À LA RECHERCHE DU « DROIT » PERDU : DECONSTRUCTING AND DEFIBRILLATING ANTITRUST AND PRIVACY LAWS

Lily Leila PURQURIAN

Revue libre de Droit

ISSN 2276-5328

Article disponible en ligne à l'adresse suivante :

http://www.revue-libre-de-droit.fr

Comment citer cet article - *How to quote this article* :

L. L. PURQURIAN: « À La Recherche du « Droit » Perdu : Deconstructing and Defibrillating Antitrust and Privacy Laws », *Revue libre de Droit*, 2022, pp. 19-57.

À LA RECHERCHE DU « DROIT » PERDU : DECONSTRUCTING AND DEFIBRILLATING ANTITRUST AND PRIVACY LAWS

Lily Leila PURQURIAN[1]

Abstract: *Privacy implications have slowly trudged their way through legal analyses. Specifically with regard to antitrust enforcement, privacy made a slow but bona fide entry into the realm's consideration after many scholars mapped an intersection between the two bodies of law. Privacy harms could be seen as a "reduction in the quality of a good or service," and thereby reparable within antitrust.*[2] *Now, however, the world has discovered that some privacy harms have actually increased the quality of goods and services.*[3] *Facebook, Google, Apple, Microsoft, and Amazon profit primarily from culling data to then experiment on users through algorithms designed to predict consumer behavior. This then gives them an upper-hand in the market. Low to zero cost services exist not because the user is the customer, but the product.*

To that logical end, market prices under a strict consumer welfare standard would invoke the anticompetitive implications for third-party advertisers — the actual customers in this triangular relationship.

When it comes to data, antitrust enforcement is thus limited by the consumer welfare standard, or at least, the price theory that currently dominates interpretations of consumer welfare. Even if there is no space to reform antitrust law's standards for consumer welfare, which the neo-Brandeisian framework and current Congressional investigations would vehemently disagree with, the amount of data transferred via mergers and acquisitions is an enduring competition and privacy problem. Just as technology develops, the legal response must also develop. The

---

[1] Lily Leila Purqurian is a law student at the University of San Diego, primarily focusing on the international intersections between antitrust and privacy law, but also dipping into securities law. She holds degrees from Sciences Po and Boston University. She can be contacted at lpurqurian@gmail.com.

[2] Peter Swire, *Protecting Consumers: Privacy Matters in Antitrust Analysis*, CTR. FOR AM. PROGRESS (Oct. 19, 2007) https://www.americanprogress.org/issues/economy/news/2007/10/19/3564/protecting-consumers-privacy-matters-in-antitrust-analysis/. *See also* Frank A. Pasquale, *Privacy, Antitrust, and Power*, 20 GEORGE MASON LAW REVIEW 1009, 1010 (2013) ("The neoliberal account of "competition promoting privacy" only achieves surface plausibility by privileging the short-term "preferences" of consumers to avoid data sharing. The narrowness of "notice-and-consent" as a privacy model nicely matches the short-term economic models now dominating American antitrust law. The establishment in the field is largely unconcerned with too-big-to-fail banks, near monopoly in search advertising, media consolidation, and other forms of industrial concentration. By focusing myopically on efficiency gains that can be temporary or exaggerated, they gloss over the long-term pathologies of corporate concentration. So, too, does a notice-and-consent privacy regime privilege on-the-fly consumer judgments to "opt-in" to one-sided contracts over a reflective consideration of how data flows might be optimized for consumers' interests in the long run. As privacy declines and companies consolidate, mainstream antitrust and privacy theory often legitimates the process. Some scholarship can even amount to the "structural production of ignorance," characterizing scenarios as "consent" and "competition" when they are experienced by consumers and users as coercive and monopolistic.")

[3] This assertion is, of course, dependent on how 'harm' and 'quality' are subjectively defined. *See* Solove & Citron, *infra* note 115 and accompanying text to understand how that harm is discussed in the context of this Comment. *See also* Sections I and II.

FTC and DOJ thus must, at minimum, consider data as a potential indicator of market power in merger review. Otherwise, antitrust law will continue to neglect significant online privacy concerns, currently left to statutory rights and remedies, that are highly relevant to competition because they concern an invaluable asset driving the modern market: data.

This Comment addresses the dangers of the continued neglect for data as an indicator of market power. Namely, by placing the rights to and control of data acquired through mergers in the hands of a few. By looking at the European Commission's review of two particular mergers, the Facebook/WhatsApp merger and the Microsoft/LinkedIn merger, this Comment solidifies the relationship between privacy and antitrust. The immediate solution, then, is for the FTC and DOJ to consider data part of their merger analysis.

INTRODUCTION

Apple's latest update of Safari includes a 'Privacy Report.' There, intelligent tracking prevention is designed to " . . . use on-device machine learning to identify and blocks them from accessing identifying information."[4] When one visits the New York Times, for example, nineteen trackers are prevented from profiling the user.[5] Of them were Chartbeat, Amazon, Kantar Operations, Oracle, Google, DoubleVerify, comScore, Neustar, Media.net Advertising, and Criterio.[6] Some of these tracking "owners," like Google and Oracle, had different trackers, presumably obtaining different information.

Apple's update is the latest in an onslaught of privacy policy renovations that are best recognized as the 4,000-word emails immediately deleted from your inbox.[7] Safari's privacy report is sandwiched between the Favorites and Most Visited at the top of a user's homepage and Siri Suggestions and Reading List underneath. Of those four, only one — the Reading List — involves manual selection by the user. The rest are algorithmic predictions that process and store information about a user to then manipulate and profit off that user's behavior.[8]

---

[4] *Screenshot of Safari homepage*, Perma (data uploaded).

[5] Oracle is one of the largest sellers of personal data worldwide. *These are the Largest Data Brokers in America*, THE PRIVACY BLOG, https://privacybee.com/blog/these-are-the-largest-data-brokers-in-america/.
The European Union has recently brought suit against Oracle and Salesforce for their data collection practices. *See* Natasha Lomas, *Oracle and Salesforce Hit with GDPR Class Action Lawsuits Over Cookie Tracking Consent*, TECHCRUNCH (Aug. 14, 2020) https://techcrunch.com/2020/08/14/oracle-and-salesforce-hit-with-gdpr-class-action-lawsuits-over-cookie-tracking-consent/. A detailed investigation of Oracle would prove tremendously useful to any antitrust or privacy attorney, but until the lawsuit is public, information about the company's practices is shrouded. The data Oracle collects, however, is so useful that Facebook lists it as one of its partner categories who it licenses with for more precision in ad targeting. *See Improving Accountability and Updates for Facebook Targeting*, FACEBOOK https://www.facebook.com/business/m/one-sheeters/improving-accountability-and-updates-for-facebook-targeting *and* Kalev Leetaru, *The Data Brokers So Powerful Even Facebook Bought Their Data*, Forbes (Apr. 5, 2018), https://www.forbes.com/sites/kalevleetaru/2018/04/05/the-data-brokers-so-powerful-even-facebook-bought-their-data-but-they-got-me-wildly-wrong/?sh=27f478583107.

[6] It has become popular to hide trackers with apps like StatCounter or D. They are oftentimes apps themselves or Google Chrome extensions.

