September 2020 · Aline Blankertz

How competition impacts data privacy

And why competition authorities should care

Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Content

Executive Summary

A small number of large digital platforms increasingly shape the space for most online interactions around the globe and they often act with hardly any constraint from competing services. The lack of competition puts those platforms in a powerful position that may allow them to exploit consumers and offer them limited choice. Privacy is increasingly considered one area in which the lack of competition may create harm. Because of these concerns, governments and other institutions are developing proposals to expand the scope for competition authorities to intervene to limit the power of the large platforms and to revive competition.

The first case that has explicitly addressed anticompetitive harm to privacy is the German Bundeskartellamt's case against Facebook in which the authority argues that imposing bad privacy terms can amount to an abuse of dominance. Since that case started in 2016, more cases deal with the link between competition and privacy. For example, the proposed Google/Fitbit merger has raised concerns about sensitive health data being merged with existing Google profiles and Apple is under scrutiny for not sharing certain personal data while using it for its own services.

However, addressing bad privacy outcomes through competition policy is effective only if those outcomes are caused, at least partly, by a lack of competition. Six distinct mechanisms can be distinguished through which competition may affect privacy, as summarized in Table 1. These mechanisms constitute different hypotheses through which less competition may influence privacy outcomes and lead either to worse privacy in different ways (mechanisms 1-5) or even better privacy (mechanism 6). The table also summarizes the available evidence on whether and to what extent the hypothesized effects are present in actual markets.

Table 1 Overview of mechanisms through which competition affects privacy

	Mechanism	Evidence
1	If there is less competition, companies can collect more personal data.	Limited effect in app markets and tentative evidence in advertising markets.
2	If there is less competition, consumers face less choice regarding privacy.	Conceptual argument, open question for competition authorities: What is the benchmark for identifying anticompetitive conduct and restoring choice?
3	If companies merge, companies can collect and use more data.	Self-evident, and a matter for competition authorities if privacy is a relevant factor for competition.

	Mechanism	Evidence
4	Personal data in the hands of dominant firms creates more harm.	None based on the (theoretical) evidence of the effects of price personalization: no link between market power and negative outcomes for consumers.
5	If there is less competition, companies can undermine competition on privacy.	Limited to the readability of privacy policies decreasing as firm size increases.
6	Dominant firms can obtain quasi-regulatory powers over personal data that hamper competition.	Harm to competition evident, unclear whether there are benefits for privacy.

Source: Stiftung Neue Verantwortung.

Based on these findings, some of the mechanisms would strongly benefit from more research to better capture their relevance across markets. Others already have sufficient empirical and conceptual support to warrant stronger intervention by policymakers. These interventions should include the following:

First, besides developing a clearer notion of what it means to provide choice on privacy from a competition perspective, several options should be pursued by a collaboration between competition and data protection authorities to increase choice vis-à-vis dominant firms. These options include involving consumers in the development of privacy policies, for example through democratic decisions on privacy policies and/or forms of community consent. Another option is to unbundle consent and/or data such that dominant firms must obtain more granular consent before being allowed to share data internally.

Second, competition authorities should recognize that in a merger, a reduction in privacy can be both out of scope of the GDPR and relevant for competition if privacy is a relevant factor for consumers. Authorities should be comfortable to rely on stated preferences to determine whether consumers care about privacy in a specific market. Revealed preferences are often less meaningful because consumers face various obstacles in making effective privacy choices.

Third, authorities as well as the wider privacy community should develop metrics to assess the quality of a privacy policy to allow for reaching a view on whether a practice improves or degrades privacy. Any set of metrics will make some simplification inevitable which is necessary to cut through the excessive complexity that currently prevents authorities from reaching a view on whether mergers or other behavior have any impact on privacy. In the

longer term, a clear on such questions is needed to reach a common framework for competition and privacy. Such a framework is important for competition and privacy authorities to consistently balance privacy and competition where trade-offs are inevitable.

Fourth, statistical agencies and academia should work together to provide more evidence on the state of competition in digital markets not only but also on privacy. For example, policymakers should know whether firms with market power collect more/more intrusive data than those without. They should also know whether and how firms with market power hamper competition on privacy, e.g. by making privacy policies unnecessarily obscure. Digital platforms have been reluctant to share such data, providing a rationale for an obligation for them to make significantly more data accessible. Statistical agencies, academic research and civil society organizations should play a role in analyzing the data and making it more widely accessible.

1. Introduction

Authorities around the world are concerned about the lack of competition in digital markets and the harm that this may bring. Privacy is increasingly considered an area where anticompetitive harm may arise. Experts argue that "the misuse of consumer data and harm to privacy is arguably an indicator of low quality caused by a lack of competition,"[1] and "market power affects both the choices that data subjects realistically have and the privacy risks they are exposed to."[2] The Bundeskartellamt, the German national competition authority, has brought the pioneering Facebook case in which the authority seeks to establish that imposing privacy terms can amount to an abuse of dominance.[3] Exactly how this happens is still subject to debate. Court decisions first invalidated and now have reinstated the decision but modified the underlying argument.[4]

Governments are developing proposals to revive competition and reduce the potential for harm. Policymakers, including the European Commission and the German Ministry for Economic Affairs and Energy, are seeking to expand competition enforcement powers and even adopt quasi-regulatory measures that put clearer limits on what conglomerate platforms can do.[5] The potential for anticompetitive harm regarding privacy has attracted increasing attention and led to calls for more integration of competition law and privacy law.[6]

1 Furman, Jason, Diane Coyle, Amelia Fletcher, Philip Marsden and Derek McAuley (2019), "Unlocking digital competition", 43.

2 Crémer, J., Y. de Montjoye and H. Schweitzer (2019), Competition Policy for the Digital Era, https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf, 73.

3 Bundeskartellamt (2019), Decision of the Bundeskartellamt B6-22/16 regarding Facebook, https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=5

4 Higher Regional Court Düsseldorf, Decision of the Higher Regional Court of Düsseldorf in interim proceedings, 26 August 2019, Case Vi-Kart 1/19 (V) and Federal Court of Justice, Decision of the Federal Supreme Court, 23 June 2020, KVR 69/19, 23 June.

5 See European Commission (2020a), "Digital Services Act package – ex ante regulatory instrument of very large online platforms acting as gatekeepers: open public consultation" and Bundesministerium für Wirtschaft und Energie (2019), "Referentenentwurf: Entwurf eines Zehnten Gesetzes zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0"

6 See e.g. EDPS (2014), "Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy"; OECD (2020), "Consumer Data Rights and Competition – Background note 2"; DAF/COMP(2020)1; Kerber, Wolfgang (2016), "Digital Markets, Data, and Privacy: Competition Law, Consumer Law, and Data Protection"; Gewerblicher Rechtsschutz und Urheberrecht: Internationaler Teil (GRUR Int) 2016, 639–647.

For this momentum to translate into effective action, policymakers need to understand through which mechanisms competition affects privacy outcomes. Only then can policymaking effectively tackle the harm that competitive dynamics entail for privacy. Those dynamics may manifest far beyond the Facebook case, for example, in the proposed acquisition of fitness tracker company Fitbit by Google[7] and complaints by Bluetooth tracker company Tile against Apple.[8]

This paper assesses the mechanisms through which competition (or a lack thereof) affects privacy, that is, what data about consumers is collected, and to what extent they can control the data collection. This paper reviews the available evidence for which mechanisms are most relevant in practice. Therefore, this paper seeks to contribute to a consistent and evidence-based framework for addressing concerns about anticompetitive effects on privacy. Section 2 sets the scene, Section 3 assesses six ways in which competition affects privacy, and Section 4 concludes.

7 Bria, Francesca, Cristina Caffarra, Gregory Crawford, Wolfie Christl, Tomaso Duso, Johnny Ryan and Tommaso Valletti (2020), "Europe must not rush Google-Fitbit deal", Politico, 23 July, https://www.politico.eu/article/europe-must-not-rush-google-fitbit-deal-data-privacy/ and Kemp, K. (2020), "Every step you take: why Google's plan to buy Fitbit has the ACCC's pulse racing", The Conversation, 23 June.

8 Albergotti, Reed (2020), "Calls grow for European regulators to investigate Apple, accused of bullying smaller rivals", The Washington Post, 28 May, https://www.washingtonpost.com/technology/2020/05/28/tile-tells-vestager-investigate-apple-antitrust-violations/

2. Setting the scene

This section provides the background for the main analysis in Section 3 in three parts. First, it explains the key concepts of this paper. Second, recognizing that bad privacy outcomes are not only a concern in concentrated markets, an explanation how current market characteristics prevent competition on privacy from emerging is provided. Third, it details what it means to pursue an evidence-based in the context of digital competition and privacy.

2.1 Understanding privacy and competition

Privacy can be understood as the desired absence of tracking of an individual's activities and/or the degree of control that individuals have over the extent and form of tracking. Informational privacy is often equated with its legal dimension as a fundamental right: It aims to ensure informational self-determination, that is, the idea that individuals should be empowered to make informed choices about and take control of the data about themselves.[9] From an economic perspective, privacy(-friendliness) is a feature of products exchanged in markets, and consumers value privacy as an intermediate good (if undesired collection of data puts them at a disadvantage when, for example, obtaining a credit) and/or as a final good with intrinsic value. However, information asymmetries, behavioral biases, consumers' weak bargaining power and externalities can lead those markets to fail (at least regarding their privacy dimension), thus preventing consumers from obtaining their desired level of privacy.[10] Privacy regulation, in the European Union under the General Data Protection Regulation (GDPR),[11] prescribes a minimum level of privacy to preserve the fundamental right, but is not designed to address the multitude of failures in the market for privacy.[12]

Competition is the process between companies that, in the absence of a market failure, ensures economic efficiency. In short, firms have an incentive to offer better and/or cheaper products to attract consumers and increase

9 This conception of privacy is abstracted from the complexity laid out in the extensive literature on different definitions and dimensions of privacy.

