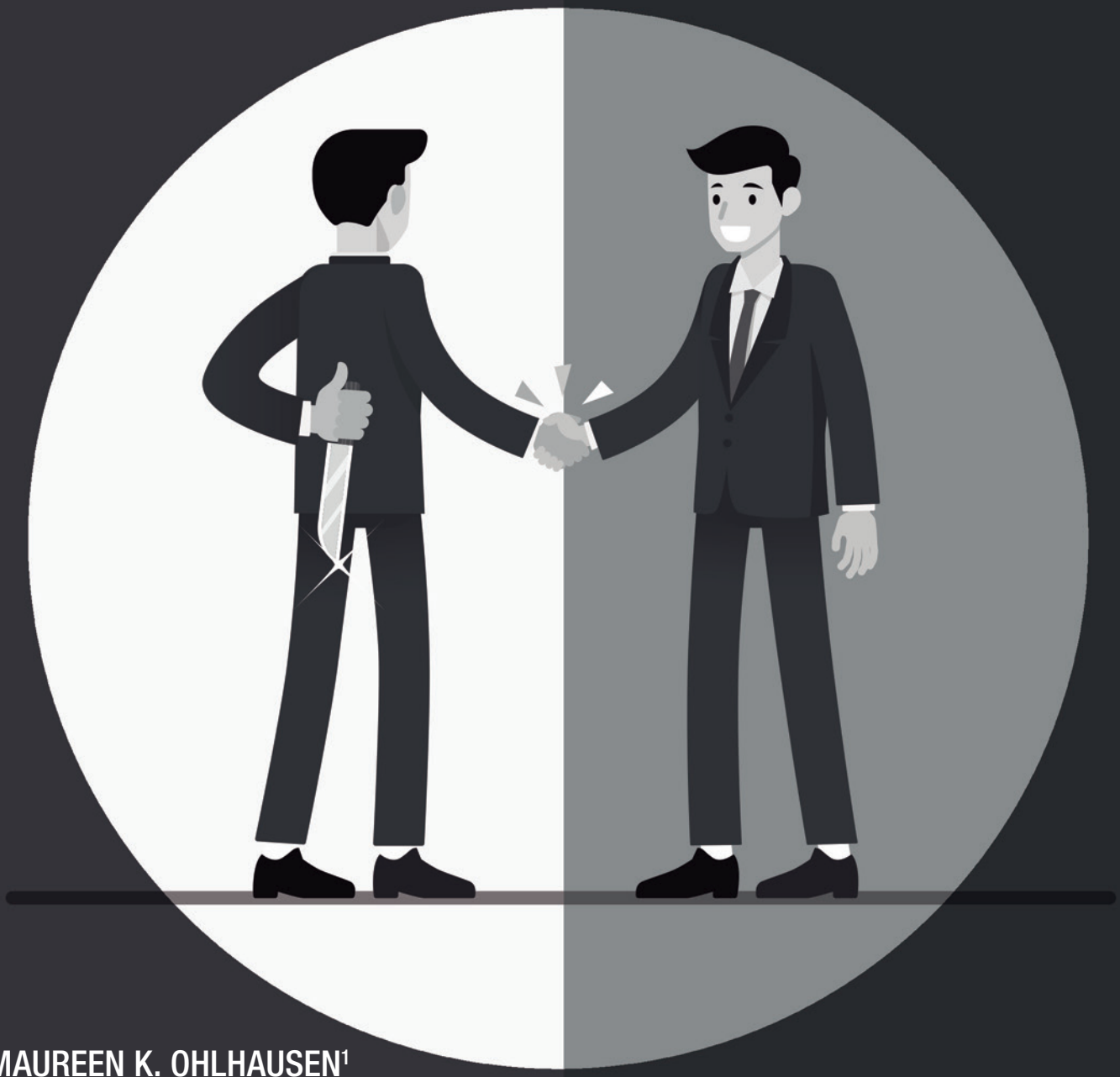
PRIVACY AND COMPETITION: FRIENDS, FOES, OR FRENEMIES?



