Data, networks, and platforms: What effects on economic development?

Antitrust and restrictions on privacy in the digital economy

Nicholas Economides
neconomi@stern.nyu.edu
Professor of Economics
Stern School of Business, New York University
Executive Director
NET Institute, New York

Ioannis Lianos
i.lianos@ucl.ac.uk
President
Hellenic Competition Commission, Athens
Professor of Global Competition Law and Public Policy
University College London

We present a model of a market failure based on a requirement provision by digital platforms in the acquisition of personal information from users of other products/services. We establish the economic harm from the market failure and the requirement using traditional antitrust methodology. Eliminating the requirement and the market failure by creating a functioning market for the sale of personal information would create a functioning market for personal information that would benefit users. Even though market harm is established under the assumption that consumers are perfectly informed about the value of their privacy, we show that when users are not well informed, there can be additional harms to this market failure.

I. Introduction

1. Traditionally, antitrust regulation was largely disjoint from privacy regulation. Presently, dominant digital platforms' practices blur the divide between antitrust and privacy regulations. The interplay of privacy protection with antitrust creates an important challenge for both the application of antitrust and privacy regulations.

2. Data protection and privacy regulations often take a fundamental rights perspective, seeing privacy as an issue of rights. Personal privacy is protected in Europe by GDPR.[1] In the United States, the California Consumer Privacy Act (CCPA) 2018[2] and several sector-specific data and privacy protection regimes have been enacted at both the federal and state levels.[3] Competition law usually takes a market failure approach and is concerned by the fact that consumer or total welfare, or well-being, may suffer from reduced data protection in a malfunctioning market for personal data acquisition, to a similar extent that it could suffer from higher prices or lower quality. A market failure approach may provide common intellectual foundations for the assessment of harms associated to the exploitation of personal data, even when the specific legal system does not formally recognize a fundamental right to privacy.

1 The EU, as well as its Member States, constitute some of the most active jurisdictions in this context, to the extent that they recognize a fundamental right to privacy (Article 7 of the Charter of Fundamental Rights) and the protection of personal data (Article 8 of the Charter of Fundamental Rights). They have established an elaborate system of data protection, most recently with the implementation of the General Data Protection Regulation (GDPR) and related legislation. The GDPR obligations apply to "controllers" which can be natural or legal persons, irrespective of whether their activity is for profit or not, irrespective of their size and whether they are private law or public law entities. Among the rights conferred to data subjects is the right to data portability, individuals having the right to receive free of charge their personal data which they provided themselves on the basis of contract or consent in a "*structured, commonly used and machine-readable format*" and to transmit the data to another controller.

2 *See* https://www.caprivacy.org.

3 The CCPA has similarities with the GDPR, but a more limited scope. In contrast to the GDPR, the CCPA does not require a "legal basis" for all processing of personal data, nor the establishment of accountability requirements, such as the appointment of data protection officers, as required by the GDPR. The right to opt-out is only available in the case of selling or sharing personal information and does not apply to the harvesting of personal information, as it is the case in the EU, which covers all "processing" of information.

3. Personal privacy is indeed significantly reduced by the extensive acquisition of personal information by platforms directly from users. This information, combined with information acquired from private and public sources, creates an almost unique identity for each user. Large digital Internet platforms use their market power to require their users to provide their personal information to the platform without compensation. Thus, digital platforms collect an immense amount of personal information of users.[4] The data is used by the platforms themselves, and is also sold to infomediaries. Data is primarily used by advertisers, but has also been used to identify marginal voters in political campaigns.

4. Recent technological progress in data analytics may also greatly facilitate the prediction of personality traits and attributes from even a few digital records of human behavior, such as "likes" or facial images on Facebook,[5] while inferring identities, such as Social Security numbers, from anonymized data has been possible for some time.[6] The development of smart cities (with extensive networks of sensors) and technologies such as artificial neural networks enable better predictions of actions as well as behaviors of smart cities' users, or even the formation of new social ties, through better modeling and simulation.[7] Digital technology facilitates the elaboration of advanced (even real-time) sociometrics and new applications, such as social credit experiments.

5. We present a model of market failure based on a requirement provision in the acquisition of personal information from users of other products/services of Google and Facebook. We establish the economic harm from the market failure and the requirement using the traditional competition law toolbox. Eliminating the requirement and the market failure by creating a functioning market for the sale of personal information is imperative.