[7] *See* Charles Warzel & Ash Ngu, *Google's 4,000-Word Privacy Policy is a Secret History of the Internet.*, N.Y TIMES (July 10, 2019), https://www.nytimes.com/interactive/2019/07/10/opinion/google-privacy-policy.html.

[8] *See* Ravie Lakshmanan, *How Facebook and Google are Using Algorithms to Predict your Next Thought*, THE NEXT WEB (May 2, 2019), https://thenextweb.com/tech/2019/05/02/how-facebook-and-google-are-using-algorithms-to-predict-your-next-thought/; *see also* Olivia Goldhill, *An Algorithm Can Predict Human Behavior Better than Humans*, QUARTZ (Oct. 18, 2015), https://qz.com/527008/an-algorithm-can-predict-human-behavior-better-than-humans/.
Google, for example, indicates in its Privacy & Terms that it "uses the information shared by sites and apps to deliver [its] services, maintain and improve them, develop new services, measure the effectiveness of advertising, protect against fraud and abuse, and personalize content and ads you see on Google and on our partners' sites and apps." *See Privacy & Terms*, GOOGLE, https://policies.google.com/technologies/partner-sites?hl=en-US (last visited Jan. 22, 2021). Such an intentionally broad definition of Google's purpose when collecting and using this information inevitably involves massive privacy implications. *See infra* Sections II, III, and IV.
Relatedly, the FTC recently brought suit against Facebook for "illegally maintaining its social networking monopoly through a years-long course of anticompetitive conduct." *See* Press Release, Fed. Trade Comm'n, FTC Sues Facebook for Illegal Monopolization (Dec. 9, 2020) (on file with author), https://www.ftc.gov/news-events/press-

Ideally, the dangers of data collection would be minimal, because consumers would have options built upon competing thresholds for how much *better* privacy could get. Just as a car purchaser may choose one car over another for its better crash protection, so too might a web browser user choose Safari over Chrome because of the better privacy protections that involve control, consent, and cooperation with your data.[9] There would be strong competition between different privacy models, all in compliance with even stronger privacy regulatory frameworks, because a user would consider privacy infringement as dangerous and menacing to one's agency and quality of life as, say, crash protection.

Although the data is scant, market forces do not seem to be reliable in the production or enhancement of privacy safeguards.[10] For one, the operating system that is responsible for one's interaction with and knowledge of certain privacy protections generally comes in three colors:

releases/2020/12/ftc-sues-facebook-illegal-monopolization. The suit will probably contain significant relevations regarding how Facebook's behaviors impact privacy.

[9] Paying users for their data is gaining traction politically and socially. *See* Eduardo Porter, *Your Data is Crucial to a Robotic Age. Shouldn't You be Paid For It?*, N.Y. TIMES (Mar. 6, 2018), https://www.nytimes.com/2018/03/06/business/economy/user-data-pay.html; *see also* Laura Hautala, *California Wants Silicon Valley to Pay you a Data Dividend*, CNET (Feb. 25, 2019), https://www.cnet.com/news/california-wants-silicon-valley-to-pay-you-a-data-dividend/.

Even former presidential candidate, Andrew Yang, pushed for users to be paid for their data and made it part of his campaign message. *See* Makena Kelly, *Andrew Yang is Pushing Big Tech to Pay Users for their Data*, THE VERGE (June 22, 2020), https://www.theverge.com/2020/6/22/21298919/andrew-yang-big-tech-data-dividend-project-facebook-google-ubi.

For a further discussion of data as property, *see generally* Salome Viljoen, *Data as Property?*, PHENOMENAL WORLD (Oct. 16, 2020), https://phenomenalworld.org/analysis/data-as-property.

[10] They also may worsen competition. *See* Randal C. Picker, *Competition and Privacy in Web 2.0 and the Cloud*, 103 NW. U. L. REV. COLLOQUY 1, 11–12 (2008) ("An uneven playing field that allows one firm to use the information that it sees while blocking others from doing the same thing creates market power through limiting competition. We rarely want to do that. And privacy rules that limit how information can be used and shared across firms will artificially push towards greater consolidation, something that usually works against maintaining robust competition.").

Consumers, also, are not able to exercise their consideration for privacy because of the *lack* of choice. "Consumers are concerned about their privacy and don't like companies knowing their intimate secrets. But they feel powerless and are often resigned to the privacy invasions because they don't have any real choice. People need to own credit cards, carry cellphones, and have email addresses and social media accounts. That's what it takes to be a fully functioning human being in the early 21st century. This is why we need the government to step in." Should we be afraid? *See* Liz Mineo, *On Internet Privacy, Be Very Afraid*, HARV. L. TODAY (Aug. 25, 2017), https://today.law.harvard.edu/internet-privacy-afraid/.

Windows, Google Chrome, and MacOS.[11] Those three have significant market power.[12] The fear, then, is that monopoly power would follow.[13] Apple and Microsoft's market power, for example, gives them significant power that includes, but is not limited to, determining the extent to which one interacts with certain apps.[14] Ceding privacy, not bolstering it,[15] is what drives a company's decision to put an app, search engine, or web browser at the center of user feeds.[16]

---

[11] The DOJ recently brought suit against Google for violating antitrust laws in the search and search advertising markets. *See* Press Release, Dep't of Just., Justice Department Sues Monopolist Google for Violating Antitrust Laws (Oct. 20, 2020) (on file with author), https://www.justice.gov/opa/pr/justice-department-sues-monopolist-google-violating-antitrust-laws.

Epic Games also recently filed an antitrust suit against Apple alleging Apple has become the precise monopoly it once criticized IBM for being, and that George Orwell might have been right about 1984. *Sarah E. Needleman, Hearing in 'Fortnite'Maker's Apple Lawsuit Tests Antitrust Claims*, THE WALL ST. J. (Sept. 28, 2020, 4:55 PM). Albeit, this suit relates to the App Store and not Apple's operating system as a whole. Rather, each operating system dominates a particular arena in its own way, which may be behavior the market would like to encourage, anyway.

For a further discussion on the *Epic Games* lawsuit, *see infra* note 16.

[12] "[T]he ability of a firm—or a group of firms, acting jointly—to raise prices above the competitive level without losing so many sales so rapidly that the price increase is unprofitable and must be rescinded." William M. Landes & Richard A. Posner, *Market Power in Antitrust Cases*, 94 HARV. L. REV. 937, 937 (1981).

[13] Monopoly power is defined as "a high degree of market power." *Id.*

[14] This is tremendous power. When public radio was first introduced and became widespread in the 1920s, Congressman Luther A. Johnson of Texas spoke poignantly about the problem of concentration of control with such a medium. His words are worth quoting in full.

There is no agency so fraught with possibilities for service of good or evil to the American people as the radio. As a means of entertainment, education, information, and communication, it has limitless possibilities. The power of the press will not be comparable to that of broadcasting stations when the industry is fully developed. If the development continues as rapidly in the future as in the past, it will only be a few years before these broadcasting stations, if operated by chain stores will simultaneously reach an audience of over a half of our entire citizenship, and bring messages to the fireside of nearly ever home in America. They can mold and crystallize sentiment as no agency in the past has been able to do. If the strong arm of the law does not prevent monopoly owenership and make discrimination by such stations illegal, American thought and American politics will largely be at the mercy of those who operate these stations. *For publicity is the most powerful weapon that can be wielded in a Republic, and when such a weapon is placed in the hands of one, or a single selfish group is permitted to either tacitly or otherwise acquire ownership and dominate these broadcasting stations throughout the country, then woe be to those who dare to differ with them.* It will be impossible to compete with them in reaching the ears of the American people.

