Reframing Antitrust Law for Big Tech: Lessons from the German Bundeskartellamt

Brennan Weiss*

TABLE OF CONTENTS

* J.D., May 2021, The George Washington University Law School. Thank you Professor William E. Kovacic for inspiring this topic and providing advice throughout the early stages of this Note.

I. INTRODUCTION

Just weeks after news broke of one of the largest data leaks in the history of Facebook—resulting in a third party's use of millions of users' data without their permission—Mark Zuckerberg appeared before Congress in an attempt to mitigate the fallout.[1] But for two days, Zuckerberg played defense as members of Congress berated his leadership and, in particular, the social network's data privacy practices. At one point, Sen. Lindsay Graham (R-SC) zeroed in on Facebook's Terms of Service.

"When you sign up for Facebook, you sign up for Terms of Service . . . It says, 'The Terms govern your use of Facebook and the products, features, apps, services, technologies, and software we offer (the Facebook Products or Products), except where we expressly state that separate terms (and not these) apply.' I'm a lawyer [and] I have no idea what that means. But when you look at the Terms of Service, this is what you get."[2] Sen. Graham then held up a thick stack of papers fastened by an extra-large binder clip. "Do you think the average consumer understands what they're signing up for?" Zuckerberg replied: "I don't think that the average person likely reads that whole document."[3]

In another exchange, Rep. Kathy Castor (D-FL) shed light on the breadth of Facebook's data collection practices as reflected in its Data Policy, which is part of the Terms of Service. She addressed Zuckerberg specifically: "We understand the Facebook users that proactively sign in are part of that platform, but you're following Facebook users even after they log off . . . You are collecting data outside of Facebook. When someone goes to a website and it has the Facebook 'Like' or 'Share' [button], that data is being collected by Facebook, correct?"[4] Zuckerberg's affirmative response was a convenient lead into Rep. Castro's proposal. "Congress should act," she urged.[5] "I do not believe that [Facebook's] controls, the opaque consent agreement, [and] the settings are an adequate substitute for fundamental privacy protections for consumers."[6]

Congress berated Zuckerberg. Yet, in the more than two years since Zuckerberg's testimony, Facebook's Data Policy remains virtually

---

1. *Mark Zuckerberg Testimony: Senators Question Facebook's Commitment to Privacy*, N.Y. TIMES (April 10, 2018), https://www.nytimes.com/2018/04/10/us/politics/mark-zuckerberg-testimony.html [https://perma.cc/EX97-3SXB].

2. *Facebook, Social Media Privacy, and the Use and Abuse of Data: Hearing Before the S. Comm. on the Judiciary and the S. Comm. on Commerce, Sci., and Transp.*, 115th Cong. (2018) (statement by Sen. Lindsay Graham, Member, S. Comm. on the Judiciary), https://www.youtube.com/watch?v=qq6NfsWGNu0 [https://perma.cc/PVC3-ZGXV].

3. *Id.* (statement by Mark Zuckerberg, CEO, Facebook).

4. *Facebook, Transparency, and Use of Consumer Data: Hearing Before the H. Comm. on Energy and Com.*, 115th Cong. (2018) (statement by Rep. Kathy Castor, Member, H. Comm. on Energy and Com.), https://www.youtube.com/watch?v=WHszEcin5uE [https://perma.cc/T6ZR-5XVL] (0:43 - 1:40).

5. *Id.* at 3:55 - 4:09.

6. *Id.*

unchanged.[7] It is also unclear whether the average consumer has any better understanding of how Facebook's data collection works, despite the hearings and prolific news stories that followed. Put simply: Congress has failed to rein in Facebook's expansive data collection practices.[8]

***

Germany has a different approach to regulating Facebook. On February 6, 2019, Germany's Bundeskartellamt, or Federal Cartel Office (FCO)—the country's top antitrust enforcement authority—held that Facebook abused its market dominance by collecting user data not only on its platforms, but also on third-party websites and applications that have integrated Facebook Business Tools (such as the "Like" or "Share" functions) into their services.[9] The FCO ordered the social network to discontinue this practice.[10]

The FCO's novel legal argument against Facebook's Data Policy—based on an antitrust theory of illegal monopolization—is an especially appealing approach in jurisdictions without comprehensive federal data privacy protections like the United States. This is because it is likely that jurisdictions with data protection laws, if they are at all structured like

---

7. Data Policy, FACEBOOK, https://www.facebook.com/about/privacy/update (last visited Oct. 9, 2020) [https://perma.cc/6KM5-6SJF] [hereinafter *Data Policy*]. This policy still allows Facebook to collect data from third-party websites that use Facebook tools, such as the 'Like' and 'Share' functions ("These partners provide information about your activities off Facebook . . . whether or not you have a Facebook account or are logged into Facebook.").

8. *See generally* Cecilia Kang & Kevin Roose, *Zuckerberg Faces Hostile Congress as Calls for Regulation Mount*, N.Y. TIMES (April 11, 2018), https://www.nytimes.com/2018/04/11/business/zuckerberg-facebook-congress.html [https://perma.cc/4487-XS3B]. However, on December 9, 2020, the FTC sued Facebook under Section 2 of the Sherman Act and Section 5 of the FTC Act for allegedly monopolizing the personal social media market based on its acquisitions of Instagram and WhatsApp. FTC Compl. ¶ 174–75 (Dec. 9, 2020), https://www.ftc.gov/system/files/documents/cases/1910134fbcomplaint.pdf [https://perma.cc/LC6H-QW9P]. While this complaint is consistent with the spirit of this article, it does not address the core privacy concerns associated with Facebook's data collection practices that are the focus of this Note.

9. Press Release, Bundeskartellamt, Bundeskartellamt Prohibits Facebook from Combining User Data from Different Sources (Feb. 7, 2019), https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html?nn=3600108 [https://perma.cc/2JMT-EMTV] [hereinafter Bundeskartellamt Press Release].

10. Facebook appealed the decision to the Higher Regional Court (HRC) in Dusseldorf, which temporarily suspended the FCO's order, but did not rule on its merits, therefore allowing Facebook to ignore the FCO's demands for the time being. *See* Sara Germano, *Facebook Wins Appeal Against German Data-Collection Ban*, WALL ST. J. (Aug. 26, 2019, 5:04 PM), https://www.wsj.com/articles/facebook-wins-appeal-against-german-data-collection-ban-11566835967 [https://perma.cc/PBQ7-3W9M]. The FCO subsequently appealed the suspension to Germany's top court, the Federal Court of Justice (FCJ). On June 23, 2020, the FCJ lifted the suspension, paving the way for the FCO to temporarily enforce its order. *See German Legal Ruling Deals Facebook Blow in Data Use*, ASSOCIATED PRESS (June 23, 2020), https://apnews.com/58fc6fe8606d7e22bf3e8a06921f7a70 [https://perma.cc/X7B7-MJJA]. The main proceedings regarding the merits of the FCO's order remain pending before the HRC.

Europe's General Data Protection Regulation (GDPR), would use the force of such laws to crack down on expansive data collection practices.[11] However, in the United States, lack of a holistic federal data privacy law[12] makes it difficult for individuals to guard against take-it-or-leave-it data collection practices—to which the user must submit unless he withdraws from the service altogether—by powerful "data-opolies" like Facebook, Apple, Google, and Amazon.[13] Therefore, those in the U.S. seeking to challenge data collection practices by large technology companies must look to other areas of existing law that could serve as a basis for bringing suit.