6. Besides the traditional analysis of the requirement and market failure, we note that there are typically informational asymmetries between the data controller and the data subject. The latter may not be aware that his/her data was harvested, in the first place, or that the data will be processed by the data controller for a different purpose or shared and sold to third parties. Maybe there was no consent for such use, or, if there was consent, it may not have extended to third parties' use. The exploitation of personal data may also result from economic coercion, on the basis of resource dependence or lock-in of the user, the latter having no other choice, in order to enjoy the consumption of a specific service provided by the data controller or its ecosystem, than to consent to the harvesting and use of his/her data. A behavioral approach would also emphasize the possible internalities (demand-side market failures) coming out of the bounded rationality, or the fact that people do not internalize all consequences of their actions and face limits in their cognitive capacities. Hence, a user may consent on the harvesting and use of his/her data, without necessarily realizing the full consequences and costs of his/her choice. This may occur in the context of an exchange in which the user is offered a free product in exchange of his/her data.

7. By recognizing that there is a market failure in the acquisition and exploitation of user information, we identify a wider problem than the issue of unauthorized harvesting and use of personal data. This harm may result even from conduct that, at first sight, could appear as increasing consumer surplus. For instance, advertised-based platforms such as Google and Facebook provide free search in exchange for acquisition of private user information. Not only do these companies benefit from market power, to the extent that they control the most popular search engine and social media platforms, but also their users are locked in since they face costs of switching to rival products. Furthermore, there are considerable information asymmetries resulting out of the opaque and constantly changing data and privacy policies, as well as the fact that users are not aware of the extent of companies' surveillance. In addition, these companies exploit consumers by offering a "zero price" in terms of monetary transaction for their product, although this "zero price" may be arbitrary and may underline the market failure in the acquisition of private user information. Present privacy regulations ignore this market failure as they are based on the "rights" of users but ignore that there is something fundamentally wrong with this "market." This is where antitrust intervention may add value.

II. Value of information

8. In a normally functioning market for personal information, transaction prices would depend on the willingness of the digital platform to buy and the willingness of a user to sell his/her personal information.

9. How much a user's personal information is worth to himself/herself differs in general from how much it is worth to a platform such as Google or Facebook. To start, the user might not quite appreciate the harm to himself/herself from the loss of his/her privacy. This may be because the value of personal privacy may vary over time, and human beings typically have a hard time estimating future prices and values, as well as their own circumstances later in life. What may seem like a small loss today may turn out to be a significant loss in the

4 Data is harvested by digital platforms across different devices such as smartphones, tablets and laptops/computers, for instance with regard to websites the user has interacted with (first data aggregator), or from other entities, through third-party tracking, the tracker harvesting data not directly from the user, but indirectly through access to the data aggregated by the first data aggregator.

5 M. Kosinski, D. Stillwell & T. Graepel, Private traits and attributes are predictable from digital records of human behavior, 110(15) *Proc. Natl. Acad. Sci. U.S.A.* 5802–5805 (2013).

6 A. Acquisti & R. Gross, Predicting Social Security numbers from public data, 106(27) *Proc. Natl. Acad. Sci. U.S.A.* 10975–10980 (2009).

7 *See*, M. Batty, K. W. Axhausen, F. Giannotti, A. Pozdnoukhov, A. Bazzani, M. Wachowicz, G. Ouzounis & Y. Portugali, Smart cities of the future, 214 *The European Physical Journal* 481–518 (2012); A. Almeida & G. Azkune, Predicting Human Behavior with Recurrent Neural Networks, 8(2) *Applied Sciences* 305 (2018).

future. But, once privacy is lost and personal information becomes the property of a digital platform, it is hard if not impossible for this information to become private again.

10. Even if the user can precisely estimate the value of his/her private information, it is likely that this value would differ from the value of this information to the digital platform. This is quite natural because a user's value is defined by a personal assessment of how much personal loss of privacy would cost him/her, while the value of the information to the platform is determined by what products or advertisements the platform could sell to the user (in the case of Google) or additionally how much the user is desirable in a social network (in the case of Facebook). Additionally, how much the personal data is worth to a platform depends on how much demand there is for data of particular features of the user to potential buyers of the data. So, the value of the personal information to the platform comes as a derived demand from the process of selling advertisements to that user and selling to third parties. The value to the platform is also enhanced by the availability to the platform of other complementary data that the user may not be aware of. These include data that Google acquires from third-party infomediaries and data (or information) intermediaries (brokers), such as Acxiom and Equifax, publicly available data such as census data, and data from trackers on websites.[8]

11. Besides differing in the value a user assigns to his/her privacy, users also vary in their value of the platform's service. Thus, together with the variability in the platform's value of the user's information, there are three separate dimensions of variation that should be considered in the context of the market failure imposed by dominant platforms.

12. The difference in the value of personal information between the user and the platform is not surprising, and, to start with, not a competition policy concern. Parties trade goods and services when they have different valuations or willingness to buy and willingness to sell. This is normal in markets.