44 DECISIONS AND REPORTS OF THE FEDERAL COMMUNICATIONS COMMISSION OF THE UNITED STATES, PART 2, 2464–65.

[15] "Surveillance is the business model of the internet." Meneo, *supra* note 10.

[16] The Epic Games lawsuit against Apple arguably serves as one example. *See* Needleman, *supra* 11. Epic Games alleges that Apple's control over iPhones led Apple to assume control over the App Store. But the App Store, Epic Games contends, is an essential facility, so it must be shared with competitors or customers reasonably. Charging 30% for any revenue generated by any iPhone app during its first year, however, is not dealing with competitors or consumers reasonably. Epic Games inevitably proposes that Apple's App Store policies are anti-competitive and therefore, against the people's right to control commerce. "Spotify, Match Group, and Facebook" have all agreed with this characterization of Apple's App Store policies in public criticisms. *See Epic Games Says Apple Threatened to Cut it Out of the App Store Entirely*, CNBC (Aug. 17, 2020), https://www.cnbc.com/2020/08/17/epic-games-says-apple-threatened-to-revoke-developer-account.html.

Apple's control of the App Store has also led it to purportedly act for consumer privacy. *See* Chance Miller, *Apple Doubles Down on iOS 14 Tracking Privacy as Facebook Panics*, 9TO5 MAC (Aug. 11, 2020), https://9to5mac.com/2020/08/11/apple-ios-14-privacy-tracking-facebook/. Apple stopped allowing easy tracking of app installs in the latest iOS, thereby making it harder for ad companies to reach valuable user information regarding the success and usability of their apps. Now, iPhone users will see a pop-up warning them that a particular app will be tracking their data for advertising purposes, and will enable them to "block the app from doing so." *See* Megan Graham, *Apple's Seismic Change to the Mobile Ad Industry is Drawing Near, and it's Rocking the Ecosystem*, CNBC (Dec. 15, 2020), https://www.cnbc.com/2020/12/15/apples-seismic-change-to-the-mobile-ad-industry-draws-near.html.

There is much to be said about how data privacy is treated on both sides of the Atlantic: one treats it as an asset while the other treats it as a right.[17] And there is inequality where there are different philosophical foundations.[18] For the most part, however, the European Union's merger review process mirrors that of the United States.[19] Yet, the EU has neglected the same privacy concerns under its neoliberal antitrust framework that American antitrust regulators do under the Chicago School of Thought.[20] This suggests that the frameworks for both antitrust and privacy

---

The decision has already infuriated Facebook, who warns that "50% of its revenue" could be compromised and, in fact, protects Apple's *own targeted ad business*, which is the hidden exception to data tracking notifications. *See id*. On the other hand, a provider's decision on what to amplify on its services has tremendous sociopolitical implications. Parler, for example, was founded in 2018 as an alternative to Twitter, who begun implementing user policies that resulted in moderated and/or banned content. The platform quickly turned into the launchpad for conservatives, conspiracy theorists, and right-wing extremists. *See* Elizabeth Culliford and Katie Paul, *Unhappy with Twitter, Thousands of Saudis Join Pro-Trump Social Network Parler*, REUTERS (June 13, 2019), https://www.reuters.com/article/us-twitter-saudi-politics-idUSKCN1TE32S; *Parler 'Free Speech' App Tops Charts in Wake of Trump Defeat*, BBC NEWS (Nov. 9, 2020), https://www.bbc.com/news/technology-54873800; *Parler: Where the Mainstream Mingles with the Extreme*, ADL (Nov. 12, 2020), https://www.adl.org/blog/parler-where-the-mainstream-mingles-with-the-extreme; Isaac Saul, *This Twitter Alternative Was Supposed to be Nicer, But Bigots Love it Already*, FORWARD (July 18, 2019), https://forward.com/news/427705/parler-news-white-supremacist-islamophobia-laura-loomer/.

Parler re-entered the news cycle after it was discovered to be the primary service used to plan the storming of the U.S. Capitol on January 6, 2021. *See* Sheera Frenkel, *The Storming of Capitol Hill Was Organized on Social Media*, N.Y. TIMES (Jan. 6, 2021), https://www.nytimes.com/2021/01/06/us/politics/protesters-storm-capitol-hill-building.html. As a result, Google pulled Parler from the Google Play Store and Amazon suspended Parler from Amazon Web Services because its lack of moderation policies posed a public safety threat. *See* Jay Peters, *Google Pulls Parler from Play Store for Fostering Calls to Violence*, THE VERGE (Jan. 8, 2021), https://www.theverge.com/2021/1/8/22221648/google-suspends-bans-parler-play-store; John Paczkowski & Ryan Mac, *Amazon Will Suspend Hosting For Pro-Trump Social Network Parler*, BUZZFEED NEWS, (Jan. 9, 2021), https://www.buzzfeednews.com/article/johnpaczkowski/amazon-parler-aws.

Apple did not immediately suspend Parler. Instead, Apple gave Parler 24 hours to submit a moderation improvement plan. Still, Parler is unloading a repository of antitrust suits against the tech giants. *See* Leah Nylen, *Parler Hits Amazon with Antitrust Suit over Shutdown*, POLITICO (Jan. 11, 2021), https://www.politico.com/news/2021/01/11/parler-amazon-antitrust-suit-457579.

This is all to say that the old adage rings true: with great [market] power comes great responsibility.

[17] For a general discussion of the differences between EU and US treatment of digital privacy, *see* Filippio Lancieri, *Digital Protectionism? Antitrust, Data Protection and the EU/US Transatlantic Rift*, 7 J. ANTITRUST ENF'T (2018).

[18] *See id.* Because the EU enshrined data protection and privacy as a human right, the subsequent General Data Protection Regulation (GDPR) followed a consent-model much stronger in its consumer protections than the United States's strongest competing privacy regulation: the California Consumer Privacy Act (CCPA). *See infra* Sections III and IV.

[19] Although there are foundational differences, *see*, *e.g.* 6 Makan Delrahim, Assistant Attorney Gen., Dep't of Just., Good Times, Bad Times, Trust Will Take Us Far: Competition Enforcement and the Relationship Between Washington and Brussels (Feb. 21, 2018), https://www.justice.gov/opa/speech/assistantattorney-general-makan-delrahim-delivers-remarks-college-europe-brussels ("[e]uropean competition law still imposes a 'special duty' on dominant market players, while we in the U.S. do not believe any such duty exists"), the reviews are subject to similar legal standards.

[20] *See infra* Sections V and VI on the Microsoft/LinkedIn merger and Facebook/WhatsApp merger.

Since the Chicago school revolutionized the direction to and of antitrust law, the consumer welfare standard has governed most judicial interpretation of anti-competitive behavior. *See generally* ROBERT H. BORK, THE ANTITRUST PARADOX: A POLICY AT WAR WITH ITSELF (1978). The implications of this philosophy were not lost on criticism. *See* Lina Khan *infra* note 25. Khan argues the Chicago School revolution shaped the predatory pricing doctrine such that predatory pricing was deemed "almost always irrational, and so is unlikely actually to occur," even though, right now, Amazon has become a titan through precisely that. *See id.* at n. 82.