This Note will argue that U.S. antitrust authorities, including the FTC and the Department of Justice (DOJ) Antitrust Division, should follow Germany's lead and aggressively pursue challenges against take-it-or-leave-it data collection practices by dominant technology companies like Facebook[14] based on an illegal monopolization theory of harm under Section 2 of the Sherman Act. Under Section 2, Facebook's Data Policy is anticompetitive because it impedes market entry by firms with potentially superior products and disincentivizes Facebook to innovate beyond what is necessary to maintain its existing users, thereby reducing the overall quality of its products and services. Part II will provide background on Facebook's Data Policy and describe the various sources from which Facebook collects data. Part III will highlight the antitrust legal framework in Germany, explain how the FCO applied that framework to Facebook, and then summarize relevant aspects of U.S. antitrust law. This section will also raise common criticisms of the use of antitrust law as a means to address privacy harms. Part IV will analyze the facts of the German case against Facebook in the context of U.S. antitrust law. This section will argue that the FCO's legal theory, albeit insufficient under Sherman Act Section 2, provides a framework upon which the FTC or DOJ could build by emphasizing how Facebook's Data Policy harms consumers by impeding market entry and reducing innovation and overall product quality. Such an illegal monopolization theory of harm would be successful under the burden-shifting framework established in

---

11. The GDPR came into effect in Europe in 2018. The landmark law sets strict limits on the kinds of data and the circumstances in which private entities can collect data from individuals.

12. Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN RELS. (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection [https://perma.cc/YU6L-GJLP].

13. "Data-opolies" is a relatively new term that refers to companies that dominate a particular platform such that they attract most of the users, sellers, advertisers, and software developers within that space. For example, Facebook is a "data-opoly" within the social networking sphere and Amazon is a "data-opoly" within the online merchant world. *See generally* Maurice E. Stucke, *Should We Be Concerned About Data-Opolies?* 2 GEO. L. TECH. REV. 275 (2018).

14. It is not this author's intention to vilify only Facebook when so many other large technology companies have equally troubling data collection practices. However, Facebook's Data Policy and its timely relevance as a result of the FCO's recent case against it in Germany make Facebook a useful case study to establish a broader framework for discouraging similar take-it-or-leave-it data privacy practices. The goal of this Note is to establish an antitrust framework that transcends the privacy challenges associated with Facebook and applies to any present or future data-collecting entity that dominates a particular domain.

Microsoft v. United States. This section will conclude with a policy discussion of the common criticisms addressed in Part III and argue that antitrust law should be used not as a placeholder for direct data privacy regulation, but rather as a means of challenging anticompetitive conduct that *results* in privacy harms.

II. FACEBOOK'S DATA POLICY

Facebook collects "the content, communications and other information you provide when you use our Products, including when you sign up for an account, create or share content, and message or communicate with others."[15] This seemingly innocuous statement obscures the true scope of its data collection. Facebook divides its data sources into three categories: (1) things users and others do and provide; (2) device information; and (3) information from partners.[16]

The first category—things users and others do and provide—is the most intuitive. It includes information gleaned from user activity on the mobile and desktop versions of Facebook (e.g. user interactions with other Facebook pages, accounts, and groups) and its "products," such as Messenger and Instagram.[17] The second category—device information—includes data from computers, phones, and other web-connected devices that consumers use when they are on Facebook.[18] It also includes information about the consumer's operating system, nearby Wi-Fi access points, device settings, IP addresses, and cookie data.[19]

The third category of data—information from partners—is the most controversial because it enables Facebook to collect information about consumers from sources outside its platform, including advertisers, app developers, and publishers (referred to as Facebook "partners") who use Facebook Business Tools.[20] Such tools include Application Programming Interfaces (APIs), Software Development Kits (SDKs), Facebook code, and the "Like" and "Share" social plugins.[21] For example, if a third party, completely unrelated to Facebook, embeds Facebook's "Like" function into its website, and you access that website, Facebook has the ability to collect information about "your device, websites you visit, purchases you make, the ads you see, and how you use their services—whether or not you have a

15. Data Policy, *supra* note 7.
16. *See id.*
17. *See id*; *What are Facebook Products?*, FACEBOOK, https://www.facebook.com/help/1561485474074139?ref=dp [https://perma.cc/9QPP-E7Z6].
18. *Id.*
19. *Id.*
20. *See* Bundeskartellamt [Federal Cartel Office] Feb. 6, 2019, B6-22/16, 1 (28:100), (Ger.) [hereinafter *Facebook*].
21. *The Facebook Business Tools*, FACEBOOK, https://www.facebook.com/help/331509497253087 [https://perma.cc/T3NR-5LMJ].

Facebook account or are logged into Facebook."[22] This means that Facebook's data collection extends far beyond what users provide on the platform and likely beyond what most users might reasonably expect or to which they might knowingly consent.

III. FACEBOOK IN GERMANY AND COMPETING MODELS OF ANTITRUST LAW

Discussion of potential antitrust implications of Facebook's data collection practices in the U.S. requires a baseline understanding of the current antitrust legal landscape. This section will describe German antitrust law's prohibition on dominance and abusive conduct. It also will explain that in finding against Facebook, the FCO relied primarily on evidence that Facebook's conduct resulted in anticompetitive effects that harmed Facebook's competitors. This section will then transition to discussing U.S. antitrust law and highlight provisions relevant to a potential claim against Facebook under the Sherman Act. And finally, this section will raise common criticisms of the use of antitrust law as a means to address privacy harms, which this Note will rebut at the end of its analysis.

A. German Antitrust Law and the Facebook Case

In Europe, the European Commission enforces antitrust rules pursuant to the Treaty on the Functioning of the European Union (TFEU).[23] Germany, as a member state of the EU, is subject to this treaty.[24] However, the TFEU applies only when a firm's conduct affects trade between EU member states.[25] The FCO has regulatory authority solely over domestic matters in Germany.[26] Therefore, this section will provide an overview of German, not European, antitrust law, including (1) a summary of Germany's antitrust legal framework; and (2) an explanation of how the FCO applied that legal framework to the Facebook case.

---

22. Data Policy, *supra* note 7. When a consumer clicks on a "Like" button that is embedded in a third-party website outside of Facebook.com, the "liked" content is automatically displayed on the Facebook platform so that the consumer's friends can see the content. A "share" button works in a similar way. When a consumer clicks a "share" button on a third-party website outside of Facebook.com, that content is automatically shared on the consumer's Facebook feed with his or her Facebook friends. *See* Facebook, *supra* note 20, at 18:56–57.

23. *Directorate-General for Competition*, EUR. COMM'N COMPETITION, https://ec.europa.eu/dgs/competition/index_en.htm (last visited Feb. 28, 2020) [https://perma.cc/UUF9-JLTA].

24. *Countries*, EUR. UNION, https://europa.eu/european-union/about-eu/countries_en (last visited Feb. 28, 2020) [https://perma.cc/U2HT-JVQE].

25. Consolidated Version of the Treaty on the Functioning of the European Union art. 101, Mar. 25, 1957, 2012 O.J. (C 326/01) 88.

26. *The Bundeskartellamt*, BUNDESKARTELLAMT, https://www.bundeskartellamt.de/EN/AboutUs/Bundeskartellamt/bundeskartellamt_node.html (last visited Feb. 29, 2020) [https://perma.cc/72HJ-RE8K].