13. However, as we show below, dominant digital platforms have intervened in the market for personal information and have created a market failure in this market, requiring antitrust scrutiny. The ability of digital platforms to create a market failure with favorable terms to themselves arises from their dominance in their primary markets, Internet search for Google and social network for Facebook. Their practices in the market for personal information raise antitrust concerns.

III. Requirement to provide free personal information imposed by dominant digital platforms

14. Digital platforms have imposed a requirement contract on users under which the platform automatically receives the user's personal information when he/she uses the platform's service (Internet search for Google, social network service for Facebook). The requirement contract imposes as a default "opt-in" under which the personal information is automatically collected by the platform.

15. Under the requirement contract, digital platforms collect the personal information without providing compensation to users beyond the in-kind compensation that a user receives from using the digital platform's product for free. Thus, the personal information market collapses and all transactions occur at a single zero nominal price. This is a market failure, implemented in favorable terms to the dominant platform.

16. One may refer to historical patterns in the industry in order to assess how rising concentration and dominance may have found their source in conduct and business strategies harming privacy, rather than competition on the merits, or may have reinforced the dominant position of the firm by erecting important barriers to entry through the control of important amounts of data. As some commentators note, in 2007 the social network market was highly competitive, with several hundred of social networks available to users, including competing offerings from Google, Yahoo and Myspace. During this time, privacy was an important parameter of competition.[9] However, the landscape changed sharply in recent years, predominately because of the business strategy of Facebook. Facebook initially put forward its "superior" privacy-centered offer, linked to the fact that it was a "closed communication network" that required users to

8 Third-party websites can embed references to external resources which the user's browser will automatically load from the third-party server, and execute JavaScript code. *See* S. Schelter & J. Kunegis, Tracking the Trackers: A Large-Scale Analysis of Embedded Web Trackers, Proceedings of the Tenth International AAAI Conference on Web and Social Media (ICWSM 2016), available at file://ad.ucl.ac.uk/homea/uctlioa/Documents/EPANT/13024-57897-1-PB.pdf. According to a study published by Ghostery in 2017 (https://www.ghostery.com/study), more than 77% of all page loads contain at least one tracker, for statistical or advertising purposes, Google being found on more than 60% of all page loads, and Facebook on more than 27%, followed by Comscore, Twitter and Yandex. Tracking capabilities are also concentrated in a few number of companies, with Google holding most power, in terms of reach of a tracker on popular websites and apps, in both websites and apps, followed by Twitter, Facebook and Microsoft for website trackers, and Amazon, Facebook and Comscore for mobile trackers. *See*, R. Binns, J. Zhao, M. Van Kleek, N. Shadbolt, Measuring third party tracker power across web and mobile (March 2010), *ACM Comput. Entertain.* 9, 4, Article 39, https://doi.org/0000001.0000001, available at https://arxiv.org/pdf/1802.02507.pdf (proposing a new metric for power to measure the effect of the consolidation among tracker companies). The recent consolidation of the tracking analytics industry with the mergers of Microsoft/LinkedIn (2016), Adobe/Livefyre (2016), Facebook/LiveRail (2014), Alibaba/Umeng (2013), Google/DoubleClick (2007), has also contributed to the emergence of a market structure dominated by a small number of firms, and a long tail of less significant trackers. See ibid.; M. Falahrastegar, H. Haddadi, S. Uhlig & R. Mortier, Anatomy of the Third-Party Web Tracking Ecosystem (2014), arXiv:1409.1066, available at https://arxiv.org/abs/1409.1066.

9 D. Srinivasan, The Antitrust Case Against Facebook (September 10, 2018), Berkeley Business Law Journal Vol. 16, Issue 1, Forthcoming, available at SSRN: https://ssrn.com/abstract=3247362.

join and disclose their information before being able to have access to the network, than existing dominant social networks at the time, such as Myspace. During this more competitive period, Facebook provided users the ability to opt-out of having their information shared with third parties, including advertisers or marketers, and promised them it would remove their information on demand.[10] Any effort by Facebook to track users' behavior, through its advertising product Beacon, or subsequently social plugin products, was unsuccessful, as it led to users' backlash and Facebook had to withdraw the product and change its privacy policies, by including a commitment to allow users to vote on future changes that contractually change user privacy.[11] However, after a decade of "false statements" and "misleading conduct," reneging on previous promises not to track users, Facebook was able to leverage the superior information it has over its users in order to sell more advertising, with the result that the market for digital advertising has been transformed to a duopoly, dominated by Facebook and Google, the two companies accounting for 90–99% of year-over-year growth in the US digital advertising industry.[12]

IV. Personal information market operating without the requirement

17. If the market for personal information were operating without the requirement, a user would be able to sell his/her personal information based on the extent that he/she valued privacy and the willingness to pay of the platform. The user may pay for platform services in the separate market for such services, Internet search for Google, social network for Facebook. Under the present requirement, the personal information market has collapsed, and we observe a market failure.