The revolution also informed the consumer welfare standard, which Khan argues "fails to capture the architecture of market power in the twenty-first century marketplace." *Id.* at 716. Because, for example, the "potential harms to

regulation are at issue, and that, without defibrillating the frameworks to adjust and respond to current market conditions, both antitrust and privacy regulation will be stuck in a loop.[21]

One could imagine why current legal frameworks under neoclassical economic models may be as obsolete as the original iPhone. The apps that we use the most – and the apps that, in turn, use us the most[22] – are rarely offered at a dollar amount.[23] Neither the app services nor the goods provided therein are valued at their dollar cost, and instead, provide free to low-cost services.[24]

---

competition posed by Amazon's dominance are not cognizable if we assess competition primarily through price and output. Focusing on these metrics instead blinds us to the potential hazards." *Id.* at 716-17.

But before that criticism could even occur, the evolution of technology rendered an already impotent philosophy even more vulnerable. Suddenly, low consumer prices were not a reliable metric of how the market is doing or whether there is space fertile for competition. *Id*. This gave rise to what is now dubbed the neo-Brandeisian movement, aiming to honor and defibrillate the philosophy of Justice Louis Brandeis. While the movement does not have a clear manifesto – and has been criticized for such – its aims are not difficult to gauge. *See, e.g.*, Daniel A. Crane, *How Much Brandeis do the Neo-Brandeisians Want?*, THE ANTITRUST BULL. (Nov. 8, 2019), https://econ.utah.edu/antitrust-conference/session_material/Anitrust%20Bulletin%20Article%202019.pdf.

Justice Brandeis was one of the most critical figures at a time when oligarchs like J.P. Morgan were lobbying and gambling their way through Washington. He predicted the crash of 1929 and heavily criticized any form of corporate 'bigness.' *See generally* LOUIS D. BRANDEIS, CURSE OF BIGNESS (1914). Coincidentally, apart from his work in antitrust and criticism of big government, he is most lauded for his defense of privacy. *See* LOUIS D. BRANDEIS & SAMUEL D. WARREN, THE RIGHT TO PRIVACY (1890). Neo-Brandeisians follow suit. The market structure, to neo-Brandeisians, is "deeply political" by setting policy, regulating markets, taxing, and asserting dominance. *See* Zephyr Teachout & Lina Khan, *Market Structure and Political Law: A Taxonomy of Power*, 9 DUKE J. OF CONST. L. & PUB. POL'Y 37-74 (2014).

These are, of course, ideological assertions that some would argue are inconsistent with the empirical work done by public choice scholars. To neo-Brandeisians, however, the answer to strongholds of market power and monopolies is to "design a system of public regulation that prevents the executives who manage [a monopoly] from exploiting their power." Lina Khan, *The New Brandeis Movement: America's Antimonopoly Debate*, 9 J. EUR. COMPETITION L. & PRAC. 131 (2018). And with that, to "ensure that executives face the right incentives to provide the best service possible to everyone who relies on the monopoly to sell or to buy a particular product or service." *Id*. This anti-monopoly stance then divorces itself from any potential social goal, hoping to instead focus on structures and a "broader set of measures" to assess market power. *Id*. For a criticism of this philosophy, *see* Daniel A. Crane, *How Much Brandeis Do the Neo-Brandeisians Want?*, 64 ANTITRUST BULL. 531 (2019).

[21] *See generally* Urs Gasser, *Recoding Privacy Law: Reflections on the Future Relationship Among Law, Technology, and Privacy*, 130 HARV. L. REV. F. 61 (2016).

For a further discussion on the Chicago School of Thought, *see* Joe S. Bain, Workable Competition in Oligopoly: Theoretical Considerations and Some Empirical Evidence, 40 AM. ECON. REV. 35, 36-38 (1950); Marc Allen Eisner, ANTITRUST AND THE TRIUMPH OF ECONOMICS: INSTITUTIONS, EXPERTISE, AND POLICY Change 107 (1991); Richard A. Posner, The Chicago School of Antitrust Analysis, 127 U. PA. L. REV. 925, 932 (1979); *and* Raghuram Rajan & Luigi Zingales, SAVING CAPITALISM FROM THE CAPITALISTS (2003).

[22] Omri Wallach, *How Big Tech Makes their Billions*, VISUAL CAPITALIST (July 6, 2020), https://www.visualcapitalist.com/how-big-tech-makes-their-billions-2020/; *They Made How Much?*, N.Y. TIMES (July 31, 2020), https://www.nytimes.com/2020/07/31/business/dealbook/tech-earnings-economy.html

[23] Barry C. Lynn, *The Big Tech Extortion Racket*, HARPER'S MAG., Sept. 2009, https://harpers.org/archive/2020/09/the-big-tech-extortion-racket/.

[24] Google, Instagram, and Facebook are all free to use, posing serious inquiries (at best) regarding what the real expense is. *See infra* Section IV. Amazon's record low costs, too, have left booksellers, authors, and publishers desperate for antitrust regulation. *See* Joint Letter to Chairman David Cicilline from the Association of American Publishers, The Authors Guild, and American Booksellers Association (Aug. 17, 2020), *available at* https://lunch.publishersmarketplace.com/wp-content/uploads/2020/08/Joint-Letter-to-Chairman-Cicilline-081520-Advance-Copy.pdf. They allege that Amazon's market power, which enables it to maintain those record low costs, stems not only from Amazon's share of the market for book distribution, but also from the astonishing *level of data* that it collects across its entire platform. Amazon tracks and uses data that provides it with an incredible amount of information about individuals and how to target them, such as: what their interests are; what products or books they have bought or pre-ordered; from whom; at what price point; what they have perused or considered purchasing; what

This makes the prospect of predatory pricing and data-opolies not just near, but also, highly rational.[25]

Big tech has been fined and monitored for some of its anticompetitive conduct. The European Commission fined Google €2.42 billion for favoring its merchant partners in its search results.[26] The Commission also fined Facebook €110 million for "providing incorrect or misleading information" during the Commission's review of the proposed acquisition of WhatsApp by Facebook.[27] Although not a fine, when Apple paid "substantially less tax than other businesses," in the form of €13 billion, there was such distorted competition that the Commission stayed on watch in Apple's proposed acquisition of Shazam.[28] Amazon, in addition to receiving tax benefits

video-games they are playing; and what television shows or movies they are watching. The result is that Amazon no longer competes on a level playing field when it comes to book distribution, but, rather, owns and manipulates the playing field, leveraging practices from across its platform that appear to be well outside of fair and transparent competition.

Id. Amazon's control does not end there. Nor do its coercive tactics. In late 2020, Amazon announced its intention to launch Amazon Pharmacy, a new service offering home delivery for prescription medication. Joe Pompliano (@JoePompliano), TWITTER (Nov. 17, 2020, 4:47 AM), https://twitter.com/joepompliano/status/1328681174278033408. Immediately after the announcement, CVS's stock dropped nearly 10%, despite CVS preparing to be a lead distributor in the COVID-19 vaccine. *See* Jesse Pound, *Walgreens Drops 9% to Lead Drug Store Stocks Lower After Amazon Launches Pharmacy Business*, CNBC (Nov. 17, 2020), https://www.cnbc.com/2020/11/17/walgreens-drops-11percent-to-lead-drug-store-stocks-lower-after-amazon-launches-pharmacy-business.html. With Amazon Pharmacy, Amazon inevitably plans to tie lower drug prices to its Amazon Prime Membership, unlocking new definitions of market power.