1. German Legal Framework

German antitrust law is set out in the Act Against Restraints of Competition (ARC).[27] Chapter One of the ARC prohibits agreements restricting competition, such as price-fixing arrangements or other collusive agreements.[28] Chapter Two of the ARC prohibits less overt, but potentially just as harmful activity related to firms that attempt to monopolize the marketplace.[29] Chapter Two is more applicable in the FCO case because Facebook is charged with abusing its dominant position in the social network marketplace resulting from its own actions, as opposed to illegally colluding with another firm to fix prices or otherwise restrict competition, which would violate Chapter One.

Sections 18 and 19 under Chapter Two are at play in the FCO case. These provisions work together. Only when an undertaking is "dominant" under Section 18 and proceeds to abuse its dominant position by engaging in conduct prohibited under Section 19 will a firm violate German antitrust law.[30] Therefore, whether a violation occurs under Chapter Two of the ARC depends on the relationship between a firm's market dominance and its conduct.[31]

A firm is dominant under Section 18 "where, as a supplier or purchaser of a certain type of goods or commercial services on the relevant product and geographic market, it has no competitors, is not exposed to any substantial competition, or has a paramount market position in relation to its competitors."[32] Section 18 also lists five factors that are particularly relevant when a firm's business model involves a multi-sided network such as Facebook,[33] including (1) direct and indirect network effects; (2) parallel use of services from different providers and the switching costs for users; (3) economies of scale associated with network effects; (4) access to data; and (5) innovation-driven competitive pressure.[34]

There are several ways an undertaking may abuse its dominance, including impeding another undertaking in an unfair manner or demanding payment or other business terms which differ from those which would likely arise if effective competition existed.[35] However, sometimes a firm's

---

27. Gesetz gegen Wettbewerbsbeschränkungen [GWB] [German Act Against Restraints of Competition], Oct. 30, 2017, (Ger.). This Note refers to an English-translated version of the Act [hereinafter *ARC*]: https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Others/GWB.pdf?__blob=publicationFile&v=3.

28. *See id* § 1.

29. *See generally id. ch. 2.*

30. *See id.* §§ 18, 19.

31. *See Facebook*, *supra* note 20, at 245:873.

32. *ARC*, *supra* note 27, § 18(1).

33. Facebook is a multi-sided network because it provides separate but interrelated products and services to multiple groups of stakeholders, including users, advertisers, developers, and publishers. *See Facebook*, *supra* note 20, at 60–61:219; *see also* Ohio v. American Express Co., 138 S. Ct. 2274, 2280 (2018).

34. *ARC*, *supra* note 27, § 18(3a).

35. *Id.* § 19(2).

dominance may itself manifest abusive conduct.[36] It is therefore "sufficient [for a violation] if the conduct proves to be anti-competitive as a result of market dominance, which does not require strict causality but rather a causality in relation to the outcome."[37] The Facebook case is an example of how a firm's dominance in itself manifests abusive conduct.

2. The FCO's Application of German Antitrust Law to Facebook

The FCO enjoined Facebook's Data Policy on two grounds. First, the FCO argued that Facebook's Data Policy violated the GDPR because Facebook did not obtain voluntary consent from users for use of their personal data.[38] However, the GDPR provisions discussed in the German case and the extent to which the FCO relied on them in its decision against Facebook are not relevant here because there is no comparable data protection regulation in U.S. federal law.[39] Therefore, unlike the FCO, the FTC and DOJ could not support a potential antitrust claim on the basis of a violation of data protection requirements.[40]

Second, the FCO argued that Facebook possessed market power that gave rise to anticompetitive effects.[41] Essentially, the FCO determined that Facebook's high market power—and virtually limitless access to consumer data—made it near impossible for any other social network to compete effectively. The source of Facebook's market power, according to the FCO, was the social network's Data Policy, which combined data collected directly from its platform with data collected from third-party websites and applications.[42] The FCO supported its case for market power by arguing that

36. *See Facebook, supra* note 20, at 245:873.

37. *Id.*

38. *See id.*, at 166:573; *See also* Andreas Mundt Presentation: Implications of the German Facebook Decision 12 (April 17, 2019), https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Reden/L1/Andreas%20Mundt%20-%20%20Global%20Competition%20Law%20Centre.html [hereinafter Mundt Presentation]. Article 6 of the GDPR requires entities to obtain consent before processing user data. As the FCO explained, the take-it-or-leave-it nature of Facebook's Data Policy deprived users of such consent.

39. *See* O'Connor, *supra* note 12.

40. It is possible that the FTC could challenge Facebook's Data Policy under Section 5 of the FTC Act, 15 U.S.C. § 45, as an unfair or deceptive act or practice, but the plausibility of this theory is beyond the scope of this analysis.

41. *See* Mundt Presentation, *supra* note 38.

42. *See* Bundeskartellamt Press Release, *supra* note 9, at 2 ("The combination of data sources substantially contributed to the fact that Facebook was able to build a unique database for each individual user and thus to gain market power.").

Facebook had a 90% share of the social network market and that direct network effects[43] prevented users from switching to other services.

The FCO analyzed Facebook and its Data Policy under Sections 18 and 19 of the ARC.[44] Under Section 18, the FCO limited Facebook's geographic market to Germany and narrowly defined its product market to include as competitors only StudiVZ and Jappy—two German social networks—and the now defunct Google+.[45] The FCO also defined Facebook as a multi-sided network because it provides products and services to various stakeholders, including consumers, advertisers, developers, and publishers, thereby triggering the FCO's authority to assess Facebook's market position pursuant to the factors expressed in Section 18 related to multi-sided networks.[46] The FCO's narrow product and geographic market definitions, in addition to its characterization of Facebook as a multi-sided network, made it near certain that Facebook would be "dominant" under Section 18.

Next, the FCO argued that Facebook's Data Policy—specifically its collection of data from third-party websites and applications—constituted abusive business terms within the meaning of Section 19.[47] Essentially, the FCO argued that the Data Policy not only enabled Facebook to gain dominance under Section 18, but it also constituted abusive conduct under Section 19. Two factors weighed heavily against Facebook in both analyses: network effects and access to data.[48]

Direct network effects among private users lead to a more concentrated social network market.[49] This "self-reinforcing feedback loop" created a lock-in effect, meaning, users whose friends and family are also on Facebook are

43. Facebook, *supra* note 20, at 110–11; 186:646. *Direct* network effects occur when a product or service increases in value as more people join. For example, one of the reasons why so many people use Facebook is because their friends and family are also on Facebook. If an individual joins Facebook, but none of his friends or family do, he would likely find the service useless. On Facebook, *indirect* network effects occur between private users and advertisers because advertisers benefit the more users join the network. Indirect network effects also occur between app developers and private users because developers benefit by having a consistent flow of work to do the more users join. Users also benefit from the increased devotion of resources to app development. *See* D. Daniel Sokol & Roisin E. Comerford, *Antitrust and Regulating Big Data*, 23 GEO. MASON L. REV. 1129, 1148 (2016); *see also* Facebook, *supra* note 20, at 60:218.

44. This Note accepts the FCO's market definition and will apply it when analyzing the facts of the Facebook case under Sherman Act Section 2 in Part IV.B(1). An analysis of the purposes, functionalities, and qualities of each of more than two dozen potential competitors of Facebook is beyond the scope of this Note because it would detract from this Note's focus on the anticompetitive nature of expansive data collection practices by large technology firms.

45. Facebook, *supra* note 20, at 74:265. In total, the FCO considered 32 other websites and applications in determining the relevant market, excluding services such as LinkedIn, Snapchat, Twitter, FaceTime, and YouTube. *Id.* at 78–97.

46. *See id.* at 64–66.

47. *Id.* at 149:524.