10 See e.g. Acquisti, A., C. Taylor and L. Wagman (2016), "The economics of privacy", Journal of Economic Literature 54 (2), 442–492.

11 The GDPR concerns data protection, of which privacy can be considered one aspect, alongside data security.

12 Although there is no literal "market" for privacy, products that are relevant for privacy are often traded in markets; privacy as the absence of and/or control over government tracking is beyond the scope of this paper.

profits, thus collectively maximizing welfare. Competition law is designed to keep markets competitive by sanctioning anticompetitive conduct by firms and making sure that mergers do not lessen competition significantly. Competition law is one of the sharpest tools in the toolbox of the European Commission, as recent investigations ending in high fines have demonstrated.[13] However, competition law is not the only tool for fixing uncompetitive market outcomes: Where such failure is rooted in the characteristics of the markets, ex-ante regulation is used to provide a solution to the market failure such that, ideally, competition can take place within the regulatory framework.

A shared objective of privacy policy and competition policy is choice.[14] It is an indicator of functioning competition, as markets generating a broad range of offers serve various needs and preferences. Choice also matters for understanding informational self-determination. Where a market offers no choice regarding privacy, for example, because of firm concentration, consumers cannot influence to what extent they are exposed to tracking unless they abandon that market entirely.

2.2 How privacy markets set adverse incentives for consumers and firms

Consumers have voiced concerns about widespread data collection in all kinds of settings.[15] Consumers and companies face strong incentives to neither demand nor supply more privacy-friendly products and services. The current lack of competition on privacy, however, should not be misread as indicating that consumers do not care about privacy. Instead, the lack of competition on privacy results from markets setting the following privacy-adverse sets of incentives for consumers and for companies.

13 See European Commission (2017a), Case AT.39740 – Google Search (Shopping), 27 June, European Commission (2018), Case AT.40099 – Google Android, 18 July and European Commission (2019), Case AT.40411 – Google Search (AdSense), 20 March.

14 Other joint objectives include consumer welfare, market integration, and a concern with power asymmetries; see Costa-Cabral, Francisco and Orla Lynskey (2017), "Family ties: the intersection between data protection and competition in EU Law", Common Market Law Review 54 (1), 11–50.

15 For example, 42% of UK consumers name privacy as a top-of-mind concern when using the internet; see Communications Consumer Panel (2016), "Digital Footprints: A Question of Trust", https://www.communicationsconsumerpanel.org.uk/research-and-reports/digital-footprints. In addition, a lack of privacy is the second-most frequently named reason for not using smart home appliances by German consumers; see Deloitte (2018), "Smart Home Consumer Survey 2018: Ausgewählte Ergebnisse für den deutschen Markt", https://www2.deloitte.com/content/dam/ Deloitte/de/Documents/technology-media-telecommunications/Deloitte_TMT_Smart_ Home_Studie_18.pdf.

Consumers value their privacy but face excessive hurdles to protect it. The complexity of privacy markets in which personal data is traded means that consumers would need to put considerable effort into understanding the implications of accepting a single privacy policy. Even if they did, the multitude of such policies that determine an individual's privacy implies that deriving the value of privacy from their behavior regarding individual data points is almost meaningless. Even in relatively simple settings, experiments have shown that consumers struggle to make choices that they consider to be in line with their preferences,[16] and that these preferences are highly context-dependent.[17] These hurdles explain the phenomenon often called the "privacy paradox": Consumers say they value their privacy but take little action in line with their statement. For example, internet users indicate that they value items of their browsing history at around 7 EUR,[18] while their behavior gives such easy access to that data that markets value it at as low as 0.0005 USD.[19] Similarly, 72% of European consumers state that they are concerned about data collected about them on the internet,[20] but 64% of consumers indicate they do not use software to protect their privacy, and 37% have never changed their browser settings.[21] However, there is no meaningful behavioral evidence for the value of privacy that would capture it more adequately than mere inferences based on consumer behavior for individual data points.

16 A significant share of consumers state that their privacy choices do not actually match their preferences; see e.g. Nouwens, Midas, Ilaria Liccardi, Michael Veale, David Karger and Lalana Kagal (2020), "Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence", To appear in the Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, April 25-30, 2020.

17 See e.g. Winegar, Angela G. and Cass R. Sunstein (2019), "How much is data privacy worth? A preliminary investigation", Journal of Consumer Policy.

18 Carrascal, Juan Pablo, Christopher Riederer, Vijay Erramilli, Mauro Cherubini, and Rodrigo de Oliveira (2013), "Your Browsing Behavior for a Big Mac: Economics of Personal Information Online", Proceedings of the 22nd International Conference on World Wide Web (WWW '13). Association for Computing Machinery, New York, NY, 189–200.

19 Olejnik, Lukasz, Minh-Dung Tran, and Claude Castelluccia (2014), "Selling Off Privacy at Auction", NDSS '14, 23-26 February.

20 European Commission (2016a), "Special Eurobarometer 447: Online Platforms", June.

21 European Commission (2016b), "Flash Eurobarometer 443: e-Privacy", December.

Companies face a trade-off between privacy and monetization which discourages them from offering more privacy-friendly products. Companies that do often compete against incumbents that pursue aggressive monetization of personal data, in particular through ad targeting (and/or other forms of personalization, such as personalized recommendations). Privacy-friendly suppliers need to find a business model that is commercially viable despite lower profitability per user[22] while facing more stringent constraints.[23]

2.3 What kind of evidence is needed

Strong views are held about how competition affects privacy, while little evidence exists for the causal links between them. However, understanding those links is important to tailor interventions to avoid undesirable market outcomes. Addressing privacy failures specifically by dominant firms makes sense only if dominance contributes to the failure.

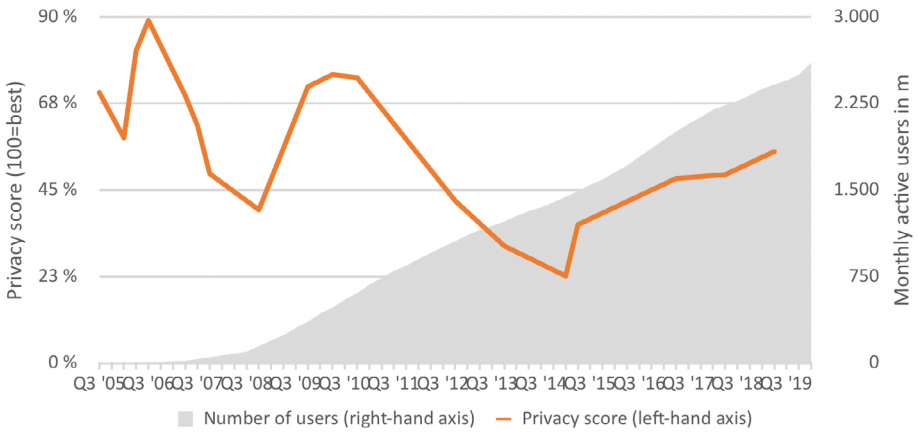
The history of Facebook provides several initial observations. Figure 1 illustrates the evolution of the platform's privacy policy, as measured by independent research, and of its market power, as proxied by the number of users. There is no linear relationship between privacy and competition, but it is more complicated. Although Facebook's privacy policy was ranked lower in early 2019 than when it was first measured in 2004, the ranking was higher and lower in between. Thus, other factors clearly are at work and disentangling them is important to understand how competition drives privacy outcomes.

22 This trade-off also applies to large firms such as Facebook, which indicated in 2018, following the Cambridge Analytica revelations, that "product development around putting privacy first" had "some impact on revenue growth". The Motley Fool (2018), "Facebook, Inc. (FB) Q2 2018 Earnings Conference Call Transcript", https://www.nasdaq.com/articles/facebook-inc-fb-q2-2018-earnings-conference-call-transcript-2018-07-25.

23 Although certain business models may still be commercially viable at lower levels of profitability, they are likely to be associated with constraints that firms with aggressive monetization do not face. For example, if auctions determine which search engines appear in a menu that consumers see when configuring new devices and browsers, privacy-friendly search engines are unlikely to appear. See DuckDuckGo Blog (2020), "Search Preference Menus: No Auctions Please", https://spreadprivacy.com/search-preference-menu-auctions/. Instead, auctions are likely to intensify the competition among providers that monetize personal data aggressively, as they can afford to spend more on acquiring individual users in such an auction.

Figure 1

Facebook's privacy behavior and user numbers over time



*Note: *change of data source from Shore/Steinman (2015) to Ranking Digital Rights*
Sources: Shore J, Steinman J. (2015), "Did You Really Agree to That? The Evolution of Facebook's Privacy Policy", Technology Science; Ranking Digital Rights; Srinivasan, D. (2019), "The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy", Berkeley Business Law Journal; Statista.

Evidence may not always allow to reach final conclusions about causality between competition and privacy, but evidence helps to reject and support theories. The following three hypotheses can be tested empirically, but provide different degrees of insights into whether the link between competition and privacy is causal:

- Most dominant firms offer bad privacy policies to their users.
- Most dominant firms offer worse privacy to their users than non-dominant firms.
- Most firms begin to offer worse privacy policies once the firms gain market power.

The first hypothesis does not allow for any conclusion about the causal relationship between market power and privacy. It could just as well be that non-dominant firms offer privacy policies that are just as bad. The second hypothesis affirms a correlation but is not informative regarding whether dominance drives privacy outcomes. It could just as well be that a bad privacy policy facilitates market power. The third hypothesis is most likely to be related to a causal influence of market power on privacy, making this hy-

pothesis the most suitable for an empirical test of the causal link between competition and privacy.