BY MAUREEN K. OHLHAUSEN[1]

1 Partner, Baker Botts LLP. The author would like to thank Brian Jacobsmeyer for his research assistance.

I. INTRODUCTION

The debate about the future of data rich tech companies has reached a fever pitch in the European Union ("EU")[2] and, to a slightly lesser extent, the United States, with some voices calling for changes to consumer privacy law, competition law, or both to address perceived concerns. The desire to impose increased restrictions on data collection, usage, and sharing in the name of consumer privacy is manifest in Europe's adoption of the General Data Protection Regulation ("GDPR").[3] The regulatory impulse is not limited to changing consumer privacy law, however, and some have advocated using competition law to impose new controls and obligations on entities that collect consumer data. In fact, there has already been some melding of consumer privacy and competition concerns in data regulation itself. For instance, the GDPR mandates data portability to allow consumers to move their data among competing entities and thereby avoid "lock in" that may otherwise give current strong players an ongoing competitive advantage. Competition concerns reflect the fact that data about, or generated by, consumers can be a valuable asset. For example, The Economist magazine famously characterized data as the new oil.[4] Reflecting this view, some have called data an essential facility and have advocated using competition law to force big tech companies to share consumer data because of its utility as an asset today and as an essential input into new products and services tomorrow.

This article will explore the challenges and limits to these theories and the tension they create between reducing and widening access to consumer data. Can privacy and competition values live in harmony as friends, will some of these proposals make them enemies, or is it a bit of both?

II. GDPR, DATA BROKERS, AND DATA PORTABILITY

The GDPR, which took effect in May 2018, generally applies to companies processing the personal data of residents of the EU. The GDPR's definition of "personal data" is broad, covering any information that can directly or indirectly identify a person, such as a name, identification number, location data, or online identifier. The regulation also has a broad geographical sweep and applies to entities outside the EU that offer goods or services to EU citizens (regardless of whether payment is required) or monitor behavior that takes place within the EU.

2 See, e.g. a 2/1/19 tweet by Giovanni Butarelli, European Data Protection Supervisor, that said, "1865 President Lincoln abolished slavery. We now face the challenge of abolishing digital servitude – where people are mined for their data, and served back personalised information in order to induce behaviours that benefit a few powerful players #CPDP2019." Putting aside the question of the appropriateness of the comparison, the statement illustrates the intensity of European privacy regulators' sentiment about data.

3 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

4 "The World's Most Valuable Resource," The Economist (London, May 6, 2017).

The GDPR's fundamental requirements are that personal data be processed lawfully, fairly, and in a transparent manner. The regulation states that personal data may only be collected for specified, explicit, and legitimate purposes and not be further processed in a manner incompatible with those purposes. It also limits data collection to what is necessary for the purposes of processing. Personal data must also be accurate and kept up to date but retained for no longer than necessary. Companies must also ensure the integrity and confidentiality of the personal data they collect, including against unauthorized or unlawful processing and against accidental loss, destruction, or damage. The entity that controls personal data is responsible for, and must be able to demonstrate, compliance with the GDPR's requirements.

The GDPR further states that processing is lawful only under certain conditions, with a prime example being when the data subject has given consent freely and in a specific, informed, and unambiguous manner. For example, the request for consent must be in an intelligible and easily accessible form and use clear and plain language.[5] Moreover, the entity controlling the personal data must be able to demonstrate that consent, and individuals can withdraw consent at any time.

Consent is not required in all situations, however, such as in connection with performing a contract with a person. The GDPR also permits processing for the data controller's legitimate interests, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject. Legitimate interest is not based on a particular purpose, like performing a contract with the individual, and it could in principle permit processing for a wide variety of purposes. The GDPR does not provide a detailed list of legitimate interests, although it offers the examples of fraud prevention, network and information security, and public security. It also states that processing employee or client data, direct marketing, or administrative transfers within a group of companies may indicate a legitimate interest.