[25] *See generally* Lina M. Khan, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710 (2017) (arguing Amazon became a titan through predatory pricing — the practice of keeping prices low to pursue growth). Current antitrust frameworks, Lina Khan argues, cannot respond to the anticompetitive harms of companies like Amazon because of the consumer welfare standard. *Id*.

[26] Case AT.39740, Google Search (Shopping), 2017 E.C. 1/2003, http://ec.europa.eu/competition/antitrust/cases/dec_docs/39740/39740_14996_3.pdf. Arguably, Google's dominance in search engines is closely related to its acquisition of DoubleClick, a company that developed and provided Internet ad serving services. *See* Louise Story & Miguel Helft, *Google Buys DoubleClick for $ 3.1 Billion*, N.Y. TIMES (Apr. 14, 2007), https://www.nytimes.com/2007/04/14/technology/14DoubleClick.html *and* Tony Yiu, *Why Did Google Buy DoubleClick?*, Towards Data Science, (May 5, 2020), https://towardsdatascience.com/why-did-google-buy-doubleclick-22e706e1fb07.

[27] European Commission Press Release IP/17/1369, Mergers: Commission Fines Facebook €110 million for Providing Misleading Information about WhatsApp Takeover (May 18, 2017), http://europa.eu/rapid/press-release_IP-17-1369_en.htm.

[28] European Commission Press Release IP/16/2923, State Aid: Ireland Gave Illegal Tax Benefits to Apple Worth up to €13 Billion (Aug. 30, 2016), http://europa.eu/rapid/pressrelease_IP-16-2923_en.htm.

to the tune of €250 million in Luxembourg,[29] also was on the Commission's watch for its most favored nation clause.[30] The same is true for Big Telecom.[31]

Yet, none of these fines seem to have deterred what they intended to and the efforts are, rather, cyclical. The five biggest companies by market value — Apple, Amazon, Alphabet, Microsoft, and Facebook — have shown that they are behemoths who are not only unafraid of regulation, but also wield enough power to dodge it altogether.[32] Privacy, an inherently non-partisan issue,[33] now dons a cloak of controversy because the companies that have escaped stricter antitrust regulations assume control over massive amounts of data, and, in most cases, *depend* on that data for their revenue.[34]

This Comment will argue that privacy and antitrust regulation in the form of merger reviews go hand in hand. While there is significant scholarship arguing the extent to which this is feasible or even imaginable, there is little contending that, without a reimagining of our approaches to *both*

[29] European Commission Press Release IP/17/3701, State Aid: Commission Finds Luxemburg Gave Illegal Tax Benefits to Amazon Worth Around €250 Million (Oct. 4, 2017), http://europa.eu/rapid/press-release_IP-17-3701_en.htm.

[30] The Commission tussled with Amazon's most favored nation clause and argued it required publishers to offer Amazon similar (or better) terms and conditions as those offered to its competitors and/or to inform Amazon about more favourable or alternative terms given to Amazon's competitors. The clauses covered not only price but many aspects that a competitor can use to differentiate itself from Amazon, such as an alternative business (distribution) model, an innovative e-book or a promotion. The Commission considered that such clauses could make it more difficult for other e-book platforms to compete with Amazon by reducing publishers' and competitors' ability and incentives to develop new and innovative e-books and alternative distribution services. The clauses may have led to less choice, less innovation and higher prices for consumers due to less overall competition in the European Economic Area (EEA) in e-book distribution.
European Commission Press Release IP/17/1223, Antitrust: Commission accepts commitments from Amazon on e-books (May 4, 2017), http://europa.eu/rapid/pressrelease_IP-17-1223_en.htm.

[31] Telecommunications companies do not rely on data to bolster their corporate profit or presence. Rather, data collection for telecommunications companies helps identify problems to improve infrastructure, service, and customer service satisfaction — much like Big Tech. Just like Big Tech, however, that data collection does not come without privacy concerns when it aids criminal investigations and the state's targeting of minorities. *See, e.g.*, Julia Angwin, Charlie Savage, Jeff Larson, Henrik Moltke, Laura Poitras, & James Risen, *AT&T Helped U.S. Spy on Internet on a Vast Scale*, N.Y. TIMES (Apr. 15, 2015) https://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html.

[32] Michael Lewitt, *How Long Can Amazon's Ingenious Antitrust Avoidance Last?*, FORBES (May 1, 2018), https://www.forbes.com/sites/michaellewitt/2018/05/01/how-long-can-amazons-ingenious-antitrust-avoidance-last/#6757c2570ac0; Russell Brandom, *The Monopoly-Busting Case Against Google, Amazon, Uber, and Facebook*, THE VERGE (Sept. 5, 2018), https://www.theverge.com/2018/9/5/17805162/monopoly-antitrust-regulation-google-amazon-uber-facebook; Michael J. Coren, *Facebook is Hiring Someone to Tell Politicians it's Not a Monopoly*, QUARTZ (Apr. 9, 2019), https://qz.com/1587472/facebook-is-hiring-a-policy-manger-to-avoid-monopoly-regulation/; Casey Newton & Zoe Schiffer, *Google and Facebook's Antitrust Problem is Getting Much More Serious*, THE VERGE (Sept. 10, 2019), https://www.theverge.com/interface/2019/9/10/20858028/google-antitrust-investigation-state-attorneys-general-facebook.

[33] Lee Rainie and Maeve Duggan, *Privacy and Information Sharing: Many Americans Say They Might Provide Personal Information, Depending on the Deal Being Offered and How Much Risk They Face*, PEW RES. CTR., (Jan. 14, 2016), https://www.pewresearch.org/internet/2016/01/14/privacy-and-information-sharing/.

[34] Chris Ip, *Who Controls your Data?*, ENGADGET (Sept. 4, 2018), https://www.engadget.com/2018-09-04-who-controls-your-data.html. *See also infra* Section II.

privacy and antitrust law, the violence done to a citizen's agency and choice is circular.[35] Users are not just consumers, they are citizens. Frameworks that once reflected this duality seem to have forgotten so. Holes in antitrust and privacy law create legal issues which have consequences in consumer privacy, choice, and agency. The FTC and DOJ thus must, at minimum, consider data as a potential indicator of market power in merger review.[36] This consideration will enable antitrust enforcement to respond to our modern economy that is not always driven by prices, but more increasingly so, by data.

Part I describes how privacy is not just a social concern but a legal issue because companies today increase their revenue by compromising user privacy. Part II then briefly describes how data collection works. The findings are jarring. Part III then delves into the most robust transatlantic privacy laws: the European Union's General Data Protection Regulation (GDPR) and its progeny, the California Consumer Privacy Act (CCPA). There are notable similarities between the two but, indeed, critical differences that need to be confronted in order to protect the privacy of Americans as a whole. Part IV uses these laws to address where antitrust plays its role. By detailing the methods by which companies have acquired the power to infringe upon Americans' privacy in the first place, the Section strengthens the link between antitrust and privacy law. While privacy regulation is important on its own because small players ignoring consumer privacy also pose threats, privacy regulation would benefit greatly from paying heed to the market power created by that user data.[37] Privacy regulation is thus auxiliary to antitrust regulation, and vice versa, because antitrust laws could limit companies' ability to access and process user data.