In this context, the Facebook case and the 10th amendment to the German Competition Act have triggered a debate about kind of causality is required for authorities to find exploitative use of dominance. The standard of causality has implications for the kind of evidence required to demonstrate such abuse. The courts, the Bundeskartellamt and the Federal Ministry of Economic Affairs and Energy have argued about whether exploitative abuse should be found only if the exploitative behavior is enabled by dominance ("behavioral causality") or whether it is sufficient if dominance contributes to the outcome being negative ("causality relating to the outcome").[24]

It is clear how to establish the behavioral causality with an empirical test (can and do non-dominant firms engage in this behavior?). However, it is not clear which empirical test is needed to establish causality related to the outcome. Does dominance need to play a causal role in bringing about the negative outcome (and non-dominant firms can lawfully engage in the behavior in question),[25] or does dominance only need to aggravate negative effects of the behavior? Legal scholars are split on this question.[26] If causality relating to the outcome is meant to be testable (which it should be), then this kind of causality should require some form of qualitative change in the effects. Otherwise, any behavior with negative consequences by a dominant firm (such as breaching environmental or labor laws) could be considered an abuse because the effects of certain behavior are likely to increase with firm size.

24 See Higher Regional Court Düsseldorf (2019), op. cit., Bundesministerium für Wirtschaft und Energie (2019), op. cit.

25 For example, exclusivity restrictions or most-favored nation clauses are more problematic when used by dominant firms than when used by non-dominant firms.

26 See Studienvereinigung Kartellrecht (2019), Stellungnahme der Studienvereinigung Kartellrecht zum Referentenentwurf 10. GWB-Novelle (GWB-Digitalisierungsgesetz) – Vorschriften über die Reform der Missbrauchsaufsicht und zum Thema Digitalisierung.

3. How competition affects privacy

Many digital markets are heavily concentrated, from search engines and app stores to social media and advertising. Although there are still attempts to reintroduce incentives to compete within these markets, authorities are becoming more sympathetic to quasi-regulatory approaches to reduce the harm that the lack of competition may create.[27] One dimension in which such harm may occur is privacy. However, there are different ways or mechanisms through which competition may affect privacy which require different approaches.

This section discusses six different mechanisms. Each mechanism is described. Then, whether there is evidence to support or disprove the practical relevance of the mechanism is assessed, and if not, what kind of evidence would be useful to do so.

The six mechanisms are as follows:

1. If there is less competition, companies can collect more personal data.
2. If there is less competition, consumers face less choice regarding privacy.
3. If companies merge, companies can collect and use more data.
4. Personal data in the hands of dominant firms creates more harm.
5. If there is less competition, companies can undermine competition on privacy.
6. Dominant firms can obtain quasi-regulatory powers over personal data that hamper competition.

Mechanisms 1–4 focus on whether market concentration may give rise to exploitative conduct,[28] by collecting more personal data, by providing less choice, or by using the data in more problematic ways than would be the case in a competitive setting. Mechanism 5 captures a combination of exploitative and exclusionary conduct.[29] Mechanism 6 focuses on the possibility of exclusionary conduct.

27 See European Commission (2020b), "Single Market – new complementary tool to strengthen competition enforcement: open public consultation"; Furman et al. (2019), op. cit., and Bundesministerium für Wirtschaft und Energie (2019), op. cit., Article 19a.

28 Exploitative conduct refers to abusive behavior by a dominant firm that exploits its customers, e.g., by charging excessive prices or by collecting excessive data.

29 Exclusionary conduct refers to abusive behavior by a dominant firm that makes it harder for other firms to compete, e.g., by making it harder for its customers to also buy from other firms.

3.1 If there is less competition, companies can collect more personal data.

Can firms that are exposed to less competition collect more personal data and thus, offer a lower level of privacy? This question has arisen in the context of the Facebook case. The Bundeskartellamt argues that the lack of alternatives forces consumers to accept privacy terms that the same consumers would reject in a competitive setting. The Federal Court of Justice concludes, based on the evidence of user preferences presented by the Bundeskartellamt, that more competition would have allowed offerings with less intrusive data practices to emerge.[30] However, this issue is not limited to Facebook. If less competition facilitates problematic data practices, concern in other heavily concentrated digital markets, from search engines to app stores, is warranted.

Box 1

Bundeskartellamt vs. Facebook

After a three-year investigation, the Bundeskartellamt announced in early 2019 that Facebook had violated the GDPR and therefore, abused the platform's dominance. Facebook was found to be a dominant social network that exploited its users by imposing unfair terms that users could not reject if they wanted to use the platform. These unfair terms enabled Facebook to collect data on its users from multiple sources beyond its platform, including other Facebook-owned platforms, such as WhatsApp and Instagram, as well as third-party websites that incorporated "Like" or "Share" buttons or used Facebook's analytics services. According to the Bundeskartellamt, consumers suffered the loss of control over their data, caused by Facebook's violation of various principles of the GDPR. The Bundeskartellamt argued that consumers did not give valid consent to being tracked to the extent they were,[31] nor did they expect to be tracked so extensively.[32] The Bundeskartellamt imposed on Facebook an obligation to obtain voluntary consent from users to merge data from various sources, effectively requiring "internal unbundling" of data.

30 Federal Court of Justice (2020), op. cit., para 86.

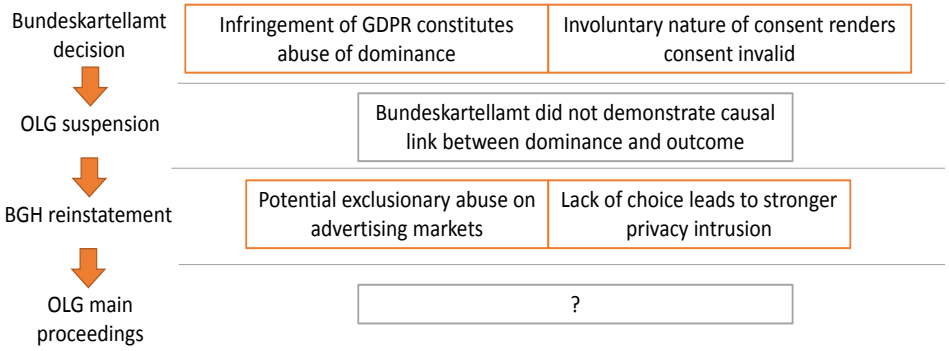
31 Bundeskartellamt (2019), op. cit., para 639.

32 Bundeskartellamt, op. cit., para 848.

As summarized in Figure 2, a local court, the Higher Regional Court (OLG) Düsseldorf, suspended the ruling because the court found that the Bundeskartellamt did not provide sufficient evidence that the allegedly abusive behavior – the infringement of the GDPR – had been enabled by Facebook's market dominance. The Bundeskartellamt appealed the suspension before the German Federal Court of Justice (BGH), which reinstated the Bundeskartellamt's decision. The federal court found that the suspension was not justified but also changed the focus of the investigation from the question of whether a GDPR infringement constitutes abuse of dominance to whether there may have been exclusionary effects on advertising markets and whether Facebook's practices unduly constrained consumer choice.

Figure 2

The main arguments at different stages of the Facebook case



Source: Stiftung Neue Verantwortung.

Conflicting views on whether market power allows firms to collect more data exist which must be tested empirically. Some argue that firms face similar incentives and constraints to collect as much data as possible within the legal boundaries, irrespective of the firms' market position. Increased data collection expands the opportunities for monetization and other uses of the data, incentivizing widespread data collection[33] unless firms pursue a strategy to differentiate their products by offering a high degree of privacy. As the consumer response to privacy as a differentiation factor is weak (see Section 2.2), it is plausible also for the competitive constraints, for example, through consumer switching, for small and large firms to be similar. Others argue, however, that market power enables firms to engage in more aggressive data practices. One reason could be that dominant firms face fewer competitive constraints than smaller firms. In principle, competitive pressure incentivizes firms to lower prices to increase demand for their products, and thus, firms have an incentive to offer better privacy settings to attract consumers. This mechanism does not work in a concentrated market, as consumers have fewer alternatives when faced with a dominant provider.

Evidence

In principle, the mechanism can be tested empirically: Do firms in a competitive environment collect less data and/or less sensitive data than dominant firms? There are powerful narratives that seem to show that as Facebook has gained market power, the platform has become increasingly less concerned about users' privacy.[34] However, it is possible to focus on facts and explanations that support a certain narrative while ignoring unexplained or even contradictory pieces of evidence. More systematic, empirical evidence could come in different forms. For example, it could be obtained by comparing certain aspects of privacy policies by a company over time (if the market concentration varied over time), or it could compare how data collection practices vary across markets characterized by different degrees of concentration.

33 See Acquisti et al. (2016) and Binns, Reuben, Ulrik Lyngs, Max Van Kleek, Jun Zhao, Timothy Libert and Nigel Shadbolt (2018), "Third Party Tracking in the Mobile Ecosystem", Proceedings of the 10th ACM Conference on Web Science (WebSci '18), Association for Computing Machinery, 23–31. The authors conducted an empirical study on the prevalence of third-party trackers on 959,000 apps from the US and UK Google Play stores. The authors found that most apps contain third-party tracking: The median number of tracker hosts included in the bytecode of an app was 10; 90.4% of apps included at least one, and 17.9% more than twenty. They also found this is a highly transnational phenomenon.