48. *See id.* at 76:274. Although these factors are traditionally used only for the purpose of assessing dominance under Section 18, the FCO also discussed them in the context of abusive conduct because they enabled Facebook to effectively exclude and harm competitors and the social network marketplace. Put another way, Facebook's dominance on its own manifested abusive conduct. *See id.* at 250:888.

49. *See id.* at 119.

less likely to switch to other social networks.[50] When users have little incentive to switch services (such as to German social networks StudiVZ and Jappy because most users are already on Facebook) switching costs are considered high.[51] These high switching costs contribute to high barriers of entry for competitors because it is difficult for other social networks to reach the critical mass of users necessary for a functioning social network.[52] Therefore, in Facebook's case, direct network effects essentially limited "the range of potential competitors," especially those with more privacy-minded data collection practices.[53]

In addition, Facebook's access to data is superior to almost every other competitor.[54] It includes data collected from user activity that occurs directly on the social network, Facebook-owned products like Instagram, and third-party websites and applications that use Facebook Business Tools.[55] Data access matters in the context of market dominance because social networks are primarily data-driven products whose characteristics and financial sustainability depend, to a significant degree, on the user data available.[56] The more data Facebook collects, the better positioned it is to secure funding, develop its technology, and personalize its services for users.[57] Thus, according to the FCO, Facebook's wide-ranging data collection constitutes abusive conduct because it enables the social network to impede market entry.[58]

---

50. *Id.*

51. *See id*. at 132:464. Admittedly, the reality is that technology enables consumers to use multiple social media apps at once. Therefore, "switching" may not be as accurate an indicator of consumer preferences as it was in a pre-online social media era. Nevertheless, Facebook does not lose market power just because some consumers start using other social media apps. For example, let's assume that younger consumers generally prefer TikTok to Facebook as their form of social expression—and these consumers consist of two different groups. Group A consists of consumers who have both Facebook and TikTok. Group B consists of consumers who only have TikTok—including consumers who never had Facebook and consumers who deleted Facebook when they joined TikTok. For consumers in Group A, retention of Facebook, despite the addition of TikTok, suggests that they still find *unique value* in Facebook's services. Otherwise, why would they keep their account? Facebook may be the only way some of those consumers connect with older family members, for example. In this case, Facebook maintains its market power over these consumers. The same is true for consumers in Group B who don't have a Facebook account. After all, Facebook's Data Policy captures the data of these consumers if they use Facebook Business Tools on third-party websites. For both sets of consumers, Facebook's Data Policy enables the social network to reach consumer data in ways other products do not.

52. *See id.* at 133:467.

53. *Id.* at 82:293.

54. *See id.* at 142:498.

55. Data Policy, *supra* note 7.

56. *See* Facebook, *supra* note 20, at 136–37:482.

57. *See id.* at 138–39:488.

58. *See id.* at 141:494.

B. U.S. Antitrust Law: Illegal Monopolization Under the Sherman Act

The Sherman Act is the defining statute of U.S. antitrust law.[59] Section 1 of the Sherman Act prohibits collusive agreements in restraint of trade, whereas Section 2 prohibits actual or attempted monopolization.[60] Section 2 makes it unlawful for "every person who shall monopolize, or attempt to monopolize, or combine or conspire with any other person or persons, to monopolize any part of the trade or commerce. . . ."[61] Section 2 is applicable here because this Note proposes greater antitrust enforcement against monopolizing firms engaged in unilateral conduct, such as Facebook's unilateral enforcement of its invasive data collection practices, but does not comment on firms engaged in concerted activity in restraint of trade, which falls under Section 1.

Illegal monopolization under Section 2 has two elements: "(1) the possession of monopoly power in the relevant market and (2) the willful acquisition or maintenance of that power as distinguished from growth or development as a consequence of a superior product, business acumen, or historic accident."[62] Monopoly power (or dominance) alone under Section 2 does not constitute illegal monopolization.[63] Instead, a firm must possess monopoly power and also demonstrate anticompetitive conduct.[64] However, the Supreme Court famously remarked that antitrust law protects competition, not competitors.[65] Conduct that exclusively harms a particular firm's competitors is not cognizable.[66] Rather, anticompetitive conduct must harm the competitive process *and* consumers.[67]

One of the leading cases governing Section 2 jurisprudence is *United States v. Microsoft*, in which the DOJ alleged that Microsoft engaged in improper exclusionary conduct through its licensing and software developer agreements.[68] In *Microsoft*, the D.C. Circuit Court of Appeals outlined the burden-shifting steps in a Section 2 claim. First, the plaintiff must establish a prima facie case that the defendant possesses monopoly power that results in anticompetitive effects (i.e. exclusionary acts harming the competitive process and consumers).[69] Monopoly power is the ability to control prices or

---

59. Sara A. Solow, *Prosecuting Terrorists as Criminals and the Limits of Extraterritorial Jurisdiction*, 85 ST. JOHN'S L. REV. 1483, 1537 (2011).

60. *See* 15 U.S.C. §§ 1, 2.

61. 15 U.S.C. § 2.

62. United States v. Grinnell Corp., 384 U.S. 563, 570–71 (1966).

63. *See generally* U.S. Dep't of Justice, *Competition and Monopoly: Single-Firm Conduct Under Section 2 of the Sherman Act,* 19 (2008) [hereinafter *Competition and Monopoly*].

64. *See* Verizon Commc'ns Inc. v. Law Off. of Curtis V. Trinko, LLP, 540 U.S. 398, 407 (2004).

65. Brunswick Corp. v. Pueblo Bowl-O-Mat, Inc., 429 U.S. 477, 488 (1977) (internal citation and quotation marks omitted).

66. United States. v. Microsoft Corp., 253 F.3d 34, 58 (D.C. Cir. 2001).

67. *Id.*

68. *Id.* at 47.

69. *Id.* at 59.

exclude competition.[70] To determine whether monopoly power exists, it is necessary to first define the relevant product and geographic markets.[71]

Federal courts in the United States define the relevant product market by examining "products that have reasonable interchangeability for the purposes for which they are produced," including consideration of the price, use, and qualities of those products, as well as the firm's market share and general entry conditions.[72] The geographic market of the product at issue may encompass an entire country or a single region or city, but in any case it must reflect the commercial realities of the industry and the areas in which the business operates in an economically significant way.[73]

After the plaintiff establishes a prima facie case of monopoly power and anticompetitive effects, the second step under *Microsoft's* burden-shifting framework provides the defendant with an opportunity to offer procompetitive justifications for its behavior, such as greater efficiency or consumer appeal.[74] If the defendant does so, the burden then shifts back to the plaintiff to rebut those justifications.[75] However, if the plaintiff cannot rebut the defendant's procompetitive justifications, the plaintiff must show that the anticompetitive harm of the defendant's conduct substantially outweighs its procompetitive benefits.[76] This burden-shifting framework can be applied to Facebook in the context of a Sherman Act Section 2 claim of illegal monopolization. However, before launching into that analysis, it is first necessary to confront the criticisms of the use of antitrust law as a mechanism to remedy privacy harms as reflected in the ongoing antitrust-privacy policy debate.