---

[35] Privacy law requires a response mechanism that is not imprisoned by the lack of a statutory or constitutional remedy. *See infra* Sections II and III. Antitrust law, in parallel, requires a broader standard for measuring "consumer welfare." *See infra* Sections IV, V, and VI.

[36] This is not a radical proposition and does not intend to be one. In fact, the European Commission has already made the transfer and control of commercially valuable user data the center of its analysis for Google's acquisition of Fitbit. *See* European Commission, press release of Dec. 17, 2020, Case M.9660, Google/Fitbit, https://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=2_M_9660. The Commission was particularly concerned with how Google's acquisition of Fitbit would give it a leg up in the "markets for online search advertising" because of the amount of health data unlocked after the acquisition. *Id*. The European Commission has approved the acquisition, however, for reasons that have not yet been released in full. It is thus imperative in the meantime to not just treat data as a *consideration* within the market power analysis, but as an *indicator* of said market power.

[37] Privacy law is particularly vulnerable because it does not have a regulatory agency for its foundation or enforcement. Rather, it has been primarily addressed through tort or contract law. *See* Restatement (Second) of Torts §§652A-E.

While tort law generally provides redressability for various renditions of an invasion of privacy, contract law governs most of the online behavior that compromises an individual's behavior. Upon joining Facebook or Amazon, for example, users accept an agreement that has great repercussions on their privacy rights. Proving that an offer was accepted, adequate reliance was placed in the given privacy policy, or there are redressable 'damages' locks them into summary judgment or dismissal. *See*, *e.g.*, In re Northwest Airlines Privacy Litigation, 2004 WL 1278459 (D. Minn. 2004) (finding that Northwest's online privacy statement does not amount to a unilateral contract and plaintiffs failed to show they accepted any 'offer'); *see also* In re Jetblue Airways Corp. Privacy Litigation, 379 F. Supp. 2d 299, 317

Parts IV to VI then investigate two cases in which mergers and acquisitions have been unable to dodge privacy concerns: the Facebook/WhatsApp merger and the Microsoft/LinkedIn merger. These cases, reviewed by agencies both in the United States and the European Union, involve analysis that supports the idea that antitrust and privacy concerns, in today's market, are inseparable.

Part VII then discusses what these decisions entail for privacy. Privacy regulation, at this point, has been deemed insufficient to address consumer agency in Big Tech. Antitrust must thus be defibrillated to do justice to consumer agency and privacy in the modern market. The DOJ and FTC can do this, and in part VIII, a solution is proffered wherein these agencies can (1) consider data an indicator of market power and/or (2) broaden the consumer welfare standard such that the primary metric is not pricing. Sometimes, the legal issues of privacy and antitrust are seen as too big to address. So why not start small.

(E.D.N.Y. 2005) (granting a motion to dismiss where the plaintiffs could not have suffered any economic loss, which is required for a breach of contract claim, after Jetblue shared their information with third parties).

In consumer lawsuits, too, class actions do not often survive summary judgment due to a lack of Article III standing. *See, e.g.*, In re iPhone Application Litigation, 2013 WL 6212591 (N.D. Cal. 2013) (plaintiffs could not show either constitutional or statutory standing in an action alleging Apple misrepresented its privacy policy and led users to pay too much for their iPhones and lose bandwidth and battery). While statutory standing is the easiest way to allow these plaintiffs the opportunity to litigate, the statutes must provide robust protections in order to afford adequate remedies. *See, e.g.*, Tyler v. Michaels Stores, Inc., 984 N.E.2d 737, 742 (Mass. 2013) (determining that a Massachusetts state law purposefully left its text, title, and caption broad and robust to "guard consumer privacy" and thus, ruled in favor of plaintiffs whose zip codes were compromised in order to send marketing materials).

Without addressing the core elements of privacy that lack teeth, the "regulatory approach [remains] unchanged." *See* Gasser.

I. WHAT IS PRIVACY?

During Mark Zuckerberg's testimony before the House of Representatives, Representative Anna Eshoo asked Zuckerberg if he would be willing to change the company's business model "in the interest of protecting individual privacy."[38] Zuckerberg responded, "I'm not sure what that means."[39]

Zuckerberg, the CEO of Facebook, was called to the House of Representatives so Congress could "examine the alarming reports regarding breaches of trust between [Facebook], one of the biggest and most powerful [companies] in the world, and its users" and, concomitantly, "widen its lens regarding larger questions about the fundamental relationship tech companies have with their users."[40]

Congress is not the only one asking these questions.[41] Since the Cambridge Analytica scandal that brought Zuckerberg to Washington, D.C.,[42] people are "changing the way they use social media."[43] The idea that citizens should be paid for their data is gaining traction,[44] even by former presidential candidates.[45] Contemporary scholarship about and litigation over the constitutionality of data privacy thus operates against the backdrop of this breach.[46]

---

[38] *Transcript of Zuckerberg's Appearance Before House Committee*, WASH. POST. (Apr. 11, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/04/11/transcript-of-zuckerbergs-appearance-before-house-committee/.

[39] *Id*.

[40] *Id*.

[41] *See supra* Sections III, IV, and V.

[42] *See* Alexandra Ma & Ben Gilbert, *Facebook Understood How Dangerous the Trump-linked Data Firm Cambridge Analytica Could Be Much Earlier than It Previously Said. Here's Everything That's Happened Up Until Now*, BUS. INSIDER (Aug. 23, 2019), https://www.businessinsider.com/cambridge-analytica-a-guide-to-the-trump-linked-data-firm-that-harvested-50-million-facebook-profiles-2018-3. Cambridge Analytica was a British consulting firm that became infamous in 2018, when Christopher Wylie revealed that millions of Facebook users' data was being used, without their consent, for political advertising. Both Ted Cruz and Donald Trump hired Cambridge Analytica for their campaigns, which enabled them to send tailored advertisements to voters, swaying them to vote for Ted Cruz or Donald Trump.
For a further discussion of the scandal that reinvigorated privacy issues, *see* Nicholas Confessore, *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*, N.Y. TIMES (Apr. 4, 2018), https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

[43] Kristen Herhold, *How People View Facebook After the Cambridge Analytica Data Breach*, THE MANIFEST (Mar. 27, 2019), https://themanifest.com/social-media/how-people-view-facebook-after-cambridge-analytica-data-breach; Ankit Bhatia, *Two Years Since Cambridge Analytica: What Has Changed?*, CPO MAG. (May 20, 2020), https://www.cpomagazine.com/data-privacy/two-years-since-cambridge-analytica-what-has-changed/.

[44] *See, e.g.*, THE GREAT HACK (Netflix 2019); Elisabeth Zerofsky, *The Investigator*, Fall 2019 COLUMBIA JOURNALISM REV., https://www.cjr.org/special_report/guardian-carole-cadwalladr.php.

[45] *See* Kelly, *supra* note 9.