34 See Srinivasan, D. (2019), op. cit.

Thus far, the empirical evidence for the effect of market concentration on privacy is limited. One recent study shows that firms in more concentrated app markets collect more personal data than firms in less concentrated markets. However, the magnitude of the relationship is small, around 1–2%.[35] When looking at a step change in the competitive environment of apps driven by the introduction of new app categories in the Android Play Store, the relationship increases to 4–6%, but remains arguably limited.[36]

The United Kingdom's Competition and Markets Authority (CMA) conducted an extensive study of online advertising and states that *[i]f there were more choice for consumers, then there could be scope for more competition between platforms as platforms would need to compete more actively to persuade consumers of the benefits of personalised advertising. There would also be scope for other platforms to compete for consumers on the basis of alternative business models offering different options in respect of the privacy choices and the services that they offer.*[37]

This reasoning is largely based on the study's qualitative findings for advertising markets, including their complexity and consumers' sense "that they had no choice but to sign up to services despite concerns."[38] When assessing data practices across platforms, the CMA finds that Google and Facebook have access to substantially more data than other platforms that collect data; see Figure 3.

35 Kesler, Reinhold, Michael Kummer, and Patrick Schulte (2019), "Competition and Privacy in Online Markets: Evidence from the Mobile App Industry", ZEW Discussion Paper 19-064.

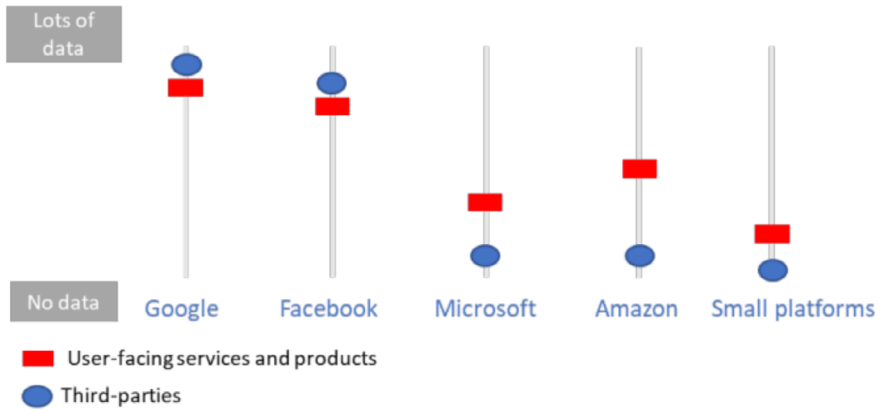
36 Results from app markets should be generalized to other digital markets with caution. One reason is that the privacy paradox may be more pronounced in app markets than in other markets possibly because of the high number of apps installed by many users. See e.g. Savage, S. J., and D. M. Waldman (2015), "Privacy tradeoffs in smartphone applications", Economics Letters 137, 171–175, who find high valuations of individual data points collected by smartphone apps, while only very few consumers pay for less data-intensive apps in practice.

37 CMA (2020), "Online platforms and digital advertising. Market study final report" 1 July, para 4.121.

38 Ibid., para 4.117.

Figure 3

Illustration of the scale of data collection by certain platforms, split by two broad data sources



Note: Small platforms include Twitter, Snap, TikTok, and Pinterest.
Sources: CMA (2020), "Online platforms and digital advertising. Market study final report" 1 July, Appendix F.

In addition, Google and Facebook are the only platforms that appear to collect even more data through third-party sources than through user-facing services and products. Although these findings do not allow for inferring a causal effect of concentration on data collection practices, the findings are compatible with the existence of such an effect.

For a clearer view on the strength of the mechanism in different settings, especially in legal proceedings that hinge on the validity of the mechanism, more studies are needed. When conducting this type of study, reverse causality warrants special caution. For example, in app markets, the positive correlation between data permissions and concentration could also be driven by the increased monetization of data-intensive apps, which, in turn, may allow them to invest more in improving their product.

Once an effect of concentration on data-collecting practices is found to be present in a specific market, a benchmark is needed to distinguish potentially abusive behavior from competitive behavior. This point is discussed further in the following section.

3.2 If there is less competition, consumers face less choice regarding privacy.

Do consumers face less choice regarding privacy when they deal with a firm that has only a few and/or weak competitors? This question arose in the Facebook case, but the answer is self-evident: Less competition means less choice (see Section 2.1). The challenge is to clearly conceptualize choice such that it is clear when the lack of choice amounts to anticompetitive harm. Specifically, in the Facebook case, the Bundeskartellamt[39] and the Federal Court of Justice[40] find that the lack of choice when faced with a dominant player puts informational self-determination at risk and constitutes exploitative abuse of users. As stated in the previous section, any such finding for Facebook is likely to be highly relevant for other concentrated markets.

Conceptualizing choice in the context of privacy and competition builds on the notions of informational self-determination and choice between options as a driver of competition (see Section 2.1). This means that a lack of alternative options can make a firm's behavior problematic just because the firm is dominant, even if its behavior does not systematically differ from that of smaller firms (i.e., even if evidence were to show that the mechanism in Section 3.1 does not apply in a specific market). Specifically, a strong market position can undermine consumer choice regarding privacy because consumers are deprived of the option to change providers to get different privacy options and can only "leave" the market altogether.

Evidence

To make this mechanism applicable to actual markets, it is important to define what it means for a company to provide sufficient choice regarding privacy. Only then is it clear whether companies need to act, or authorities need to intervene to increase choice. For example, it is not plausible that dominant firms with high privacy standards should be obligated to offer more choices to consumers to share more data.

First, a competitive benchmark must clarify when competition is no longer assumed to provide sufficient choice, requiring additional scrutiny of privacy practices. A starting point could be dominance, a well-established concept in competition law, but it may have to be combined with some measure of tracking capabilities. Some companies may gain "data power" before reaching the threshold of dominance, while others may have market power with-

39 Bundeskartellamt (2019), op. cit., para 876.

40 Federal Court of Justice (2020), op. cit., para 103.

out significant tracking capabilities. Although defining a relevant threshold is not easy, current discussions about special rules for firms with gatekeeper power[41] or cross-market significance[42] show that it is possible to develop new concepts that better capture the dynamics of digital markets.

Second, to provide sufficient choice, with which requirements must the behavior of those firms comply? In the Facebook case, the Federal Court of Justice finds that not allowing consumers to choose whether they want personalization based on data collected only on facebook.com or also on other domains amounted to an anticompetitive restriction of choice.[43] Implicit in this finding appears to be the notion that the consent given by consumers to legitimize the firms' processing is not as voluntary as it should be to enable real choice. Others suggest abandoning consent as a legal ground for processing data by data-powerful companies, suggesting that "the existence of market power in a competition law sense may act as an indicator challenging the validity of consent as a legitimate ground for processing of personal data."[44] A similar argument has been made by the European Data Protection Supervisor.[45]

Conceptualizing choice vis-à-vis firms with data power as additional requirements to obtain consent is a reasonable approach. This approach would enable competition and data protection authorities to test whether such requirements are met. Choice should empower consumers to make meaningful decisions. For example, if companies enable people to adjust privacy settings to their preferences (with all data optional except that necessary for providing a service), consumers benefit from the privacy policy that best matches their preferences.

41 See European Commission (2020a), op. cit., and European Commission (2020b), op. cit.

42 See Furman et al. (2019), op. cit., and Bundesministerium für Wirtschaft und Energie (2019), op. cit., Article 19a.

43 Federal Court of Justice (2020), op. cit., para 58.

44 Graef, Inge, Damian Clifford, and Peggy Valcke (2018), "Fairness and Enforcement: Bridging Competition, Data Protection and Consumer Law", International Data Privacy Law 2018 8(3), 207.

45 EDPS (2014), op. cit., 35.

3.3 If companies merge, companies can collect and use more data.

Can companies reduce their privacy provisions by acquiring other companies and thus expanding their tracking capabilities? Google, Facebook, and others have bought numerous businesses that not only allowed the companies to tap into new markets but also enabled them to expand and deepen their capabilities to collect and analyze personal data. The most recent controversy is Google's proposed acquisition of Fitbit that the European Commission is investigating. Experts have been calling for closer scrutiny of the possibilities that the additional data will give to Google,[46] with the impact on privacy an important factor.

Mergers are special events for competitive review because market concentration and links between markets may increase substantially. Competition authorities can test whether the merger-driven changes are likely to harm the competitive process. The authorities can prescribe remedies to mitigate the harm, or can even block transactions. However, authorities are still hesitant to consider the impact on privacy in their competitive assessment. In principle, the GDPR applies before and after a merger. From a competition perspective, the more relevant question is whether privacy quality degrades irrespective of whether the GDPR is complied with.

It makes sense to assess the impact of a merger on privacy in the same way that competitive implications for price or innovation are scrutinized. Merging datasets with personal data often has privacy implications, e.g., if this enables the construction of larger profiles.[47] Currently, privacy risks are not assessed, with competition authorities directing the responsibility for assessing privacy implications to data protection authorities. However, this misses the point, because data protection authorities can intervene only if the GDPR is breached, not if privacy practices deteriorate but still remain compliant with the law.

46 See Privacy International (2020), "The Google/Fitbit merger – NOT ON OUR WATCH!" https://www.privacyinternational.org/campaigns/googlefitbit-merger-not-our-watch, Bria et al. (2020), op. cit., Kemp, K. (2020), op. cit.

47 For a review, see e.g. Binns and Bietti (2019), op. cit.

Evidence

Competition authorities, including the European Commission, have argued that privacy considerations should not play a role in competitive assessments of mergers because companies do not compete on privacy.[48] This, however, should not be misread as evidence that consumers do not value their privacy. The lack of competition on privacy is more appropriately linked to a lack of transparency and bad incentives (see Section 2.2).