C. Criticisms of Antitrust as a Mechanism to Address Privacy Harms

The oft-cited purpose of antitrust law is to protect competition, so on the surface, this makes antitrust law a curious mechanism for addressing privacy harms.[77] Critics of the use of antitrust law in the privacy domain often argue that the appropriate response to privacy concerns should not be antitrust enforcement, but rather greater privacy protections.[78] As one critic noted, "If elected officials believe that large Internet companies are not doing enough to protect privacy, the proper response is to enact national privacy regulation."[79] But one might think that the lack of a comprehensive federal privacy law in the United States along with Congress's perceived inability to pass bipartisan

70. United States v. E.I. Du Pont de Nemours & Co., 351 U.S. 377, 391 (1956).
71. *Competition and Monopoly*, *supra* note 63, at 26.
72. *Id.* at 21; *Du Pont*, 351 U.S. at 404.
73. Brown Shoe Co. v. United States, 370 U.S. 294, 336–37 (1962).
74. *Microsoft*, 253 F.3d at 59.
75. *Id.*
76. *See id.*
77. *See Brunswick*, 429 U.S. at 488.
78. Joe Kennedy, *Data and Privacy Are Not Antitrust Concerns*, INNOVATION FILES (Oct. 15, 2019), https://itif.org/publications/2019/10/15/data-and-privacy-are-not-antitrust-concerns [https://perma.cc/MBU6-DBFT].
79. *Id.*

legislation[80] demonstrate the need for an exception to the seemingly hard-and-fast rule that antitrust and privacy cannot mix. Nevertheless, critics maintain that antitrust law should only be used when there is harm to competition, not to fill gaps in privacy laws.[81]

Critics argue that antitrust may also be inappropriate to address privacy harms because although U.S. antitrust regulators have considered challenging data practices of large technology companies on antitrust theories of harm in the past, they ultimately declined to pursue such theories or concluded no violation.[81] For example, in their 2016 article assessing the application of antitrust to privacy harms, Daniel Sokol and Roisin Comerford point to the FTC's decision in 2007 to clear Google's merger with DoubleClick as evidence of regulators' reluctance to use antitrust to address privacy concerns.[82] In its statement concerning the proposed merger, the FTC argued that it lacked the legal authority to require conditions that do not relate to antitrust, and that regulating the privacy practices of one company could actually harm competition.[83]

Critics contend that court intervention into the data practices of specific companies may disincentivize innovation if firms are worried about violating antitrust laws. [84] As a consequence, companies may reduce investment in research and development, thus providing consumers with lower quality products and services.[85] Court intervention also raises administrative concerns because a firm's data policies and technological operations tend to be complex.[86] Even if a court deems a particular data practice illegal, it may simply lack the expertise and competence needed to apply the appropriate legal remedy.

In addition, critics argue that data collection may not actually restrict or harm competition because it is widely accessible, at very little cost, to virtually everyone.[87] The data that Facebook collects, for example, is not exclusive to Facebook. Users can, and often do, share the data they voluntarily provide to Facebook to other companies as well.[88] Therefore, critics argue that data does not implicate competition because "its use by one party does not diminish its value to anyone else."[89]

---

80. *See* O'Connor, *supra* note 12; *see generally Congress and the Public*, GALLUP, https://news.gallup.com/poll/1600/congress-public.aspx (last visited Oct. 9, 2020) [https://perma.cc/JR8W-ND5F] (demonstrating Congress's poor public approval ratings).

81 *See* Sokol & Comerford, *supra* note 43, at 1159.

81. *See id.* at 1151.

82. *Id.* at 1152.

83. Statement of the Federal Trade Commission, *Statement Concerning Google/DoubleClick*, FTC File No. 071-0170, at 2–3, Dec. 20, 2007, https://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf.

84. *See* Sokol & Comerford, *supra* note 43, at 1159.

85. *See id.*

86. *See id.* at 1159–60.

87. *See* Kennedy, *supra* note 78.

88. See *id.*

89. *Id.*

IV. FACEBOOK IN THE UNITED STATES: APPLYING THE GERMAN DECISION UNDER U.S. LAW

Having established the legal frameworks of illegal monopolization claims in Germany under the ARC and in the U.S. under Sherman Act Section 2, and having identified criticisms of the use of antitrust as a means to remedy data privacy harms, this section will (1) explain that the FCO's theory, albeit a strong foundation for a viable antitrust claim, falls short under Sherman Act Section 2 because the FCO failed to emphasize consumer harm; (2) describe how the FTC or DOJ should strengthen the FCO's theory of illegal monopolization and present a viable challenge against Facebook under Sherman Act Section 2; and (3) rebut criticisms of the use of antitrust to address privacy harms because they miscalculate the relationship between data collection, privacy, and competition, are outdated, and fail to factor in political considerations unique to the U.S.

A. The FCO's Legal Theory Fails Under the Sherman Act

The FCO's theory of abusive conduct would provide a strong foundation for challenging Facebook's Data Policy in the U.S. under the Sherman Act. In particular, the FCO's theory of market dominance would likely satisfy the monopoly power requirement under a Sherman Act Section 2 claim. However, the FCO's theory of abuse of dominance would likely fail under the Sherman Act because it does not sufficiently demonstrate how Facebook's Data Policy harms consumers. Therefore, the DOJ or FTC could not likely bring a successful Sherman Act Section 2 claim against Facebook without further developing the FCO's legal theory to address consumer harm.

The elements necessary to prove illegal monopolization under the German ARC are nearly identical to those under Sherman Act Section 2. Both require monopoly power and bad conduct, although the terms used to express each of those elements differ. For example, whereas Section 18 of the ARC refers to "market dominance," Section 2 of the Sherman Act refers to "monopoly power."[90] However, they are interchangeable because the factors courts consider in deciding whether either one exists—including substitutability, entry conditions, and market share—are roughly the same. Both require a market definition consisting of relevant product and geographic markets.[91] Under German law, courts determine the relevant product market—or the "market position" of the firm in question in relation to its competitors (as the ARC describes it)—by considering various factors.[92] One factor is "switching,"[93] which is synonymous with substitutability, a key component of the product market analysis under the Sherman Act.[94] The

90. *ARC*, *supra* note 27 at § 18; *Grinnell*, 384 U.S. at 570–71.

91. *See ARC*, *supra* note 27, at § 18(1); *see also Competition and Monopoly*, *supra* note 63, at 26.

92. *ARC, supra* note 27, at § 18(1).

93. *Id.* at § 18(3a) n.2.

94. *See Du Pont*, 351 U.S. at 404.

product market analysis under both the ARC and the Sherman Act also require consideration of entry conditions.[95]

Moreover, in the German case against Facebook, the FCO analyzed the purposes and functions of over a dozen potential competitors, including media such as Snapchat, Google+, Twitter, LinkedIn, Telegram, and YouTube, to determine whether users regard those companies as competitors of Facebook.[96] This analysis essentially mirrors the test for product substitutability under the Sherman Act established in *United States v. Du Pont*, which requires consideration of the "price, use and qualities" of products reasonably interchangeable by consumers.[97]

In addition, the FCO's consideration of Facebook's 90 percent market share[98] is also a relevant factor in a typical Sherman Act analysis. Therefore, based on the FCO's consideration of Facebook's substitutability, barriers to entry, and market share—the three main characteristics of a product market analysis under the Sherman Act—the FCO's theory of market dominance would satisfy the first element of an illegal monopolization claim under Sherman Act Section 2.

Because monopoly power alone is insufficient to constitute illegal monopolization under the Sherman Act, it is necessary to examine whether the FCO's theory of Facebook's abuse of dominance would satisfy the anticompetitive conduct element of an illegal monopolization claim under the Sherman Act. If so, both elements of Section 2—monopoly power and anticompetitive conduct—would be satisfied and the FCO's case against Facebook could constitute a viable antitrust claim in the U.S. However, the FCO's theory likely falls short of the Sherman Act's anticompetitive standard because it does not sufficiently emphasize how Facebook's Data Policy harms consumers.