[46] *See generally* Patrick Day, *Cambridge Analytica and Voter Privacy*, 4 GEO. L. TECH. REV. 583 (2020), https://georgetownlawtechreview.org/cambridge-analytica-and-voter-privacy/GLTR-07-2020 *and* Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687 (2020), https://lawdigitalcommons.bc.edu/bclr/vol61/iss5/3.

For what many identify as the breach that not only cost Americans an election, but also, their trust and relationship with the devices they "always go back to,"[47] the United Kingdom fined Facebook £500,000, the maximum fine allowed at the time of the breach,[48] and the Federal Trade Commission (FTC) around $5 million.[49] Documentaries have taken on the task of making mainstream knowledge exactly what went wrong[50] and the conversations surrounding data protection and privacy have inspired celebrities, who rely on platforms like Instagram for their reach and relevance, to freeze their accounts for 24 hours in protest of the misinformation and hate speech that runs rampant on these platforms.[51] While the responses to such data breaches, even the biggest of our time, are multiple, there is one common denominator: we always come back to these platforms.[52]

II. HOW DATA COLLECTION WORKS

Users may know big tech knows a lot about them.[53] At this point, it has become something of a sadistic joke amongst users that their iPhones listen to them, Google knows more about them than their spouses, the FBI is watching, or that Alexa is more of a spy than a robot companion.[54] These jokes are followed by a submission to the notion that these companies or agencies know just about everything about a user.[55] But maybe it is not taken as entirely true because users want to believe

[47] Kellen Browning, *Celebrities Plan an 'Instagram Freeze,' but Reaction is Icy*, N.Y. TIMES (Sept. 15, 2020), https://www.nytimes.com/2020/09/15/technology/instagram-freeze-facebook.html.
[48] Rob Davies & Dominic Rushe, *Facebook to Pay $5bn Fine as Regulator Settles Cambridge Analytica Complaint*, THE GUARDIAN (July 24, 2019), https://www.theguardian.com/technology/2019/jul/24/facebook-to-pay-5bn-fine-as-regulator-files-cambridge-analytica-complaint.
[49] *Id.*
[50] *See supra* note 44, THE GREAT HACK; *see also* Dan Swinhoe, *The 15 Biggest Data Breaches of the 21st Century*, CSO (Apr. 17, 2020), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.
[51] *See* Browning, *supra* note 47. Since Cambridge Analytica, Big Tech has been under attack for exploiting consumer biases to keep users locked into their networks. *Id.* This is also problematic for democracy, because research has shown that people are more likely to avoid echo chambers when they have access to multiple different platforms for news, thoughts, opinions, and engagements. *See* Elizabeth Dubois & Grant Blank, *The Echo Chamber is Overstated: The Moderating Effect of Political Interest and Diverse Media*, 21 Information, Communication & Society 729 (2018).
[52] *See e.g.* THE SOCIAL DILEMMA (Netflix 2020). This docu-drama illuminates how addictive mechanisms are implanted into social media platforms to mine more data. It may be common knowledge that people are being mined for their data, but "few realize how deep the probe goes. If you think the trade-off is merely getting targeted ads for your favorite sneakers, you are in for a big shock." Kevin Crust, *Review: A Call to Digital Arms, 'The Social Dilemma' Demands Change*, L.A. TIMES (Sep. 9, 2020, 3:11 PM), https://www.latimes.com/entertainment-arts/movies/story/2020-09-09/review-social-dilemma-facebook-google-netflix.
[53] *See* THE SOCIAL DILEMMA, *supra* note 52.
[54] The suspicions have developed their own subset of investigative journalism. *See, e.g.*, Rani Molla, *Your Smart Devices Listening to You, Explained*, VOX (Sept. 20, 2019, 12:30 PM), https://www.vox.com/recode/2019/9/20/20875755/smart-devices-listening-human-reviewers-portal-alexa-siri-assistant. But frankly, Alexa and like devices are not just listening to you. They are studying you. *See* Grant Clauser, *Amazon's Alexa Never Stops Listening to You. Should You Worry?*, N.Y. TIMES (Aug. 8, 2019), https://www.nytimes.com/wirecutter/blog/amazons-alexa-never-stops-listening-to-you/.
[55] Plenty of films and series were created under the premise that we are giving into technology's control. *See, e.g.* HER (Warner Bros. Pictures 2013) *and* BLACK MIRROR (Netflix 2011).

that is not entirely legal or morally just. This may be a contributing reason as to why users are not keen on changing their online behavior.[56] Nonetheless, this Comment must unfortunately break the news that there is no joke—Big Tech does know almost everything about a user.[57] And it is important to know exactly what that means to grasp the gravity of the privacy and antitrust concerns at hand.

Facebook, for example, gathers information about a user's work, income level, race, religion, political views, and the ads a user clicks on.[58] This is all, of course, in addition to the elementary data points: a user's phone number, email address, location, and the type of devices used.[59] Google, on the other hand, collects any user's name, phone number, payment information, email address, emails the user writes and receives, any stored videos and photos, stored documents, stored spreadsheets, and YouTube comments.[60] IP addresses, system activity, date, time and referrer URL of requests, interaction between apps, browser type, device type, application version number, carrier name, and operating system are also collected.[61] And finally, as to a user's activity on Google, almost everything is fair game.[62] A user's search terms, videos watched, views and interactions with content and ads, video and audio information if audio features are used, time, frequency and duration of activity, purchase activity, the people a user communicates with or shares content with, activity on third-party sites and apps, browsing history, calling-party number, receiving party number, forwarding numbers, times and dates and calls of text, call duration, routing

---

[56] *See, e.g.,* Lee Rainie, *Americans' Complicated Feelings About Social Media In an Era of Privacy Concerns*, PEW RES. CTR. (Mar. 27, 2018), https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/ (despite privacy concerns, there are "modest associations between people's social media use and higher levels of trust, larger numbers of close friends, greater amounts of social support, and higher levels of civic participation.").
For a further discussion on the relationship between online behavior and privacy concerns, *see* Susanne Barth, *The Privacy Paradox – Investigating Discrepancies Between Exprsesed Privacy Concerns and Acutal Online Behavior – A Systematic Literature Review*, 34 TELEMATICS AND INFORMATICS 1038 (2017) https://doi.org/10.1016/j.tele.2017.04.013 *and* Tomas Chamorro-Premuzic and Nathalie Nahai, *Why We're So Hypocritical About Online Privacy*, HARVARD BUS. REV. (May 1, 2017) https://hbr.org/2017/05/why-were-so-hypocritical-about-online-privacy.
[57] Angela Moscaritolo, *What Does Big Tech Know About You? Basically Everything.*, ENTERPRENEUR (Feb. 5, 2019), https://www.entrepreneur.com/article/327513.
[58] Aliza Vigderman & Gabe Turner, *The Data Big Tech Companies Have On You*, SECURITY.ORG (Oct. 27, 2020), https://www.security.org/resources/data-tech-companies-have/. That is unfortunately not all when it comes to Facebook, especially as it continues to acquire companies like Instagram and WhatsApp.
An Instagram user has filed a lawsuit against the social networking company, claiming that Facebook spied on users through their iPhone cameras, "obtaining extremely private and intimate personal data on their users, including in the privacy of their own homes." *See* Kate Duffy, *Facebook Spied on Instagram Users Through their iPhone Cameras, A New Lawsuit Claims*, BUS. INSIDER (Sept. 18, 2020), https://www.businessinsider.com/facebook-spied-on-instagram-users-through-iphone-cameras-lawsuit-says-2020-9.
[59] *See supra* Vigderman & Turner, note 58.
[60] *Id.*
[61] *Id.*
[62] *Id.*

information, and types of calls are all collected.[63] The only user activity *not* collected are merely user messages, networks/connections, content, reviews, and privacy settings.[64] Otherwise, GPS, sensor data from a user's device, information about things near the device (like wifi access points and cell towers) and local newspapers, third-party marketing partners, and advertisers are all also in the mix of collected data. Amazon is not much better.[65]