Competition authorities may struggle to recognize competition on privacy when it is in front of them. For example, the European Commission recognized the importance of the WhatsApp superior privacy policy for consumers, but the commission did not consider post-merger privacy reductions to be relevant for competition. The commission mentioned in the Facebook/WhatsApp merger clearance that "privacy and security [...] are becoming increasingly valued" and that "[p]rivacy concerns also seem to have prompted a high number of German users to switch from WhatsApp to Threema in the 24 hours following the announcement of Facebook's acquisition of WhatsApp."[49] Nonetheless, the European Commission considered the platforms' different privacy features to indicate that Facebook and WhatsApp were not close competitors,[50] concluding that "[a]ny privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the Transaction do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules."[51] It is not clear what kind of evidence would have prompted the European Commission to consider the foreseeable impact on privacy as a matter for competition.

Some have proposed explicitly considering privacy in merger proceedings by adding them to the scope of "public interest" that requires balancing with the competitive outcome of a merger.[52] This option is highlighted in a joint study by the Bundeskartellamt and the French Autorité de la Concurrence.[53]

48 See Ocello, Eleonora, Cristina Sjödin and Anatoly Subočs (2015), "What's Up with Merger Control in the Digital Sector? Lessons from the Facebook/WhatsApp EU merger case", European Commission Competition merger brief.

49 European Commission (2014), Case No COMP/M.7217 – Facebook/WhatsApp, 3 October, para 174.

50 Ibid., para 102.

51 Ibid., para 164.

52 See Lynskey (2019), op. cit., 218–219.

53 They mention how cultural diversity is intended to be taken into consideration in the European Union's actions and raising the question whether a similar approach could be taken in relation to data protection. Bundeskartellamt and Autorité de la concurrence (2016), "Competition Law and Data".

Although rare, public interest assessments are feasible in practice. For example, media plurality was the subject of a UK review of the Twenty-First Century Fox/Sky merger undertaken in parallel with the investigation by the European Commission.[54] However, politicians may be tempted to include other variables, such as sustainability or implications for labor markets, in the same way, providing ample opportunity for problematic political interference through merger policy.

A better approach would be to make it easier to include privacy in merger decisions: If many consumers articulate concern about privacy in a specific market (especially if the target offers higher privacy protections), that could be deemed sufficient to consider the privacy implications of the merger. Given the difficulties that consumers who wish to take action to protect their privacy (see Section 2.2) face, seemingly privacy-unconscious behavior should not count as a strong argument for dismissing stated privacy concerns. Whether companies comply with the GDPR is a separate question (which data protection authorities are better placed to tackle), but privacy can suffer as a consequence of less competition without a breach of the GDPR, and that should be a concern for competition authorities.

3.4 Personal data in the hands of powerful firms can create more harm.

Is personal data in the hands of dominant firms more dangerous than the same data in the hands of smaller firms? Some raise concerns whether larger firms, even if they do not have access to significantly more personal data, can cause more detriment to consumers with the data. This would be the case if dominant firms were able to apply differential treatment or discriminate more effectively and extract more consumer surplus by doing so. Such harm could arise, for example, if a large booking platform like Booking.com had a greater ability to set prices for individual hotels in line with a consumer's willingness to pay than the hotel itself (assuming it had access to the same information[55]).

54 See European Commission (2017b), "Mergers: Commission Clears 21st Century Fox's Proposed Acquisition of Sky under EU Merger Rules", Press release.

55 In practice, larger companies tend to have access to more data also about individual consumers. However, from a theoretical perspective, it makes sense to disentangle two effects: can firms that are exposed to less competition collect more data, assuming similar uses of data, (Section 3.1) or can they use the same data for more problematic purposes (this section)?

In general, it is challenging to assess which factors drive differential treatment to consumers' detriment. One well-studied form of differential treatment is price personalization; i.e., a firm sets different prices for different consumers based on the data the firm has about them. For price personalization, a broad literature exists that assesses implications for different market participants. It finds that whether personalized prices increase or decrease consumer welfare depends on the market characteristics.[56] The question in relation to privacy and competition is whether larger market concentration makes personalized pricing systematically more problematic for consumers.

Evidence

A recent survey of the theoretical literature concludes that "[t]here is very limited theoretical relationship between ex ante market power and consumer outcomes."[57] The authors find that the effect of price discrimination is more likely to increase competition as well as consumer welfare if price discrimination is based on switching costs or brand preference. The opposite is true if price personalization increases search costs. However, it is not clear whether and why the latter would apply more often to concentrated markets. Similarly, a joint study by the Bundeskartellamt and the French Autorité de la Concurrence highlights the potential procompetitive and welfare-enhancing effects price personalization can bring about.[58] The OECD also finds that even in concentrated markets, price discrimination can increase incentives to innovate.[59]

Empirical studies would help to test whether the theoretical models adequately capture how price personalization works in practice. Empirical studies would be useful to corroborate the finding that dominance is not a driving factor of potential consumer harm through price personalization, and to test which factors determine the effects in actual market settings.

However, the current theoretical findings do not rule out the possibility that consumers may be more skeptical about price personalization by larger players which, in turn, could be driven by perceptions of procedural fairness

56 See for an overview, Office of Fair Trading (2013), "The economics of online personalised pricing", OFT 1488.

57 Townley, Christopher, Eric Morrison and Karen Yeung (2017), "Big Data and Personalised Price Discrimination in EU Competition Law", King's College London Law School Research Paper 2017-38.

58 Bundeskartellamt and Autorité de la concurrence (2016), op. cit.

59 OECD (2018), "Personalised Pricing in the Digital Era. Background Note by the Secretariat", DAF/COMP(2018)13, 21.

and asymmetry in bargaining power.[60] It is an open question how such fairness concerns should be addressed, and what role privacy should play.

It is possible that other data uses or other forms of differential treatment have more negative effects when pursued by dominant firms. However, the absence of theoretical or empirical evidence of dominance being a driver of negative effects of price personalization suggests that there is no obvious reason to assess data practices by dominant firms with a focus on these uses. For personalized prices, it is desirable to better understand the potential benefits and harms, from the perspective of competition, but also from a broader fairness perspective. However, this is irrespective of whether prices are personalized by a small or a dominant firm.

3.5 If there is less competition, companies can undermine competition on privacy.

Would competition on privacy be more effective in markets that were more competitive? This would be the case if the lack of competition on privacy were a result of dominant firms influencing whether consumers perceive privacy as a relevant product feature.[61] Therefore, dominant firms would be able to impose worse privacy settings than would be the case in a competitive setting – but as a consequence of their actions to undermine not just competition in general but also competition specifically on privacy. For example, if Facebook and Google were to make their privacy policies intentionally obscure, privacy-friendly competitors such as DuckDuckGo and Mastodon would face higher hurdles to convince consumers that their privacy offerings are superior. Consumers might not understand that Facebook's and Google's policies are bad for consumer privacy. Thus, consumers would find it hard to assess the benefits of switching to DuckDuckGo and Mastodon, making them more reluctant to switch.

60 For an overview of fairness concerns in digital markets, see Jenkins, H. and A. Blankertz (2020), "Regulating e-commerce through competition rules: a fairness agenda?" in Gerard, Damien, Assimakis Komninos and Denis Waelbroeck (eds.), Fairness in EU Competition Policy: Significance and Implications. An Inquiry into the Soul and Spirit of Competition Enforcement in Europe, GCLC Annual Conference Series.

61 See Kemp (2019), op. cit.

Different mechanisms may allow dominant firms to undermine competition on privacy:

- First, large firms can be perceived as setting a standard in privacy policies that discourages consumers from comparing privacy policies across providers. 62 Although many non-dominant firms monetize personal data (see Section 2.2), and have an interest in obscuring this, they are likely to be much less effective at doing so. Given the huge market presence of many large digital platforms, their privacy policies can be expected to be disproportionately influential on whether consumers perceive reading and comparing privacy policies to be feasible and useful. In addition, the extensive capabilities of those large companies in designing products would make them well placed to develop accessible privacy policies. The firms conduct extensive testing of their users' experience and routinely adjust products accordingly. Thus, these firms have superior insights and capabilities to shape their policies to dis- or encourage consumer willingness to engage with privacy policies. Therefore, even if a start-up wishes to enter the market with a more privacy-friendly product, the start-up can struggle to motivate consumers to assess the differences between privacy policies. If consumers become accustomed to not understanding privacy policies, they do not bother to engage even with privacy-friendly products.
- Second, the behavior of large firms may also have a disproportionate effect on how consumers perceive the trustworthiness of privacy policies. Even if consumers could compare privacy policies, they may lack confidence in whether those policies effectively constrain a company's data practices. Reasons for such distrust may include the policies' lack of future commitment. This allows firms to weaken privacy protections step by step. This practice has been extensively documented regarding Facebook's terms and conditions,63 as well as in the legibility of Google's privacy notice.64 The frequent reports on company

62 Kemp (2019) states that "[t]he central problem is not that consumers fail to read privacy policies, but that concealed data practices currently prevent this from being an effective means of comparing the privacy quality offered by different suppliers."

63 Companies can easily reverse any procedures that are intended to give consumers more (influence on) privacy. One example was the announcement by Facebook in 2009 that future changes to terms of use and privacy policies would be subject to user participation and binding voting processes, Facebook (2009), "Facebook Opens Governance of Service and Policy Process to Users", 26 February, https://about.fb.com/news/2009/02/facebook-opens-governance-of-service-and-policy-process-to-users/
For a comprehensive overview of Facebook's changes to it privacy policies, see Srinivasan, D. (2019), op. cit.