18. The market for personal information could operate without the requirement if the default were "opt-out," that is if the users had an option not to provide their information to the platform for free. In this opt-out regime, some users would prefer to sell their information for a positive price, while others would prefer not to participate in this market at all. This would be entirely consistent with a functioning market.

19. The opt-out default was instituted by GDPR based on the idea that otherwise the rights of the individual would be violated and not antitrust considerations. No such requirement exists in the United States.

20. Even if the default regime were to change to opt-out now, the market for personal information is unlikely to operate as a competitive market. A digital platform can implement almost price discrimination towards the user because of the personal information it collects. If no further remedies are imposed, except for changing the regime to opt-out, a significant distortion to the market for personal information would remain as the buyer of personal information would be a perfectly price discriminating monopsonist.

V. Harms

21. The requirement contract combining the primary market of the platform (Internet search for Google) results in harming users who would be willing to pay for the primary service of the platform but are not willing to sell their personal information to the platform at zero price. Some of these users may be willing to sell their information at a positive price.

VI. Analysis

22. We use Google as the dominant platform imposing the requirement, but this narrative can be easily adapted to Facebook. We define a user type as triplet of dollar amounts (x, y, z) with variation across users in x, y, and z. The amount $x is defined as how much the particular user is willing to pay to use Google Internet search, $x > 0$. $y is defined as the value to Google of the personal data that the user provides to the company, $y > 0$. $-z < 0$ is defined as the loss of value to the user of his/her private information to Google when privacy is lost.

23. We consider three alternative competition regimes. The first one is the current requirement regime, in short "opt-in," where the personal information of the user is automatically received and used by the platform which requires personal data provision to provide Internet search. The second one is the world with no requirement regime and competition in the personal data market, where Google has the possibility to perfectly price discriminate to induce the user to sell his/her personal information but faces competition with rivals in the personal data market. In this world, the default is "opt-out," which means that the company is not allowed to use any information gathered from the user unless the user affirmatively consents, and there is no requirement to provide personal information to access the search service. In this regime, we assume that Google competes with other firms in search and also faces competition in the personal search market. We assume that all rivals are very well informed on the features of the user and can practice perfect price discrimination. In the third regime, the default is "opt-out" and Google is a perfectly price discriminating monopsonist in the acquisition of personal user information. This is a no requirement regime with a perfectly price discriminating monopsonist. Thus, the key difference between regime 1 and regimes 2 and 3 is the imposition of the

10 Ibid.

11 Ibid.

12 Ibid.

requirement contract or lack thereof. The key difference between regimes 2 and 3 is in the degree of competition among buyers in the personal information market, with regime 2 assuming competition and regime 3 assuming monopsony.

1. Analysis under perfect information

1.1 Analysis of the present requirement regime with default opt-in (regime 1)

24. A perfectly informed user accepts the requirement and provides data to Google if his/her value from the use of Google Internet search is higher than his/her cost of loss of privacy, $x > z$. Under the requirement, Google receives an incremental benefit G equal to $y, $G = y$, the value of the user's data to Google. In summary, when a user accepts the requirement, the benefits to the user and Google are:

$$\text{If } x > z\text{: } CS = x - z > 0,\ CS < x,\ G = y > 0.$$

25. In this regime, Google is able to leverage the value the consumer receives from Internet search to induce the consumer to accept the requirement and thereby receive benefit $y. Once its search is in operation, Google does not face an incremental cost for serving an additional user in Internet search. On the contrary, additional users increase the precision of Internet search, bringing additional value to Google, beyond $y, which we ignore in the calculations.

26. If the benefit to the user from search is smaller than the cost of losing privacy, $x < z$, the user does not accept the requirement, does not provide personal data to Google, does not use Google search, and stays at zero consumer surplus. Google receives zero benefit as well.

$$\text{If } x < z\text{: } CS = 0,\ G = 0.$$

1.2 Analysis of the no requirement regime with competition in the personal data market (regime 2)

27. We now analyze a hypothetical regime where the default is "opt-out," assuming that personal data provision is not required to receive Google Internet search. Thus, now the user uses Google Internet search, but does not give the right to Google to use his/her personal data, even if Google collects it. Provision of personal data is now a choice of the user. Google charges a price p1 for the search and pays a personalized price p2 to the user for personal data provision. We assume that rivalry among Internet search companies drives the price in the Internet search market to zero $p1 = 0$,[13] resulting in benefits from participation in the Internet search market:[14]

$$CS = x,\ G = 0.$$

28. Since the maximum benefit from personal data to Google is y, Google would be willing to pay up to $p2 = y$ for personal data acquisition, resulting in benefit