The GDPR does not explicitly address whether data brokers, who collect consumer data from a variety of sources and create profiles for a number of purposes, may fall under a legitimate interest exception. In 2014, the Federal Trade Commission issued a comprehensive report about the data broker industry ("Data Broker Report").[6] Based on an in-depth study of nine data brokers, it described how data brokers collect personal information about consumers from a wide range of commercial, government, and other public sources and provide it for a variety of purposes, including verifying an individual's identity, marketing products, and detecting fraud. While acknowledging risks to consumers, the Data Broker Report also identified several consumer benefits such as targeted marketing that allows consumers to find more easily goods and services that meet their needs. Importantly, the Report also concluded "consumers benefit from increased and innovative product offerings fueled by increased competition from small businesses that are able to connect with consumers they may not have otherwise been able to reach."

If the data broker model is prohibited outright or made impractical by the GDPR, this may reduce competition in some aspects. Entities that wish to target new customers or create new products but have not collected consumer data themselves may be disadvantaged if they cannot buy or otherwise access such data. Ironically, the GDPR may in this way actually help entrench the position of incumbents who have collected large amounts of consumer data.

The GDPR also grants consumers a number of explicit rights,[7] and, interestingly from the competition perspective, includes a right of data portability. Pursuant to this right, an individual must be able to receive his or her personal data from the data controller, in a structured, commonly used, and machine-readable format and transmit the data to another controller where the processing is based on consent and carried out by automated means. Although this right is clearly related to the GDPR's overall goal of giving people greater control over their data, as other commentators have explained, it also has the additional aspect of possibly enhancing competition by making switching easier and reducing the effects of lock-in.[8]

5 For example, on January 21, 2019, the French National Data Protection Commission ("CNIL") imposed a penalty of 50 million euros against Google LLC, under GDPR for lack of transparency, inadequate information, and lack of valid consent regarding their ad personalization. https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc.

6 Data Brokers: A Call for Transparency and Accountability, A Report of the Federal Trade Commission (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

7 The GDPR also grants individuals a number of rights, such as access, rectification, and erasure (often called the right to be forgotten).

8 See, e.g. Banda, Carolina, "Enforcing Data Portability in the Context of EU Competition Law and the GDPR," (September 13, 2017). MIPLC Master Thesis Series (2016/17), available at https://ssrn.com/abstract=3203289.

In sum, the GDPR's overall goal is to give consumers greater control over their data. It may enhance competition to the extent consumers take advantage of the right of data portability and where lock-in and switching costs have been barriers to competition. But, as the FTC concluded in its Data Broker Report, access to consumer data may be an important spur to competition. If the GDPR bars or greatly burdens this access, it may reduce competition.

The FTC Data Broker Report is just one example of the competitive importance of data, including data about or created by consumers. The next section will address how current antitrust law has treated data as an asset and where it has imposed data sharing as an antirust remedy.

III. DATA AS AN ASSET AND DATA SHARING UNDER CURRENT U.S. LAW

Specialized data related to personal information — think real estate records or credit data — have previously been subject to antitrust analysis. In today's online world, however, the debate in competition law circles centers around how to treat data about or created by consumers that is collected through online platforms and used by these entities to target ads, improve current offerings, and create new products. This type of consumer data is often an input for other products and services. For example, Waze (owned by Google) collects and aggregates the location and speed of travel of individual users' phones and uses it to produce dynamic trip directions based on changing traffic conditions. Consumer data is also a commodity asset for advertisers, allowing them to target their ads more precisely, which makes those ads more valuable and thus allows the platforms that hold such data to charge a higher price for that advertising space than other advertising channels.

Antitrust enforcers in the U.S. have experience with competitive issues involving data about or generated by consumers.[9] An example is the 2013 *Bazaarvoice* case, in which the DOJ successfully challenged a merger involving companies that provide software platforms for online ratings and reviews ("R&R") of products created by consumers that manufacturers and retailers host, share, distribute, and display. After a bench trial, the court found a relevant market for R&R platforms and that "syndication, switching costs, intellectual property/know how, and reputation are formidable barriers to new firms entering the market for R&R platforms."[10] The court also found persuasive the fact that both competitors referred to each other as duopolists in the R&R market and that Bazaarvoice would have a high market concentration after the acquisition, likely enabling it to charge monopolistic prices.