64 Litman-Navarro, Kevin (2019), "We Read 150 Privacy Policies. They Were an Incomprehensible Disaster", https://www.nytimes.com/interactive/2019/06/12/opinion/face-

breaches of policies and commitments further reduce consumer trust in privacy policies. This lack of trust may harm not only the firms involved but also firms that want to provide a product that offers higher privacy standards. These standards may not only be difficult to distinguish due to the concealed nature of data practices in the wider market but also hard to believe.

Evidence

Through such mechanisms, dominant players may be able to shape the competitive process and make it harder for competitors to successfully offer privacy-friendly products. Thus, ineffective competition may aggravate the lack of competition on privacy, further reducing competitive constraints on firms to limit the intrusiveness of their data practices. In contrast to the previous mechanisms that rely on some form of competitive benchmark to demonstrate the exploitative nature of the privacy practices, this mechanism includes exclusionary effects; that is, consumers may be harmed because the behavior is capable of reducing competition on privacy. That reduces the need for a meaningful privacy benchmark if exclusionary effects can be demonstrated. For that, it would be important to show that more transparent data practices lead to more competition. Alternatively, it would also be helpful to provide evidence that large firms' data practices affect the data practices across markets more widely.

These claims are not easy to test in practice because many markets are influenced by the presence of a large player that pursues aggressive data monetization and has an incentive to discourage competition on privacy. Thus, even if privacy policies turn out to be similarly opaque across markets, this may be driven by widespread suppression of competition on privacy.[65]

Little systematic evidence for how competition affects the extent to which competition on privacy takes place exists. As a starting point, the findings of a recent study of privacy policies are in line with larger firms hampering competition on privacy.[66] The study finds that privacy policies, with increasing firm size, are longer, are more difficult for the average reader to understand, and are accompanied by a higher number of third-party trackers.[67]

book-google-privacy-policies.html.

65 See Costa-Cabral and Lynskey (2016), 14.

66 Ramadorai, Tarun, Ansgar Walther, and Antoine Uettwiller (2019), "The Market for Data Privacy", CEPR DP13588.

67 Their legal language is also clearer, indicating that larger firms may be better at using legal expertise to ensure the compliance of their data practices. What is missing, however, is evidence that the design or format of privacy policies or other aspects related to data practices have an impact on the feasibility of competition on privacy.

3.6 Dominant firms can obtain quasi-regulatory powers over personal data that hamper competition.

Can powerful companies use their market position to decide how personal data is shared within their ecosystem, potentially reducing competition? When dominant firms decide whether to share personal data and/or enable its collection, privacy may be enhanced, but competition may suffer as a result. Small firms may find themselves shut out because they are unable to compete with the dominant firms in related markets that draw on personal data as an input.

There are several examples where such behavior has occurred. Chrome, a Google-operated browser, announced that it would phase out third-party cookies by the end of 2021 to reduce undesired tracking.[68] However, others have criticized that Google harms privacy more than many providers of third-party cookies do, and that Google uses privacy as an excuse to strengthen its position in advertising markets.[69] Google's acquisition of Fitbit, a producer of fitness trackers, has been accompanied by similar concerns about Google's ability to engage in more invasive data practices while making data less accessible for providers of healthcare or insurance services.[70] Similarly, Bluetooth technology start-up Tile filed a complaint about Apple's restrictions on the use of location data by apps that is more restrictive for third-party apps than for Apple's own apps.[71]

In principle, limits on the sharing of personal data are welcome. However, those limits do not improve privacy, and can harm competition if the same data is used without concern within a company but not accessible to external companies, even if they offer privacy standards that are at least as high and provide a service that consumers value. For example, although the German competition law reform makes it easier to obtain access to data from other companies,[72] there is significant legal uncertainty about what this means for

68 Lardinois, Frederic (2020), "Google Wants to Phase Out Support for Third-Party Cookies in Chrome Within Two Years", https://techcrunch.com/2020/01/14/google-wants-to-phase-out-support-for-third-party-cookies-in-chrome-within-two-years/.

69 Bovard, Rachel (2020), "Why Google's New Limits On Third-Party Cookies Are Another Attempt To Control The Web", https://thefederalist.com/2020/02/17/why-googles-new-limits-on-third-party-cookies-are-another-attempt-to-control-the-web/

70 See Kemp (2020), op. cit and Bria et al. (2020), op. cit.

71 Albergotti, Reed (2020), "Calls grow for European regulators to investigate Apple, accused of bullying smaller rivals", The Washington Post, 28 May, https://www.washingtonpost.com/technology/2020/05/28/tile-tells-vestager-investigate-apple-antitrust-violations/

72 See Bundesministerium für Wirtschaft und Energie (2019), op. cit., see also Blankertz, A. (2019), "Digital blueprint. A German proposal for tackling dominance and data", Competition

personal data, i.e., under what conditions such access is compatible with the GDPR and the impact of competition on privacy.

Evidence

When does not sharing data enhance privacy, and when does it shut out competitors? How to draw the line between privacy-enhancing and potentially exclusionary behavior is not yet clear. Examining the impact of the behavior on privacy and on competition would be the first step: If privacy protection does not improve, but competition suffers, the behavior should not be permitted. This would be the case if, for example, Apple uses its increased access to Bluetooth data to provide products similar to that by Tile but does not include higher privacy protection. In such a case, it is not clear why Tile should not be granted access to the data in the same way (assuming the consumer is made aware of the data use in compliance with the GDPR). The challenge is to distinguish between more and less privacy-friendly practices (both of which should be presumed compliant with the GDPR), which requires further research and reaching (preliminary) consensus on how to measure privacy.[73]

Preliminary evidence is available for assessing the effects of the behavior in question. As a starting point, the CMA finds in its market study on online advertising that Facebook and Google have a strong competitive advantage vis-à-vis smaller market players through superior access to first-party data.[74] In addition, the companies "increasingly appear to be acting in a quasi-regulatory capacity in relation to data protection considerations, setting the rules around data sharing not just within their own ecosystems, but for other market participants."[75] Regarding Google's announcement that the platform would discontinue third-party cookies, the CMA estimates that in the short term, advertisers, if unable to target advertising using cookie data, would lose about 70% of their revenue if they competed against others that could target using such data.[76] This shows the far-reaching effects of this behavior on competition. However, it is at least questionable whether it constitutes an enhancement of privacy if Google prevents others from using data for targeting but continues to target users directly.

Law Insight, December.

73 For an overview of different privacy metrics, see Wagner, Isabel and David Eckhoff. 2018. Technical Privacy Metrics: A Systematic Survey. ACM Comput. Surv. 51, 3, Article 57,July.

74 See CMA (2020), op. cit., para 5.307 and 5.308.

75 Ibid., para 5.315.

76 Ibid., Appendix F.

Although a privacy-enhancing effect may not always exist, the fact that such effects may exist points toward potential tension between competition and privacy. To what extent can competitive restrictions be tolerated if they also increase privacy? Currently, there is no common framework for assessing this kind of question from a competition perspective and from a privacy perspective.

4. Conclusion and recommendations

Table 1 summarizes the six mechanisms and the availability of the evidence reviewed in Section 3.

Table 1

Overview of mechanisms through which competition affects privacy

	Mechanism	Evidence
1	If there is less competition, companies can collect more personal data.	Limited effect in app markets and tentative evidence in advertising markets.
2	If there is less competition, consumers face less choice regarding privacy.	Conceptual argument, open question for competition authorities: What is the benchmark for identifying anticompetitive conduct and restoring choice?
3	If companies merge, companies can collect and use more data.	Self-evident, and a matter for competition authorities if privacy is a relevant factor for competition.
4	Personal data in the hands of dominant firms creates more harm.	None based on the (theoretical) evidence of the effects of price personalization: no link between market power and negative outcomes for consumers.
5	If there is less competition, companies can undermine competition on privacy.	Limited to the readability of privacy policies decreasing as firm size increases.
6	Dominant firms can obtain quasi-regulatory powers over personal data that hamper competition.	Harm to competition evident, unclear whether there are benefits for privacy.

Source: Stiftung Neue Verantwortung

In summary, the impact of competition on privacy manifests in various ways. Some of the mechanisms would strongly benefit from more research to bet-

ter capture their relevance across markets and a clear measure of the quality of a privacy policy to facilitate comparison. Others, however, have sufficient empirical and conceptual support to warrant stronger intervention by policymakers. These interventions should include increased requirements for consent and internal data-sharing, as well as include consumers to shape privacy policies to promote choice. Furthermore, the impact of mergers on privacy should be considered if consumers express concerns regarding the data involved.

Although competition and data protection authorities must collaborate to define choice and a common framework for assessment, four concrete measures should be taken to mitigate anticompetitive harm on privacy:

- **Choice vis-à-vis dominant firms must be ensured**. Options for doing so include involving consumers in the development of privacy policies and unbundling consent and/or unbundling data such that dominant firms must obtain more granular consent before sharing data internally.
- Given the obstacles consumers face in protecting their privacy, authorities should be comfortable **relying on stated preferences** to assess whether consumers care about privacy in a specific market. This consideration applies specifically to **mergers where a reduction in privacy can be beyond the scope of the GDPR and relevant for competition**.
- **Metrics to assess the quality of a privacy policy** are needed to facilitate assessing whether a practice improves or degrades privacy. This will make some simplification inevitable but is necessary to consistently assess, for example, whether practices with exclusionary effects benefit privacy.
- **More evidence** is needed to comprehensively assess the impact of competition on privacy across markets. Digital platforms have been reluctant to share such data, providing the rationale to obligate them to make significantly more data accessible. This can then be assessed by statistical agencies and academic researchers.

