree of intra-platform competition, as well as on the efficacy of targeted advertising (based on observed consumers’ preferences and behavior) to enhance demand.

More specifically, when (i) users perceive the intermediary’s private label and the sellers’ products as relatively close substitutes, and (ii) consumers are sufficiently responsive to advertising, the hybrid platform opts not to share the collected demand information with the remaining sellers, thereby granting its own retailer an information advantage vis-à-vis the third-party sellers operating in its marketplace. Nonetheless,

⁵⁰ See Autorité de la Concurrence and Bundeskartellamt (2016), “Competition Law and Data” (p.13).

⁵¹ See e.g. <https://promarket.org/congress-can-move-now-to-stop-amazons-cloning-factory-heres-how/>, where it is also defended that by creating an environment of intense product market competition through product cloning, dominant hybrid platforms may also, allegedly, hurt innovation by independent merchants.

⁵² See Padilla, J., Piccolo, S., Riera, A. & H. Vasconcelos (2020c) “Welfare-Enhancing Favouritism in Hybrid Marketplaces,” mimeo, University of Bergamo. See also Neil Dryden, Sergey Khodjamirian & Jorge Padilla, (2020), “Revisiting Lina Khan’s “Amazon’s Antitrust Paradox,” mimeo, Compass Lexecon, for a more general discussion of self-preferencing in platform markets.

under these circumstances, which describe the economic context which is relevant to assess the complaints against the hybrid platform model, this strategy turns out to be lined up with consumers' preferences, as it avoids consumer losses due to surplus extraction through intense and accurate price discrimination strategies, on the one hand, and lack of (valuable) targeted advertising resulting from intense price competition, on the other.

Hence, a second policy implication from our research is then that there is no solid economic basis for the presumption that consumers are always hurt when hybrid marketplaces favor their private labels by denying access to their consumers' personal information to third-party sellers.

VII. CONCLUDING REMARKS

Consumers should factor the business model used by the platforms they patronize when deciding whether to trust them with their data, since the way in which such platforms will use their data and protect their privacy will differ across business models. In a nutshell, we find that they should trust hybrid marketplaces more than pure intermediaries and, in particular, much more than online advertising platforms.

Regulators should also factor the business model used by the platforms they monitor when deciding whether, and to what extent, interfere with their privacy policies. The underlined differences between hybrid or dual business models and pure intermediation models should be taken into account when defining those important policies or planning interventions aimed at protecting consumers' interests. In particular, the competitive, organizational, and contractual environment wherein many well-known hybrid marketplaces operate makes us believe that they can be trusted to adopt strategies that limit the amount and scope of personal data collected from end-users, on the one hand, and that express responsibility by refraining from disseminating the same personal data to third-party sellers, on the other, thereby protecting and defending the privacy of their consumers.