$$G = y - p2.$$

29. Once the market for personal information does not have the requirement, other firms will bid up to $y to acquire the personal information of a user. Competition among them will result in each of them offering the same price $y to the same user, resulting in zero benefit for each of them. Therefore, the user and Google benefits will be:

$$CS = x - z + p2 = x - z + y,\ G = 0.$$

30. The user prefers to accept the Google monetary offer as long as his/her value of privacy is lower than what Google is willing to pay for his/her information, $z < y$, resulting in:

$$\text{If } y > z\text{: } CS > x,\ G = 0.$$

31. Conversely, when a user values his/her privacy more than what Google is willing to pay for his/her information, $z > y$, the maximum monetary offer Google can make to induce data provision, $y, will not be accepted by the user because it would result in lower user consumer surplus than when the user did not provide data, $CS = x + y - z < x$, keeping in mind that the user has consumer surplus $CS = x$ when not providing data. Therefore, if $y < z$, the user accepts no offer.

$$\text{If } y < z\text{: } CS = x,\ G = 0.$$[15]

32. It is important to note that users are better off, and Google is worse off ($\Delta CS > 0$, $\Delta G \leq 0$) when the requirement is removed and there is competition in the personal data market. Essentially, users are better off because they now have more choices and they are not constrained by the Google-imposed requirement. Google is worse off because without the requirement, it can extract less surplus from the users.

33. Also note that removing the requirement does not kill Google's business model of providing free search while collecting information about users, and selling this information to advertisers. For a wide range of parameters, users sell their personal data under no requirement. This includes users who would not participate in the market under the requirement but are won over by the positive price Google offers in its absence. The users who cannot be won over by Google in the absence of the

13 If competition is less intense, price will be xk, $0 < k < 1$, with similar results.

14 We ignore the positive network effect reaped by Google.

15 The following example provides a good illustration. Consider a user with $(x, y, z) = (2, 3, 1)$. Since $y > z$ and $x > z$, the user participates under the requirement and also sells his/her data without the requirement. Similarly, with $(3, 2, 1)$: $y > z$ and $x > z$ implying that the user participates under the requirement and also sells his/her data in its absence. Alternatively, consider a user with $(x, y, z) = (1, 3, 2)$. This user would not participate under the requirement since $x < z$, but would sell his/her data in its absence since $y > z$. Also consider user $(x, y, z) = (3, 1, 2)$. Since $x > z$, he/she would participate under the requirement, but would not sell his/her personal information in its absence since $y < z$. There are also those who would not participate under the requirement since $x < z$ and also would not participate in its absence since $y < z$, for example $(x, y, z) = (1, 2, 3)$ or $(2, 1, 3)$.

requirement are only those who value their privacy more than Google values their data (z > x, z > y). Additionally, among those who value their privacy more than Google values their data (z > y), there are some users who were participating under the requirement, but having been freed from the requirement, do not sell their data at prices Google is willing to offer (x > z > y).

34. The market for acquisition of personal data by Google works well and has the various features of a functioning economic market. For example, there is variation in the willingness to pay defining a demand curve, and, given an offer price by Google, some users participate in the market at the price offered by the buyer while others do not.

35. We have shown that a vibrant market for personal information sold to Google has been killed through Google's practice to impose provision of personal data as a requirement for access to Google's Internet search service. This is a "market failure" and can be fixed by antitrust authorities in the US, the EU, and other jurisdictions.

36. We have shown that users are worse off, and Google is better off under the requirement. Assuming that users are well informed and can determine rationally whether it makes sense to provide their data, absence of the requirement will lead to users being paid by the digital platforms for harvesting of their data. Removing the requirement improves consumer surplus since users get paid for selling their data to the platform. Typically, this will also lead to more data being collected.

1.3 Analysis of the no requirement regime with a monopsonist in the personal data market (regime 3)

37. In a third hypothetical regime, after opt-out, Google remains a monopsonist in the market for personal data. Google is able to charge a price for search and a second price for the provision of personal data. We assume that the price for search may not fully extract the benefit of search for the user, possibly because of competition with rival browsers. So, when the user uses Google Internet search but does not allow Google to use his/her personal data, the user has a benefit x – p1, where the price charged by Google for search only is p1 = kx, $0 \leq k \leq 1$.[16] It is likely that perfect price discrimination in the search market is not possible, so it is reasonable to expect that k will be less than 1.

38. Now consumer surplus and Google's benefit from the search market are

$$CS = (1 - k)x > 0 \text{ if } k < 1, G = kx.$$

All users will buy search from Google as long as k < 1.