Section 19 of the ARC prohibits "abuse of a dominant position" whereas Section 2 of the Sherman Act prohibits anticompetitive conduct. These prohibitions are synonymous because under the ARC, the FCO will only find that a firm abused its dominant position if it engages in anticompetitive conduct, such as impeding another firm in an unfair manner or demanding unfair business terms.[99] In its case against Facebook, the FCO argued that Facebook's Data Policy constituted abusive business terms by raising the barriers to entry into the social network market, thereby excluding competitors.[100] This theory, however, would be problematic under American law because it focuses almost exclusively on harm to competitors.

U.S. antitrust regulators typically require a showing of *consumer* harm. Under the Sherman Act, conduct is not anticompetitive solely because it excludes competitors.[101] It must also harm the competitive process and

95. *See ARC, supra* note 27, at § 18(3) n.5; *see also Competition and Monopoly*, *supra* note 63, at 21.

96. *See generally Facebook*, *supra* note 20, at 73–97.

97. *Du Pont*, 351 U.S. at 404.

98. *See Facebook, supra* note 20, at 110.

99. *ARC, supra* note 27, at § 19(2) nn.1, 2.

100. *Facebook*, *supra* note 20, at 149:524; 250:888.

101. *Microsoft*, 253 F.3d at 58.

consumers.[102] Therefore, although the FCO's theory would provide a strong foundation for challenging Facebook's Data Policy under the Sherman Act, the FTC and DOJ would have to better emphasize how the policy harms consumers.

B. A Revised Theory of Anticompetitive Harm Under Sherman Act Section 2

The FCO's theory of Facebook's market dominance and its subsequent finding that Facebook abused its dominance would be inadequate under Section 2 of the Sherman Act. However, a reworking of the FCO's theory, including greater emphasis on the harm that Facebook's Data Policy causes consumers, could lead to a successful challenge against Facebook in the U.S. This section will apply the burden-shifting framework established in *Microsoft* and argue, using the facts of the German case, that the FTC and DOJ could bring a successful claim against Facebook under Sherman Act Section 2.

1. The Government Could Make a Prima Facie Case of Facebook's Monopoly Power

Under the first step of the *Microsoft* burden-shifting framework, the FTC and DOJ would be able to satisfy the two elements of a Sherman Act Section 2 claim—first, that Facebook possesses monopoly power and second, that Facebook's willful acquisition or maintenance of that power is distinguished from growth or development as a consequence of a superior product, business acumen, or historic accident—thereby establishing a prima facie case of illegal monopolization.[103]

Proof of monopoly power depends on how the FTC and DOJ define the relevant product and geographic markets. Here, the relevant product market includes Google+, StudiVZ, and Jappy.[104] More popular websites and applications such as Snapchat, Twitter, LinkedIn, Telegram, and YouTube differ substantially in their use and qualities as compared to Facebook.[105] Therefore, consumers do not regard these other websites and applications as having "reasonable interchangeability for the purposes for which they are produced."[106]

Having established the relevant market, the case for Facebook's possession of monopoly power is strengthened by examining Facebook's share of the relevant market in addition to general entry conditions.[107] Within the defined market, Facebook's share of daily active users exceeds 90

102. *Id.*

103. *Grinnell*, 384 U.S. at 570–71; *see Microsoft*, 253 F.3d at 59.

104. *Facebook*, *supra* note 20, 74:265.

105. As explained in *supra* note 44, this Note accepts the FCO's market definition because such an analysis (which took the FCO years of investigation) would detract from this Note's focus on anticompetitive effects.

106. *Du Pont*, 351 U.S. at 404.

107. *Competition & Monopoly*, *supra* note 63, at 21.

percent.[108] This is well above the 70 percent minimum American courts generally require for Section 2 cases.[109] In addition, Facebook has the most daily active users of any social network in the world[110] and thus benefits from both direct and indirect network effects, which enable Facebook to employ wide-ranging data collection practices at the expense of potential competitors. Therefore, social networks seeking to enter the market are impeded because they simply may not be able to compete with the sheer amount of data that Facebook collects from its users. Having defined Facebook's relevant market by assessing the extent to which consumers regard Facebook as interchangeable with various other websites and applications and considering Facebook's 90 percent market share and difficult market entry conditions for nascent firms, the FTC and DOJ would likely be able to prove that Facebook possesses monopoly power.

2. The Government Could Make a Prima Facie Case of Anticompetitive Effects

The FTC and DOJ will also likely be able to show that Facebook has been able to maintain its monopoly power through anticompetitive means—by use of its invasive Data Policy—rather than as a consequence of its superior product, business acumen, or historic accident, thereby satisfying the second element under Section 2. Facebook's Data Policy effectively excludes competitors that might employ better privacy-protective measures by collecting so much data from consumers that it becomes difficult for other firms without such data to compete. This "locks-in" consumers who might otherwise consider switching to other social networks.[111] Furthermore, absence of a vigorous competitive environment disincentivizes innovation, thereby reducing overall product and service quality and harming consumers.

Facebook's Data Policy enables it to collect data not just from the information users voluntarily provide directly on the Facebook platform, but also from user activity on separate Facebook-owned products like Instagram, and on third-party websites and applications with embedded Facebook Business Tools.[112] Data that enables use of algorithms is perhaps the most important commodity in the social network market because it serves as the foundation of any social network's business model.[113] For example, data provides funding for Facebook through its advertisers, who are able to use data to target advertisements towards specific groups of people.[114] Data also provides Facebook's software developers with the flexibility necessary to

108. *Facebook*, *supra* note 20, at 110.

109. *See Competition & Monopoly*, *supra* note 63, at 21.

110. Dustin W. Stout, *Social Media Statistics 2020: Top Networks By the Numbers*, https://dustinstout.com/social-media-statistics/ (last visited Oct. 9, 2020) [https://perma.cc/87Z9-N9DN].

111. *See Facebook, supra* note 20, at 130:460.

112. *Data Policy*, *supra* note 7.

113. *Facebook*, *supra* note 20, at 136–37:482.

114. *See Ad Targeting*, FACEBOOK, https://www.facebook.com/business/ads/ad-targeting (last visited Oct. 9, 2020) [https://perma.cc/2GDK-EM77].

create better and more personalized technologies that in turn attract and satisfy more users.[115]

Such network effects enable Facebook to enforce its Data Policy with few, if any, repercussions because it has already reached the "critical mass" of users needed to establish a successful social network. Moreover, most users seeking Facebook-like services would find it inconvenient to delete their Facebook accounts.[116] The cycle of network effects harms competition because it doesn't give competitors who might otherwise succeed in the marketplace, especially those with more privacy-minded data collection policies, the chance to do so. Facebook already dominates the social network market and will likely continue to dominate it so long as its Data Policy remains in force. The Data Policy, therefore, impedes market entry.