In *Bazaarvoice*, the court upheld the challenge to the combination of two platforms that used consumer-generated data because of a likely reduction in competition in the market for such platforms, and the DOJ required the defendant to divest the overlapping asset in a settlement. Other merger cases involving specialized data have allowed the merger to occur but required data sharing as a remedy. For example, in a series of mergers involving entities with databases of public real estate records used for title insurance underwriting (called title plants), the FTC has required the merging parties to sell a copy of their title plant.[11]

In another example of data sharing as an antirust remedy (albeit not involving consumer data), in 2015, the DOJ sued to block Cox Automotive's acquisition of Dealertrack. Cox Automotive is the owner of the AutoTrader and Kelley Blue Book brands. As part of its acquisition, Cox sought to purchase Dealertrack's inventory management solution business ("IMS") — a business unit devoted to providing analytics and algorithms to assist car dealers with the management of their vehicle inventory. DealerTrack also held ownership of valuable vehicle information data.

The DOJ was concerned that Cox would not only become an effective monopolist in the IMS market but also would acquire valuable vehicle information data that served as inputs to IMS businesses. With control over that data, Cox could "deny or restrict access" to the data "and thereby unilaterally undermine the competitive viability of Cox's remaining IMS competitors." To allow the deal to go through, the DOJ not only required Cox to divest the IMS portion of Dealertrack's business, it also required Cox to enable the continuing exchange of data and content between the websites it owns and the divested IMS business.

9 See, e.g. Ohlhausen & Okuliar, "Competition, Consumer Protection and the Right [Approach] to Privacy," 80 ALJ 121, 143-46 (listing antitrust cases involving data about or generated by consumers) (2015).

10 See *Bazaarvoice* Memorandum Opinion at p. 133.

11 See, Complaint, *Fidelity Nat'l Fin., Inc.*, FTC Dkt. No. C-4425 (Dec. 23, 2013), available at https://www.ftc.gov/system/files/documents/cases/140305fidelitcmpt.pdf; Complaint, *Fidelity Nat'l Fin., Inc.*, FTC Dkt. No. C-4300 (Sept. 16, 2010), available at http://www.ftc.gov/sites/default/files/documents/cases/2010/09/100916fidelitycmpt.pdf; Complaint, *Fidelity Nat'l Fin., Inc.*, FTC Dkt. No. C-3929 (Feb. 25, 2000), available at http://www.ftc.gov/sites/default/files/documents/cases/2000/02/fidelitycmp.pdf; Complaint, *Commonwealth Land Title Ins. Co.*, FTC Dkt. No. C-3835 (Nov. 12, 1998), available at http://www.ftc.gov/sites/default/files/documents/cases/1998/11/ftc.gov-9810127cmp.htm; Complaint, *LandAmerica Fin. Grp., Inc.*, FTC Dkt. No. C-3808 (May 27, 1998), available at http://www.ftc.gov/sites/default/files/documents/cases/1998/05/ftc.gov-9710115.cmp_.htm.

IV. DATA AS AN ESSENTIAL FACILITY

Some would like to take this sharing of data outside the realm of traditional remedies for competitive overlaps in mergers and require data rich companies to provide access to their data assets on the ground that it is simply necessary to compete. In a striking example, last year in Davos, George Soros attacked "giant IT companies" arguing, "[T]he fact that they are near-monopoly distributors makes them public utilities and should subject them to more stringent regulations, aimed at preserving competition, innovation, and fair and open universal access."[12]

In an interesting U.S. case, hiQ — a startup that scrapes data from LinkedIn, analyzes that data, and sells its analytics to businesses for workforce management purposes — sued LinkedIn under California competition law because LinkedIn had sent a cease and desist letter ordering hiQ to stop scraping its data in violation of LinkedIn's User Agreement, citing privacy concerns for LinkedIn users.[13] Notably, hiQ argues that "LinkedIn's conduct violates the 'essential facilities' doctrine, 'which precludes a monopolist or attempted monopolist from denying access to a facility it controls that is essential to its competitors.'"[14] The court granted a preliminary injunction against LinkedIn, finding that there was a reasonable likelihood of success that this claim would prevail on the merits.