39. Google offers payment p2 to users who are willing to sell their personal data to it. The user benefits from Internet search by $x, pays p1 = kx for search, loses $z for losing privacy, and receives p2 as monetary compensation from Google for selling his/her personal data. Google receives the personal data which it values at y, charges p1 for search and pays p2 to the user for providing that data. Therefore, the user's consumer surplus and benefit to Google are:

$$CS = x - z - p1 + p2 = x(1 - k) - z + p2, G = y + kx - p2.$$

40. If the value of the personal data of the user to Google is higher than the value of loss of privacy to the user (y > z), Google can offer up to $y and be better off than when no data is provided. Since Google is dominant and knows the user so well that it can practice perfect price discrimination in the market for the provision of personal data, it will offer the lowest possible amount of money that will make the user provide data, by making his/her consumer surplus slightly higher than CS = x(1 – k), which is the consumer surplus of no data provision. Therefore, Google will offer to the user p2 = z to buy his/her data, resulting in:

$$CS = x(1 - k) - z + z = x(1 - k) > 0, G = y + kx - z > 0.$$

Notice that Google's payment for personal data as a monopsonist (in regime 3) p2 = z is smaller than the amount it pays p2 = y when it faces competition in the personal data market in regime 2.

41. For users with y < z, the maximum offer Google can make to induce data provision, $y, will not be accepted by the user because it would result in lower user consumer surplus than when the user does not provide data:

$$CS = x(1 - k) - z + y < (1 - k)x.$$

Therefore, when y < z, the user does not provide data and the user's consumer surplus and Google's benefit are:

$$CS = x(1 - k) > 0, G = xk > 0.$$

42. Comparing regimes 2 and 3, we find that users are better off in regime 2 and Google is worse off:

$$\text{If } y > z, \Delta CS = y - z + xk > kx > 0. \Delta G = -(y - z + xk) < -xk < 0.$$

$$\text{If } y < z, \Delta CS = kx > 0. \Delta G = -kx < 0.$$

16 k = 1 is the special case when Google is able to extract the full benefit of the user from Internet search.

43. Clearly, competition in the personal data market makes users better off and Google worse off in comparison to Google being a monopsonist in the personal data market. This underlines the fact that removing the opt-in requirement is insufficient to restore users' consumer surplus. The analysis above shows the need for strict remedies that would restore competition on the marketplace, and therefore going beyond the removal of the requirement.

2. Asymmetric information

44. Under perfect information, the user knows x, his/her valuation of Google's or Facebook's services. But is this really the case? At present, the user does not pay for the access to Google or Facebook. These are "free" products in terms of monetary payment. However, the user pays (has a cost) by providing personal data to Google and Facebook for free. This may reduce the user's privacy or may enable the digital platform or whoever else is controlling this data to exploit the user in the future by personalized pricing, etc. Hence there is an issue of transparency of the full costs for the user of the engagement with Facebook. The user just sees the current monetary costs (zero) and does not take into account future costs. Behavioral economic literature on discounting, silver lining effect (the users are attracted by a small gain—zero price to use Google or Facebook—and dissociate that from a large loss—been exploited in the future through perfect price discrimination) may explain why we need to take seriously into account behavioral biases.

45. Our model also takes into consideration the cost of losing privacy. So, the user is willing to pay $x for using, say, Facebook, but the take-it-or leave-it contract of Facebook implies that he/she will lose privacy that he/she values at $z. So, under perfect information, the net willingness to pay of a user under the present default opt-in conditions is $x-z. If the default was opt-out, the user would be willing to pay $x. In a behavioral setup, the user may underestimate the value of the loss of privacy.

46. Users do not know how much their data is valued by advertisers/Google/Facebook as they have no access to the information on the value of that data in the context of the digital platform's transactions with advertisers and infomediaries at the other side of the platform.

47. Digital platforms argue that data harvesting and network effects also provide value to the users. However, it is unclear what the exact value of the network effects which benefit the users is. But even assuming that the data is valuable because of network effects, it is difficult to determine the part of the value that represents the individual contribution brought by the data of the specific user. The user anyway gets better service as his/her data may enable the platform to provide more relevant queries in some cases and to improve the quality of search for tail queries. The issue is, however, if the platform collects more data than is needed for improving the service or the quality of the platform: the extra harvesting of data creates "behavioral surplus" that will itself be highly valued in behavioral futures markets.[17]

17 See S. Zuboff, The Age of Surveillance Capitalism (Public Affairs, 2019).

48. The lack of competition between networks does not provide information (transparency) about how much the user is valued by digital platforms, so that the users could have information enabling them to bargain to achieve a "better" deal. This leads to no surplus left for users as it affects their ability for collective action towards the monopolist/monopsonist, for instance by switching to a rival network. In any case, the choice may be quite limited, in view of the consolidation of the sector, and in particular the dominance of the advertised-based model.