Facebook's Data Policy is similar to the license agreements in *Microsoft* in that both effectively blocked consumer access to competitor products and increased the overall usage share of each company's respective product. In *Microsoft*, the DOJ sued the tech giant for imposing restrictive licensing agreements on manufacturers of computer operating systems, among other alleged exclusionary acts.[117] The D.C. Circuit held that the license agreements were restrictive, and consequently anticompetitive, because they required manufacturers to pre-install Microsoft's internet browser on operating systems in place of competitor browsers like Netscape.[118] This restriction effectively reduced the overall usage share of competitors' browsers, thereby preserving Microsoft's browser monopoly.[119]

Usage share matters for companies like Facebook and Microsoft because it correlates with direct network effects.[120] Direct network effects, in turn, determine in large part whether a product in the digital context fails or succeeds.[121] The more people use Microsoft's browser, the more data Microsoft will be able to collect about users' search queries, which will enable Microsoft to better adapt its browser to consumer tendencies and preferences. Indirect network effects were also important in *Microsoft* because the more people used Microsoft's browser, the more that browser attracted software developers who could write sophisticated code for applications that attracted even more users.[122] Therefore, just as Microsoft's restrictive licensing agreements prevented rival browsers from gaining the critical mass of users necessary to attract more users and software developers (thereby solidifying Microsoft's monopoly in the browser market), Facebook's Data Policy provides the social network with the data it needs to adapt its products and services just enough so that its existing users do not leave, thereby protecting Facebook's monopoly over social networks.

115. *See Facebook, supra* note 20, at 138–39:488.
116. *See id.* at 133:467.
117. *See Microsoft*, 253 F.3d at 47.
118. *Id.* at 60–61.
119. *Id.*
120. *See Facebook*, *supra* note 20, at 186–87:646.
121. *See id.* at 60:218.
122. *Microsoft*, 253 F.3d at 60.

The Data Policy also disincentivizes Facebook to innovate to attract new users or provide better quality products and services. Facebook can maintain its dominance in the marketplace simply by retaining its existing users. Therefore, its Data Policy is sufficient to collect the data necessary to improve its products and services for the purpose of maintaining its user share, but not for the purpose of offering better quality products and services to improve the social network marketplace in general. If Facebook had access to less data, it may not appeal as successfully to user tendencies and preferences, which might cause a substantial number of dissatisfied users to delete their accounts. Faced with the prospect of competitors attracting those dissatisfied users, Facebook would likely be incentivized to innovate and invest more in research and development.[123]

Facebook's Data Policy is also anticompetitive because it harms consumers. Direct network effects "lock in" consumers, which means that they generally do not find it useful to switch to an alternative network because they have already established many connections on Facebook.[124] It is likely that users will only switch products if they can convince their family and friends to do so as well, but this can be difficult.[125]

Facebook takes advantage of the "lock-in" effect by enforcing its Data Policy, essentially leaving consumers with no choice but to accept the terms of their data collection practices if they want to remain on a network where they can easily connect with most of their family and friends. Therefore, consumers are harmed by the exclusion of potential competitors of Facebook who, without the lock-in effect, might actually succeed in the marketplace by innovating in unique ways and providing better services. Such vigorous competition would benefit consumers. Yet potential competitors who do not have the critical mass of users necessary to trigger direct network effects (and therefore do not collect the amount of data needed to challenge Facebook's control of the market) are shut out of the marketplace, irrespective of their business acumen or the superiority of their products and services.

Here, the FTC or DOJ would likely meet its burden of establishing a prima facie case of anticompetitive effects. However, an additional harm to consumers is worth a mention, not to lend support to the anticompetitive

123. This is not to say that Facebook fails to innovate completely in response to the evolving social media landscape. In August 2020, for example, Facebook launched "Instagram Reels," a feature similar to TikTok. *See* Shannon Bond, *Facebook Launches Instagram Reels, Hoping to Lure TikTok Users*, NPR (Aug. 5, 2020), https://www.npr.org/2020/08/05/899319721/facebook-launches-reels-hoping-to-lure-tiktok-users [https://perma.cc/X4ME-ZAHZ]. Similarly, in 2016, Facebook added "stories" to Instagram that nearly mirrored Snapchat's prominent story feature. *See* Shannon Bond, *Instagram's New Stories Are a Near-Perfect Copycat of Snapchat Stories*, THE VERGE (Aug. 2, 2016), https://www.theverge.com/2016/8/2/12348354/instagram-stories-announced-snapchat-kevin-systrom-interview [https://perma.cc/BD98-GXA9]. These "innovations" suggest that Facebook may indeed face competition. However, Facebook arguably still offers a more comprehensive social media product than any other company, while other companies are left competing at the edges of service differentiation instead of taking on Facebook's main platform head-on.

124. *See Facebook, supra* note 20, at 131:462.

125. *Id.*

element of a Sherman Act Section 2 claim, but rather to demonstrate the kind of harm against which antitrust law can protect if anticompetitive conduct is framed in the right way. Facebook's collection of data from third-party websites and applications includes sensitive data, such as device-identifying information and location data.[126] As the FCO explained, this "makes it possible to identify users, ensuring they can be fully traced on the Internet, while the users concerned have virtually no control mechanisms."[127] Large data collections increase the risk of data leaks to third parties.[128] Even if the leaks are unintentional, they can cause serious harm in the form of identity theft, extortion, or fraud.[129]

In light of the fact that the FTC and DOJ have never used their antitrust authority to solely safeguard privacy, making such a case would be highly unpredictable, and likely unsuccessful, considering the DOJ only filed *one* monopolization case under Section 2 from 2000-2018.[130] Therefore, anticompetitive conduct, such as the imposition of Facebook's Data Policy, should be framed in traditional antitrust terms (i.e. exclusionary conduct that harms consumers by reducing Facebook's incentive to innovate, thereby reducing the quality of its products and services), rather than through revolutionary notions of antitrust harms that are uncertain to appeal to courts.

3. Facebook's Likely Procompetitive Justifications Fail

The second step under the *Microsoft* burden-shifting framework offers Facebook the opportunity to offer procompetitive justifications for its Data Policy.[131] Facebook argues that its Data Policy, including its collection of data from third-party websites and applications, makes it easier to "tailor each person's Facebook experience so it's unique to you."[132] It also argues that its Data Policy helps Facebook protect people's safety and security by disabling accounts tied to terrorism, child exploitation, and election interference.[133]

However, Facebook does not explain how a more limited data collection policy would interfere with its personalization operations.[134]

---

126. *Id.* at 237:838.

127. *Id.*

128. David Ingram, *Facebook Says Data Leak Hits 87 Million Users, Widening Privacy Scandal*, REUTERS (Apr. 4, 2018), https://www.reuters.com/article/us-facebook-privacy/facebook-says-data-leak-hits-87-million-users-widening-privacy-scandal-idUSKCN1HB2CM [https://perma.cc/QH58-NNKG].

129. *Facebook*, *supra* note 20, at 256:910.

130. *Antitrust Division Workload Statistics FY 2000-2009*, DOJ, https://www.justice.gov/sites/default/files/atr/legacy/2012/04/04/281484.pdf [https://perma.cc/P7EE-PNR9]; *Antitrust Division Workload Statistics FY 2009-2018*, DOJ, https://www.justice.gov/atr/file/788426/download [https://perma.cc/8J57-VJWW].

131. *See Microsoft*, 253 F.3d at 59.

132. Yvonne Cunnane & Nikhil Shanbhag, *Why We Disagree With the Bundeskartellamt*, FACEBOOK (Feb. 7, 2019), https://about.fb.com/news/2019/02/bundeskartellamt-order/ [https://perma.cc/96Y9-MA9N].

133. *Id.*

134. *See Facebook*, *supra* note 20, at 209:736.

Presumably, Facebook can tailor each person's experience based on the data it collects from user activity that occurs directly on the Facebook platform. It is not clear why Facebook will not be able to personalize user experiences without collecting data from Facebook-owned products like Instagram and third-party websites and applications with embedded Facebook Business Tools.[135] No evidence suggests that Facebook's Data Policy increases efficiency or improves Facebook's ability to appeal to consumers. Simply stating that is the case does not make it so. Therefore, the FTC and DOJ would be able to successfully rebut Facebook's first procompetitive justification.