The issue of whether companies who accumulate a large amount of consumer data should be required to share it on the basis that it is an essential facility also arose at the European Commission's recent conference on digital policy. In response to a question about whether companies who accumulate large data sets should be forced to share it, Professor Ariel Ezrachi responded that treating big data as an essential facility may be a "worthwhile remedy" to address alleged data monopolization by large tech companies.[15] He cautioned, however, that some information may be private and subject to the GDPR, thus making it different from a typical essential facilities analysis.

V. PRIVACY AND COMPETITION: A COMPLICATED RELATIONSHIP

The confluence of privacy and competition law creates numerous dilemmas. Sharing as a competition remedy has traditionally been invoked where data is difficult or expensive to create, raising an entry barrier that keeps out competitors who need access to such data. As discussed above, this has been imposed typically in a merger analysis, where two holders of such a data set want to combine. By contrast, the concern driving privacy law, like the GDPR, is that consumer data has become too widely available, with a perceived loss of consumer control. The remedy adopted for privacy concerns limits collection and restricts sharing of data, except at the consumer's direction. Arguments that consumer data should be treated as an essential facility are hard to square with evidence that data is abundant and available from many sources, as the FTC Data Broker Report showed. The GDPR, or similar laws, are likely to make consumer data harder to obtain and share. Evidence thus far suggests that the GDPR has reduced the collection of data but has also helped entrench some large online companies and hurt smaller players, possibly due to the cost of compliance with the law's complex requirements.[16] Using competition law to force sharing of consumer data as an essential facility, perhaps to mitigate this effect, would undercut the fundamental purpose of the privacy law.

A recent example of this complicated relationship is the German Bundeskartellamt's recent decision that Facebook abused a dominant position as a social network by combining into detailed profiles user data from its own website, its Instagram and Whatsapp services, and from third parties. Though not a data protection agency, the Bundeskartellamt asserted that Facebook violated the GDPR and thus engaged in an exploitative practice that hurt consumers, as well as competitors, who were not able to amass data in the same way. Their proposed remedy is to require Facebook to get consent from users before combining data in this way and to allow consumers to use the services in the same way, even if they do not consent. Whether this blended consumer protection and competition approach will withstand scrutiny or extend outside Germany is unclear, as Facebook has appealed and the head of DG Competition said the decision cannot serve as a template for EU action.[17]

12 Buzzfeed.news, "George Soros Just Launched a Scathing Attack on Google and Facebook," 1/25/18.

13 *hiQ Labs, Inc. v. LinkedIn Corp.*, 273 F. Supp. 3d 1099 (N.D. Cal. 2017).

14 *Id.* at 1117.

15 GCR, "Big data is not a typical essential facility, Ezrachi says," 1/17/19.

16 See, e.g. https://techcrunch.com/2018/10/09/gdpr-has-cut-ad-trackers-in-europe-but-helped-google-study-suggests/.

17 https://www.bloomberg.com/news/articles/2019-02-08/germany-s-facebook-order-will-be-studied-by-eu-vestager-says.

VI. CONCLUSION

Given the raging debate about the role of large tech platforms in our economy and their effects on consumer privacy, competition law and privacy law will continue to interact in complex and sometimes inconsistent ways. In deciding the appropriate relationship between the two, it is important to keep clearly in mind the values that undergird each area of law. Antitrust can take privacy and data, even consumer data, into account to the extent they are tied to a competitive impact, such as when a merger combines specialized data that is not otherwise reasonably available in the market. Invoking it to force data sharing outside these areas is not only unsupported in antitrust law, it may run counter to privacy protections. Privacy law pursues the important goal of helping individuals assert more control over personal data. It can also risk reducing competition, however, and these risks must be taken into account to ensure consumers' interests in both competition and privacy are respected.

CPI COMPETITION POLICY INTERNATIONAL

CPI Subscriptions

CPI reaches more than 20,000 readers in over 150 countries every day. Our online library houses over 23,000 papers, articles and interviews.

Visit competitionpolicyinternational.com today to see our available plans and join CPI's global community of antitrust experts.