49. One should also add the social costs of the lack of knowledge by users of the broader social costs of letting their data being harvested by Facebook or Google: costs to democracy and pluralism, which may be important concerns, also for competition law, in some jurisdictions.

VII. Remedies

50. We are in favor of antitrust action to restore the conditions of a well-functioning data market. In regime 2 in the model above, we assumed that in the opt-out world there was significant competition so that the purchaser of personal information is forced by competition to offer to pay user $y for personal information, the full value of the personal information to the company. If such competition among purchasers of personal information were not present, and, for example, Google remained a monopsonist, as in regime 3, the user would not be appreciably better off in the opt-out world rather than the opt-in world. So, a remedy cannot be just the change from opt-in to opt-out but has to accomplish or at least imitate competition in the market for personal data sale.

51. A part of a possible solution dealing with the risk that users have been imposed conditions to which they did not provide their voluntary consent is that the "default" regime be changed from "opt-in" to "opt-out." Applying these principles to the case of Internet search and social networks, one may argue that Google and Facebook have no incentive to make this change on its own, and therefore this has to be achieved by regulation. This is certainly the choice made by the EU when adopting the GDPR, which put in place an "opt-out regime." However, even if one changed to "default opt-out," this will not have provided an adequate response, as the dominant social network may impose, because of its market dominance, the conditional use of the website to the "consent" provided by the users of their data being harvested. Hence, an "opt-out regime" will not be enough because of the asymmetrical bargaining power between the digital platforms enjoying a dominant position and the users.

52. One option may be to mandate that the digital platform offer the same product by asking for a fee, if data is not to be harvested and the users not being subject to targeted advertising. In cases in which the data of the specific user is quite valuable, it would be possible to require the digital platform to provide a positive payment to these users so that they can join the social network. Again this will raise several issues.

53. First, because of its dominant position Facebook may deny users "free" access to its services if they opt to exercise their privacy rights, it may overcharge users or not pay them the competitive price to join the social network or to buy their data. As discussed earlier, social networks of the size of Facebook have network effects and benefit from feedback loops. Strong network effects result in high market share inequality among networks, much higher profitability for large size network, barriers to entry for new networks, as well as providing the ability of a larger network to subsidize some "influential" users to subscribe.

54. Second, another issue is the missing market that would enable users to evaluate the full cost and benefit of their transaction with Facebook/Google. Once we understand the interaction between user and Facebook/Google as a market interaction we may fully grasp the possibility that the dominant position of the buyer of data (monopsony) may lead to inefficient exchanges, or that the monopsony buyer may have a lot of user-specific information and can implement sophisticated price discrimination strategies.

55. This calls for antitrust enforcement, in particular conduct as well as structural remedies, privacy regulation, but also other regulatory tools that would aim to set up a market between users and the network, ensure the transparency in the collection of data (so that users know what is collected), ensure transparency in the use of data (so that users know how their data is used), and ensure user's consent in data collection and specific use eventually with a possible compensation to the user for "selling" his/her data to a company like Google or Facebook.

56. Such regulation should make "opt-out" the default. If a user opts-out, Facebook or Google would not be able to use or sell the data the user discloses to Facebook/Google. Users may be compensated for opting-in, thus allowing Facebook/Google to harvest the user's raw data as well as his/her "activities" and "connections." This default opt-out will create a market between the user and Facebook or Google, where the user sells his/her data to the digital platform. More concretely, with regard to Google, opt-out should be the default for Android browsers, and Google search. Users should have opt-out choice for other personal data, such as health data, even if this data was not acquired from the users. Users should also be able to easily set their browser to delete cookies and trackers at end of use/session and should be able to avoid Chrome.

57. This opens the possibility for a possible compensation to the user for "opting-in" that is, for "selling" his/her data to a company like Google or Facebook. Depending on the extent that a user opts-in, he may be compensated in different amounts for allowing

- collection ("opt-in") of his/her personal data directly from the company he/she interacts with (say Google);
- use of his/her data for a specific purpose by Google (say for marketing vs political campaigns); and
- sale of data to third parties by Google.

The EU takes a different perspective as pricing remains unaffected by the opt-in/opt-out decision.

58. Pricing the data should nevertheless avoid the pitfall of letting the monopolist/dominant digital platform uses its superior bargaining power vis-à-vis individual users to ask for the monopsony price (in terms of data harvesting). This raises the question of identifying the but-for the infringement world, in order to determine the competitive monetary value of the data and thus ensure the proper payment of the users (if positive prices are charged), or the amount the users should be asked to pay (in data value or monetary prices) in order to have access to the product. In building this counterfactual the decision-maker should take into account the situation prior to the competition law infringement (before-and-after test) and/or the situation at a comparable, in terms of relevant characteristics, market which is nevertheless significantly more competitive than the market under examination.