4.1 Mechanism-specific recommendations

On mechanism 1: There is limited empirical evidence for whether companies collect less personal data when facing more competition, and evidence is hard to obtain with the amount of data currently available. Academic researchers should **provide more evidence** to assess whether firms with mar-

ket power collect more or more intrusive data than those without. Providing this evidence is possible only with access to significantly more data on the platforms' practices. Authorities and statistical agencies should **obligate digital platforms to share more data** to allow for a systematic analysis of their impact on privacy.[77]

On mechanism 2: With choice as a shared objective of competition and privacy policy, it is important to reach a **clearer understanding of what it means for a company to offer choice regarding privacy**. This requires the involvement of privacy and competition scholars, for example, based on the notion that the scope of competition law should include wider social implications of market interactions,[78] and a collaborative approach between authorities.[79]

A clearer notion of choice will also help develop **mechanisms to ensure choice vis-à-vis dominant firms that does not rely on individual bundled consent.** Imposing additional requirements for dominant firms to rely on consent as a legal basis for data processing could be an expression of the special responsibility of powerful firms to ensure users still have choice when making decisions about their privacy. Different options exist:

- **Involving consumers in the development of privacy policies**: This would shift some of the burden of consent to an earlier stage at which consumers would need to be given real influence over the outcome. Facebook tried democratic decision-making regarding the use of personal data in the past but abandoned the practice.[80] Alternatives or complements may include forms of community consent, for example, involving ethics boards, citizen juries, surveys, or open discussions about Legitimate Interests Assessments.[81]
- **Unbundling consent and unbundling data**: As the Bundeskartellamt required Facebook to do, dominant firms could be obligated to obtain more granular consent from consumers. Specifically, this could mean giving consumers the option to share only data necessary to provide a service, with data collected from other sources optional. This approach

77 Expert Group for the Observatory on the Online Platform Economy (2020), "Progress Report Expert Group for the Observatory on the Online Platform Economy Work stream on Measurement & Economic Indicators".

78 Lianos, Ioannis (2018), "Polycentric Competition Law", https://ssrn.com/abstract=3257296

79 Binns and Bietti (2019), op. cit., 37.

80 See footnote 63.

81 Tennison, Jeni (2020), "Community consent", 17 January, https://www.jenitennison.com/2020/01/17/community-consent.html.

is gaining popularity not only with data protection scholars but also with economists.[82] In doing so, however, it is important design an intervention to avoid effects that consent as stipulated by the GDPR is known to have. That is, the GDPR can reinforce concentration, and consent may be obtained more easily by large and incumbent firms because they tend to serve larger market segments,[83] and because their reputation makes consumers less responsive to the firms' data practices.[84]

On mechanism 3: In a merger, a reduction in privacy can be beyond the scope of the GDPR and relevant for competition authorities. Given the challenges for consumers face to make effective privacy choices (see Section 2.2), competition authorities should be comfortable **relying on stated preferences to assess whether consumers care about privacy in a specific market**. If there are privacy risks as a consequence of increased concentration following a merger, this would not have to prevent the merger, but appropriate remedies would need to be agreed to maintain privacy quality, such as preventing merging of profiles unless explicitly approved by a user.

On mechanism 4: There is no evidence that dominant firms are likely to create more harm than smaller firms with the same amount of data.

On mechanism 5: **More evidence** would be helpful to understand whether and how firms with market power hamper competition on privacy e.g. by making privacy policies unnecessarily obscure and undermining trust in them. Although there is some evidence that the legibility of privacy policies decline with firm size, it is important to test whether this has an impact on the feasibility of competition on privacy.

On mechanism 6: The quasi-regulatory powers of some particularly powerful firms create concerns, because the negative effects on competition are evident, but the supposed enhancing effects on privacy less so. As a first step, it would be helpful to develop **metrics for assessing the quality of a privacy policy** to facilitate reaching an understanding of whether a practice improves privacy. Any such measure comes with challenges, such as how

82 Condorelli, Daniele, Jorge Padilla (2019), "Data-Driven Predatory Entry with Privacy-Policy Tying".

83 Campbell, J., A. Goldfarb and C. Tucker (2015), "Privacy regulation and market structure", Journal of Economics & Management Strategy 24(1), 47–73.

84 Although consumers generally download fewer apps when they come with privacy-sensitive permissions, this is not true for apps provided by well-known brands. Kummer, Michael and Patrick Schulte (2016), "When Private Information Settles the Bill: Money and Privacy in Google's Market for Smartphone Applications", ZEW Discussion Paper 16-031, 26.

to reduce complexity in a way that is not misleading or prone to gaming by firms. A positive side effect of privacy metrics is that they could also increase transparency for consumers who are currently overwhelmed by complexity but may be more willing to engage and take action if privacy policies are easier to comprehend and compare.[85] Increasing transparency may also be a more prudent way to strengthen privacy than developing stricter regulation,[86] and could stimulate competition on privacy.

If greater privacy were found to come at the expense of competition in certain cases, a **common framework is necessary for competition and privacy authorities to make consistent trade-offs** to resolve tensions between privacy and competition. The primary objective should always be to preserve as much as possible of one while increasing the other. For example, privacy-enhancing technologies may help to preserve confidentiality while enabling more competition,[87] and stronger data portability can also contribute to competition.[88] If this is not feasible, there should be clear guidance for how to balance privacy and competition to avoid conflicting views and decisions by authorities.

85 The primary audience for such metrics should be experts as consumers may need different metrics and formats to better understand privacy implications, see e.g. Ben-Shahar, Omri and Adam Chilton (2016), "Simplification of privacy disclosures: an experimental test", The Journal of Legal Studies 45 (S2), 41–67 and Conpolicy (2018), „Wege zur besseren Informiertheit. Verhaltenswissenschaftliche Ergebnisse zur Wirksamkeit des OnePager-Ansatzes und weiterer Lösungsansätze im Datenschutz".

86 Economic models indicate that transparency is superior to a level of data collection prescribed by the regulator, see de Cornière, Alexandre and Taylor, Greg (2020), "Data and Competition: a General Framework with Applications to Mergers, Market Structure, and Privacy Policy", TSE Working Papers 20-1076.

87 CMA (2020), op. cit., Appendix G.

88 See Krämer, Jan, Pierre Senellart, and Alexandre de Streel (2020), "Making data portability more effective for the digital economy", CERRE Report.

Acknowledgements

I am very grateful to those who have provided input and comments in numerous exchanges, including Simon Assion, Bird & Bird, David Howarth, K&L Gates, Katharine Kemp, UNSW Sydney, Wolfgang Kerber, Universität Marburg, Sebastian Louven, Universität Oldenburg, Orla Lynskey, London School of Economics, Heiko Richter, Max-Planck-Institut für Innovation und Wettbewerb, SNV student assistant Fintan Viebahn, and many more.

Bibliography

Acquisti, A., C. Taylor and L. Wagman (2016), "The economics of privacy", Journal of Economic Literature 54 (2), 442–492.

Albergotti, Reed (2020), "Calls grow for European regulators to investigate Apple, accused of bullying smaller rivals", The Washington Post, https://www.washingtonpost.com/technology/2020/05/28/tile-tells-vestager-investigate-apple-antitrust-violations/.

Ben-Shahar, Omri and Adam Chilton (2016), "Simplification of privacy disclosures: an experimental test", The Journal of Legal Studies 45 (S2), 41–67.

Binns, Reuben, Ulrik Lyngs, Max Van Kleek, Jun Zhao, Timothy Libert and Nigel Shadbolt (2018), "Third Party Tracking in the Mobile Ecosystem", Proceedings of the 10th ACM Conference on Web Science (WebSci '18), Association for Computing Machinery, 23–31.

Blankertz, A. (2019), "Digital blueprint. A German proposal for tackling dominance and data", Competition Law Insight, December.

Bovard, Rachel (2020), "Why Google's New Limits On Third-Party Cookies Are Another Attempt To Control The Web", https://thefederalist.com/2020/02/17/why-googles-new-limits-on-third-party-cookies-are-another-attempt-to-control-the-web/.

Bria, Francesca, Cristina Caffarra, Gregory Crawford, Wolfie Christl, Tomaso Duso, Johnny Ryan and Tommaso Valletti (2020), "Europe must not rush Google-Fitbit deal", Politico, 23 July, https://www.politico.eu/article/europe-must-not-rush-google-fitbit-deal-data-privacy/.

Bundeskartellamt (2019), Decision of the Bundeskartellamt B6-22/16 regarding Facebook, https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=5.

Bundeskartellamt and Autorité de la concurrence (2016), "Competition Law and Data".

Bundesministerium für Wirtschaft und Energie (2019), "Referentenentwurf: Entwurf eines Zehnten Gesetzes zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0".

Campbell, J., A. Goldfarb and C. Tucker (2015), "Privacy regulation and market structure", Journal of Economics & Management Strategy 24(1), 47–73.

Carrascal, Juan Pablo, Christopher Riederer, Vijay Erramilli, Mauro Cherubini, and Rodrigo de Oliveira (2013), "Your Browsing Behavior for a Big Mac: Economics of Personal Information Online", Proceedings of the 22nd International Conference on World Wide Web (WWW '13). Association for Computing Machinery, 189–200.

Competition and Markets Authority (2020), "Online platforms and digital advertising. Market study final report" 1 July.

Communications Consumer Panel (2016), "Digital Footprints: A Question of Trust", https://www.communicationsconsumerpanel.org.uk/research-and-reports/digital-footprints.

Condorelli, Daniele, Jorge Padilla (2019), "Data-Driven Predatory Entry with Privacy-Policy Tying".

Conpolicy (2018), „Wege zur besseren Informiertheit. Verhaltenswissenschaftliche Ergebnisse zur Wirksamkeit des OnePager-Ansatzes und weiterer Lösungsansätze im Datenschutz".