The FTC and DOJ would also be able to successfully rebut Facebook's second procompetitive justification concerning improved safety and security. Facebook does not articulate how it is able to better detect and disable accounts tied to terrorism, child exploitation, and election interference as a result of its collection of data from Facebook-owned products and third-party websites and applications.[136] Would collecting data *only* from user activity on the Facebook platform harm Facebook's ability to track and remove dangerous accounts? If so, to what extent? Or would the effect of such a revised data policy be negligible? It is difficult to imagine how Facebook would even be able to measure any difference. Therefore, Facebook's second procompetitive justification would likely fail, and the FTC and DOJ would have a cognizable claim against Facebook's Data Policy under Sherman Act Section 2.

C. Why the Critics Are Wrong: Antitrust Should Be Used to Address Privacy Harms

The final hurdle in bringing an antitrust claim against Facebook's Data Policy involves the ongoing debate among policymakers and academics about the use of antitrust law to address privacy concerns. However, if antitrust is to be used at all against dominant technology companies like Facebook, claims under Section 2 of the Sherman Act are most likely to succeed in countering critics who believe that antitrust and privacy should not mix. Criticisms of the use of antitrust to address privacy harms do not pass muster for three main reasons. First, they miscalculate the relationship between data collection, privacy, and competition. Second, they are outdated because they fail to consider technology advancements that enable companies to collect more data. And finally, they fail to address U.S. political considerations.

Critics argue that antitrust law should only be used when there is harm to competition, not to fill gaps in privacy laws.[137] This is valid criticism. There are legitimate concerns about whether antitrust enforcement agencies have the authority to address privacy harms. Moreover, if the FTC and DOJ start using antitrust to remedy privacy harms, elected officials may become complacent and refrain from proposing significant federal privacy legislation if they think there are competent agencies already addressing privacy issues.

135. *See id.* at 212:743.
136. *See id.* at 214:750.
137. *See* Kennedy, *supra* note 78.

Therefore, critics are correct to the extent that antitrust law should not be used to crack down on conduct for the *purpose* of safeguarding privacy. However, antitrust law should be used more aggressively to challenge anticompetitive conduct that *results* in privacy harms. For example, Facebook engages in anticompetitive conduct by enforcing an invasive data policy that excludes competitors and harms consumers by limiting social network alternatives, disincentivizing Facebook to innovate beyond that which is necessary to retain its existing users and reducing the overall quality of its products and services.[138]

None of these harms directly involve privacy. However, if the DOJ or FTC bring a successful Sherman Act Section 2 claim against Facebook under the anticompetitive theory proposed here, an injunction or other similar court order would inevitably reduce privacy harms by restricting Facebook's Data Policy and limiting Facebook's access to user data. Therefore, critics overlook how the FTC or DOJ could address privacy harms by applying the traditional antitrust framework and maintaining focus on protecting competition. This Note simply proposes more aggressive use of the traditional framework to keep up with the many unprecedented privacy challenges we face today.

The notion that antitrust should not be used to address privacy harms simply because there is no relevant case law on the matter[139] is outdated and overlooks the extent to which technological capabilities have improved over the last couple of decades. Daniel Sokol's and Roisin Comerford's reference to the FTC's clearance of the Google/DoubleClick merger in 2007 as evidence that regulators would not want to bring an antitrust challenge against a future privacy harm neglects the realities of today's technology companies. In the last decade, computing power, network speed, data capture, storage capabilities, and internet bandwidth have improved dramatically.[140] These improvements have enabled sophisticated technology companies to collect more consumer data than ever before.[141] This reality calls for increased skepticism of corporate data collection and alternative theories for how to remedy associated privacy harms. To this end, antitrust law should be used more aggressively to address such privacy concerns.

Arguments concerning the difficulties of administering antitrust remedies for privacy harms are equally unconvincing. Judges hear cases all the time involving issues in which they lack expertise. *Microsoft*, for example, involved complicated facts about operating system browsers and other technological concepts, yet the D.C. Circuit managed to make sense of the facts and apply the law as it saw fit. Moreover, aggressive use of antitrust law would not require judges to learn the ins and outs of privacy law because privacy issues would not serve as a basis of any claim. As noted above, more aggressive use of antitrust law would not require the abandonment of the traditional antitrust framework. Therefore, arguments by the FTC and DOJ

138. *See supra* Part IV.B.2.

139. *See* Sokol & Comerford, *supra* note 43, at 1152.

140. NAT'L ACADS. OF SCIENCES, ENG'G, AND MED., INFO. TECH. AND THE U.S. WORKFORCE 34 (2017), https://www.nap.edu/read/24649/chapter/1.

141. *See id.* at 22–23.

would still focus on anticompetitive conduct. Privacy harms would not play any role in the parties' briefs or arguments before the court.

Finally, several political considerations in the U.S. support the notion that antitrust should be used more aggressively to address privacy concerns. Unlike Europe, the U.S. lacks a comprehensive federal privacy law.[142] This is unlikely to change anytime soon considering gridlock in Congress and the difficulty that comes with passing major bipartisan federal legislation.[143] Therefore, antitrust regulators can play a useful role in filling the void by more aggressively exercising their authority under Sherman Act Section 2 to challenge anticompetitive conduct that results in privacy harms to consumers.

There is substantial public support for greater enforcement.[144] For example, 40 percent of more than 1000 respondents in a May 2019 survey said they would support antitrust action against Facebook.[145] Moreover, only 22 percent of more than 2,000 respondents in an October 2018 survey said they trust Facebook with their personal data, including their browsing history, location data, contacts, and photos.[146] The public's frustration with Facebook and other large technology companies provides federal antitrust regulators with greater incentive to intervene.

V. CONCLUSION

In February 2019, Germany's FCO challenged Facebook's Data Policy on a novel antitrust theory of abuse of dominance, holding that its collection of data from user activity on the Facebook platform, other Facebook-owned products such as Instagram, and third-party websites and applications constituted abusive conduct. Although the FCO's theory would likely fail under U.S. antitrust law because of its inadequate emphasis on anticompetitive harm to consumers, the FTC and DOJ could still learn from the FCO's aggressive use of antitrust to remedy privacy harms. By reworking the FCO's theory to focus more on consumer harm, the FTC and DOJ could challenge Facebook's data collection practices under Sherman Act Section 2, thereby staying true to traditional antitrust goals of combatting anticompetitive conduct while also addressing related privacy harms.

Admittedly, antitrust law will not address all privacy harms. But then again, no one body of law, save perhaps comprehensive federal privacy legislation, will fully address all privacy concerns associated with the data collection practices of so many of today's largest technology companies. Regulators already have at their disposal the tools they need to protect

142. O'Connor, *supra* note 12.

143. *See* GALLUP, *supra* note 80.

144. Felix Richter, *American Public Supports Antitrust Action Against Facebook*, STATISTA (May 15, 2019), https://www.statista.com/chart/18024/public-support-for-antitrust-action-against-facebook/ [https://perma.cc/Q4GE-YD2K].

145. *See id.*

146. *How Much Do US Internet Users Trust Select Companies with Their Personal Data?* HARRIS POLL (Nov. 8, 2018), https://www.emarketer.com/chart/227523/how-much-do-us-internet-users-trust-select-companies-with-their-personal-data-of-respondents-oct-2018 [https://perma.cc/F3JZ-HZ7C].

consumers from invasive take-it-or-leave-it data collection practices. They should use them.