59. Several other remedial options exist in order to restrict the privacy-harming potential of digital platforms with market power. It might be possible to break up the platforms horizontally by introducing in the market several horizontal competitors. However, one may observe the relatively low effectiveness of this remedy in view of the "winner takes most competition" effect in markets with intensive network effects. Even if there are new entrants in this market, the resulting market structure may not be significantly different and competition will be "for the market" rather than intensifying "competition in the market," at least in the medium to long term. A vertical separation of the platform, by prohibiting them to expand in vertically related markets may also provide some temporary relief but may also slip to some form of detailed regulation, a hybrid between utilities' regulation and data protection/privacy regulation. Of course, this may become an acceptable option in some circumstances.

60. Platforms may opt to pay for the users' data thus leading to the emergence of a licensing market for user data for users opting-in to share their data with the platforms. At the same time this enables the users to port this data to platforms offering them a higher return and better conditions in terms of higher value for their privacy (e.g., lower data input for equivalent, in terms of quality, search output).

61. Exclusive licensing of personal data to a company will imply a monopsony and will not solve the problem of competition in the personal data market. We could institute non-exclusive licensing through a licensing agency that would collect the data from each user and distribute it to platforms. The user would be paid the sum of the willingness to pay of all the company bidders. However, what determines how much a user gets paid or pays? Assuming similar competing networks, a user would like a larger social network because there are more possibilities of interaction, and therefore his/her willingness to pay $x increases in the size of the network. If we assume that the influence of a user is on a finite number of friends, a smaller network may be willing to pay more

to add him/her, so $y does not increase with network size, for networks above a moderate size. Additionally, a dominant network will be able, in general, to pay users less and/or demand higher payments from users, because of the use of its market power, and of the information about the features of the users. So, we expect that most users will pay more to subscribe in a large and dominant network and be paid less by it. In order to determine what will constitute a "fair" value one will need to refer to the value in a competitive market. However, this is not possible in the specific case as there is no perfectly competitive market and there cannot be one because of network effects. Digital platforms may exercise their buying power leading to a downward pricing pressure in the market for personal data for input suppliers (the users) and therefore deprive them from a portion of their revenues. Because of the buying power of digital platforms (or the monopsony they may benefit from) and the fact that this sorry situation results from the initial requirement contracts bundling digital services with personal data competition law should grant to the users a legitimate interest in prices which shall not be "artificially" low. In some jurisdictions, low pricing may be found to be unfair pricing and therefore infringe the abuse of dominance provisions.

62. A possible solution to this problem is for NCAs to facilitate the users to collectively bargain with the platforms rates for the payment they will receive for the data harvested in order to protect their personal data.[18] The value of personal data and therefore the price to which these may be sold to digital platforms may also increase by some input limitations by a digital and/or data protection regulator as to the amount of data to be harvested. It could also be limited by collective bargaining between privacy-prone users (if the number of users with strong preferences for privacy is significant) and the digital platforms, eventually through the constitution of collecting societies by the various groups of users that would also bargain with the digital platforms. One may consider the existence of one collecting society or several representing different preferences for privacy protection, assuming consumer preferences about privacy are heterogeneous.

63. Additional remedies that may address the problem of the lack of a market for personal data is data portability providing users the ability to export their social graph or their search history.

64. Interoperability remedies may also be used to intensify inter-platform competition. For instance, Facebook could change from a closed to an open communication network enabling its users to also send messages to users of other social networks. This would require the adoption of an open API for user messages, chats, posts, and other communications. Similarly, Google could open APIs that would allow users to submit queries simultaneously to a number of search engines.

65. Finally, it is important to add the existence of technological solutions to the problem of restrictions to privacy by the business conduct of digital platforms or more generally user-initiated and driven practices that may frustrate the aims of the ad-based business model, such as adding ad blockers[19] and the development of tracking protection technologies.[20] For instance, NCAs may mandate the development of a unique "Do not track" switch that may apply for all networks and prohibit or even bring abuse of dominance cases for exploitation against Facebook or Google if they try to bypass these technologies or forbid their use in their platforms.[21] ■

18 See https://www.economist.com/the-world-if/2018/07/07/data-workers-of-the-world-unite.

19 See https://iapp.org/news/a/the-privacy-consequences-in-the-rise-of-ad-blockers.

20 See https://blog.mozilla.org/blog/2019/06/04/firefox-now-available-with-enhanced-tracking-protection-by-default and https://www.wired.com/story/privacy-browsers-duckduckgo-ghostery-brave.

21 This may be necessary in view of the strategies of some of these platforms to put an end to the use of ad-blocking software. See https://www.inc.com/jason-aten/google-is-putting-an-end-to-ad-blocking-in-chrome-here-are-5-best-browser-alternatives.html.