Costa-Cabral, Francisco and Orla Lynskey (2017), “Family ties: the intersection between data protection and competition in EU Law”, Common Market Law Review 54 (1), 11–50.

Crémer, J., Y. de Montjoye and H. Schweitzer (2019), Competition Policy for the Digital Era, https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf.

de Cornière, Alexandre and Taylor, Greg (2020), “Data and Competition: a General Framework with Applications to Mergers, Market Structure, and Privacy Policy”, TSE Working Papers 20-1076.

Deloitte (2018), ”Smart Home Consumer Survey 2018: Ausgewählte Ergebnisse für den deutschen Markt”, https://www2.deloitte.com/content/dam/ Deloitte/de/Documents/ technology-media-telecommunications/Deloitte_TMT_Smart_ Home_Studie_18.pdf.

DuckDuckGo Blog (2020), ”Search Preference Menus: No Auctions Please”, https://spreadprivacy.com/search-preference-menu-auctions/.

EDPS (2014), ”Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy”.

European Commission (2014), Case No COMP/M.7217 – Facebook/WhatsApp, 3 October.

European Commission (2016a), “Special Eurobarometer 447: Online Platforms”, June.

European Commission (2016b), “Flash Eurobarometer 443: e-Privacy”, December.

European Commission (2017a), Case AT.39740 – Google Search (Shopping), 27 June.

European Commission (2017b), ”Mergers: Commission Clears 21st Century Fox’s Proposed Acquisition of Sky under EU Merger Rules”, Press release.

European Commission (2018), Case AT.40099 – Google Android, 18 July.

European Commission (2019), Case AT.40411 – Google Search (AdSense), 20 March.

European Commission (2020a), “Digital Services Act package – ex ante regulatory instrument of very large online platforms acting as gatekeepers: open public consultation“.

European Commission (2020b), “Single Market – new complementary tool to strengthen competition enforcement: open public consultation”.

Expert Group for the Observatory on the Online Platform Economy (2020), “Progress Report Expert Group for the Observatory on the Online Platform Economy Work stream on Measurement & Economic Indicators”.

Facebook (2009), “Facebook Opens Governance of Service and Policy Process to Users”, 26 February, https://about.fb.com/news/2009/02/facebook-opens-governance-of-service-and-policy-process-to-users/.

Federal Court of Justice (2020), “Bundesgerichtshof bestätigt vorläufig den Vorwurf der missbräuchlichen Ausnutzung einer marktbeherrschenden Stellung durch Facebook“, press release, KVR 69/19, 23 June.

Furman, Jason, Diane Coyle, Amelia Fletcher, Philip Marsden and Derek McAuley (2019), “Unlocking digital competition”.

Gewerblicher Rechtsschutz und Urheberrecht: Internationaler Teil (GRUR Int) 2016, 639–647.

Graef, Inge, Damian Clifford, and Peggy Valcke (2018), "Fairness and Enforcement: Bridging Competition, Data Protection and Consumer Law", International Data Privacy Law 2018 8(3), 200–223.

Higher Regional Court Düsseldorf, Decision of the Higher Regional Court of Düsseldorf in interim proceedings, 26 August 2019, Case Vi-Kart 1/19 (V).

Jenkins, H. and A. Blankertz (2020), "Regulating e-commerce through competition rules: a fairness agenda?" in Gerard, Damien, Assimakis Komninos and Denis Waelbroeck (eds.), Fairness in EU Competition Policy: Significance and Implications. An Inquiry into the Soul and Spirit of Competition Enforcement in Europe, GCLC Annual Conference Series.

Kemp, K. (2020), "Every step you take: why Google's plan to buy Fitbit has the ACCC's pulse racing", The Conversation, 23 June.

Kerber, Wolfgang (2016), "Digital Markets, Data, and Privacy: Competition Law, Consumer Law, and Data Protection".

Kesler, Reinhold, Michael Kummer, and Patrick Schulte (2019), "Competition and Privacy in Online Markets: Evidence from the Mobile App Industry", ZEW Discussion Paper 19-064.

Krämer, Jan, Pierre Senellart, and Alexandre de Streel (2020), "Making data portability more effective for the digital economy", CERRE Report.

Kummer, Michael and Patrick Schulte (2016), "When Private Information Settles the Bill: Money and Privacy in Google's Market for Smartphone Applications", ZEW Discussion Paper 16-031.

Lardinois, Frederic (2020), "Google Wants to Phase Out Support for Third-Party Cookies in Chrome Within Two Years", https://techcrunch.com/2020/01/14/google-wants-to-phase-out-support-for-third-party-cookies-in-chrome-within-two-years/.

Lianos, Ioannis (2018), "Polycentric Competition Law", https://ssrn.com/abstract=3257296.

Litman-Navarro, Kevin (2019), "We Read 150 Privacy Policies. They Were an Incomprehensible Disaster", https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html.

Nouwens, Midas, Ilaria Liccardi, Michael Veale, David Karger and Lalana Kagal (2020), "Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence", To appear in the Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, April 25-30.

Ocello, Eleonora, Cristina Sjödin and Anatoly Subočs (2015), "What's Up with Merger Control in the Digital Sector? Lessons from the Facebook/WhatsApp EU merger case", , European Commission Competition merger brief.

OECD (2020), "Consumer Data Rights and Competition – Background note 2"; DAF/COMP(2020)1.

OECD (2018), "Personalised Pricing in the Digital Era. Background Note by the Secretariat", DAF/COMP(2018)13.

Office of Fair Trading (2013), "The economics of online personalised pricing", OFT 1488.

Olejnik, Lukasz, Minh-Dung Tran, and Claude Castelluccia (2014), "Selling Off Privacy at Auction", NDSS '14, 23-26 February 2014, San Diego, CA, USA.

Privacy International (2020), “The Google/Fitbit merger – NOT ON OUR WATCH!” https://www.privacyinternational.org/campaigns/googlefitbit-merger-not-our-watch.

Ramadorai, Tarun, Ansgar Walther, and Antoine Uettwiller (2019), ”The Market for Data Privacy“, CEPR DP13588.

Savage, S. J., and D. M. Waldman (2015), ”Privacy tradeoffs in smartphone applications“, Economics Letters 137, 171–175.

Shore J, Steinman J. (2015), “Did You Really Agree to That? The Evolution of Facebook’s Privacy Policy”, Technology Science.

Srinivasan, D. (2019), “The Antitrust Case Against Facebook: A Monopolist’s Journey Towards Pervasive Surveillance in Spite of Consumers’ Preference for Privacy”, Berkeley Business Law Journal.

Studienvereinigung Kartellrecht (2019), Stellungnahme der Studienvereinigung Kartellrecht zum Referentenentwurf 10. GWB-Novelle (GWB-Digitalisierungsgesetz) – Vorschriften über die Reform der Missbrauchsaufsicht und zum Thema Digitalisierung.

Tennison, Jeni (2020), “Community consent”, 17 January, https://www.jenitennison.com/2020/01/17/community-consent.html.

The Motley Fool (2018), ”Facebook, Inc. (FB) Q2 2018 Earnings Conference Call Transcript“, https://www.nasdaq.com/articles/facebook-inc-fb-q2-2018-earnings-conference-call-transcript-2018-07-25.

Townley, Christopher, Eric Morrison and Karen Yeung (2017), ”Big Data and Personalised Price Discrimination in EU Competition Law“, King’s College London Law School Research Paper 2017-38.

Wagner, Isabel and David Eckhoff. 2018. Technical Privacy Metrics: A Systematic Survey. ACM Comput. Surv. 51, 3, Article 57, July.

Winegar, Angela G. and Cass R. Sunstein (2019), “How much is data privacy worth? A preliminary investigation”, Journal of Consumer Policy.

Über die Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Die Stiftung Neue Verantwortung (SNV) ist ein gemeinnütziger Think Tank, der an der Schnittstelle von Technologie und Gesellschaft arbeitet. Die Kernmethode der SNV ist die kollaborative Entwicklung von Politikvorschlägen und -analysen. Die Expert:innen der SNV arbeiten nicht allein, sondern entwickeln und testen Ideen gemeinsam mit Vertreter:innen aus Politik und Verwaltung, Technologieunternehmen, Zivilgesellschaft und Wissenschaft. Unsere Expert:innen arbeiten unabhängig von Interessengruppen und Parteien. Unsere Unabhängigkeit gewährleisten wir durch eine Mischfinanzierung, zu der viele verschiedene Stiftungen, öffentliche Mittel und Unternehmensspenden beitragen.

Über die Autorin

Aline Blankertz leitet das Projekt „Datenökonomie“, das ökonomische, technische und gesellschaftliche Fragestellungen untersucht, um innovative datenpolitische Handlungsempfehlungen zu entwickeln. Vor der Stiftung Neue Verantwortung leitete Aline bei der wirtschaftswissenschaftlichen Beratung Oxera Analysen zur Plattformökonomie, Datenschutz, Algorithmen, Fairness in E-Commerce und Intermediärshaftung. Sie studierte an der Hochschule St. Gallen (Schweiz), Universidad Torcuato di Tella (Argentinien), University of Oxford (Großbritannien), WWU Münster und Chulalongkorn University (Thailand).

So erreichen Sie die Autorin

Aline Blankertz
Projektleiterin Datenökonomie
ablankertz@stiftung-nv.de
+49 (0)30 40 36 76 98 1

Imprint

Stiftung Neue Verantwortung e. V.
Beisheim Center
Berliner Freiheit 2
10785 Berlin

T: +49 (0) 30 81 45 03 78 80
F: +49 (0) 30 81 45 03 78 97

www.stiftung-nv.de
info@stiftung-nv.de

Design:
Make Studio
www.make-studio.net

Layout:
Jan Klöthe