Amazon's platform is inherently less immersive than Google and, as an e-commerce website, does not existentially depend on data.[66] Despite not *needing* data to have a return on investment, however, Amazon still collects social security and driver's license numbers, location information, and sensor data from a user's device.[67] Amazon also collects information on search terms, videos watched on Prime, purchase activity, reviews written, browsing history, address, browser type, and operating systems.[68]

Apple, albeit, has the most respect for data collection when the other competitors are Amazon, Twitter, Facebook, and Google.[69] This is a rather abysmal notation, however, when one remembers exactly what apps they may, for example, use on their Apple iPhone.[70] The apps typically used on iPhones are allowed to practically eviscerate all the privacy protections baked into the iPhone by tracking and collecting user data both when the app is and is not in use.[71] Further, Apple is not as existentially concerned with data as the others, so its collection is still noteworthy.

So what does big tech *do* with all of this data? There is a growing misconception that this data is sold, but that would assume data is fungible.[72] Big tech does not elect to sell exactly what produces

[63] *Id.*
[64] *Id.*
[65] *See supra* Vigderman & Turner, note 58.
[66] Although, with the advent of Alexa, Ring, and a few other intrusive Amazon products, Amazon is becoming far more immersive than a mere e-commerce platform.
[67] *See supra* Vigderman & Turner, note 58.
[68] *Id*. For more information on the data Amazon collects, *see supra* note 30.
[69] *Id.*
[70] In the ranking of the most-used apps on the Apple iPhone, Instagram, owned by Facebook, ranks number 6. Facebook ranks 7, Messenger, owned by Facebook, ranks 8, Gmail, owned by Google, ranks 10, and Amazon ranks 13. *See* Mobile App Rankings, SimilarWeb. *See Mobile App Rankings*, SIMILARWEB, https://www.similarweb.com/apps/top/apple/store-rank/us/all/top-free/iphone/ (last visited Jan. 18, 2021). We cannot necessarily attribute data collected by third-party apps on an iPhone to Apple, but we can still acknowledge how the interaction between these devices and their uses end up compromising more privacy than we bargained for.
[71] It is worth noting, however, that Apple is going out of its way to make data collected by third-party apps hard. *See* Jack Nicas and Mike Isaac, *Facebook Takes the Gloves Off in Feud With Apple*, N.Y. TIMES (Dec. 16, 2020) https://www.nytimes.com/2020/12/16/technology/facebook-takes-the-gloves-off-in-feud-with-apple.html.
[72] Data is not fungible because databases are not "containers that hold data the way that steel barrels hold crude oil or railroad cars hold lumber." *See* Lyn Robison, *Correcting the Misconceptions About the Nature of Data that Thwart Information Quality*, 4 MIT INFO. QUALITY INDUS. SYMP. 529, 535 (July 14–16, 2010), http://mitiq.mit.edu/IQIS/Documents/CDOIQS_201077/Papers/05_03_7C-1.pdf. It is also not like money, where "one

its revenue. Rather, that data is harvested to develop algorithms.[73] Third-party advertisers are shopping for the most competitive algorithm to target their advertising when deciding which social media platform to pay.[74] Amazon, for example, even decided to pay its users a $10 credit to grow its predictive model.[75] The more data a company has, the more competitive their models are to third-party advertisers who feed their net worth.[76]

When it comes to antitrust considerations, what *kind* of data is paramount, because it reveals the potential relationships, technology processing, business visions, or network effects at hand. The anticompetitive behavior in question, for example, may not be related to data, but rather, to a company's engineering prowess in developing algorithms. Big Tech, further, does not necessarily *want* data, but *attention*, and data is but one component in maximizing attention. But data is still part of that analysis.

Admittedly, in the context of a merger, data collection may not be as massive as it may seem. There is no magic formula for determining consumer behavior, but it may be fair to say that amongst its many traits, it can be duplicative. So a company may amass data through a merger that it already had. Data, in that case, is also "non-rivalrous" because companies can collect the same data on their own accord.[77] In fact, the same strains of our data are collected by multiple companies at any given time, and a merger does not necessarily amass "new" data by the numbers. What it does, instead, is place the rights to and control of that data in the hands of a few. In these contexts, data is not a market good or natural resource, but a materialized social relation, constituted by both technical and legal systems.[78] One would be remiss not to consider how this data may be manipulated, abused, or distorted.[79] One would be even more remiss not to consider how this has already occurred.[80] This manipulation conflicts with the economic freedom and opportunity that

---

dollar is just as good as another and all that is needed are the totals." *Id.* at 536. Rather, data is "a description of relevant portions of reality" and thereby, a materialized social relation. *Id.* at 543.

[73] For a further discussion on how these algorithms are developed, *see* THE SOCIAL DILEMMA, *supra* note 52. This Comment does not intend to fearmonger, but the dangers of these algorithms can feel overwhelmingly unlimited. There is a new term, for example, 'algorithmic warfare,' which is "built on the assumption that combat actions will happen faster than humans' ability to make decisions." So Artificial Intelligence (AI) will go to war — without us knowing if it is for or against us. *See* Khari Johnson, *The U.S. Military, Algorithmic Warfare, and Big Tech*, VENTURE BEAT (Nov. 8, 2019), https://venturebeat.com/2019/11/08/the-u-s-military-algorithmic-warfare-and-big-tech.

[74] *Id*.

[75] Sidney Fussel, *What Amazon Thinks You're Worth*, THE ATLANTIC (July 18, 2019), https://www.theatlantic.com/technology/archive/2019/07/amazon-pays-users-access-browser-data/594199/.

[76] *Id*.

[77] Darren S. Tucker & Hill B. Wellford, *Big Mistakes Regarding Big Data*, The Antitrust Source (Dec. 2014), *available at* https://www.morganlewis.com/-/media/antitrustsource_bigmistakesregardingbigdata_december2014.ashx.

[78] *See* Robison, *supra* note 72.

[79] *See supra* Sections I and II.

[80] *Id*. Facial recognition technology and license plate readers, for example, have already been used in manners that the law has not caught up to. *See* Nicole Martin, *The Major Concerns Around Facial Recognition Technology*, FORBES

antitrust law intends to protect.[81] And because privacy law has not yet developed to address the profound problems presented by these technical systems,[82] antitrust-enforcement agencies must.

(Sep. 25, 2019, 3:15 PM) https://www.forbes.com/sites/nicolemartin1/2019/09/25/the-major-concerns-around-facial-recognition-technology/?sh=32bbe73a4fe3.

[81] "The goal of the antitrust laws is to protect economic freedom and opportunity by promoting free and fair competition in the marketplace. Competition in a free-market benefits American consumers through lower prices, better quality, and greater choice. Competition provides businesses the opportunity to compete on price and quality, in an open market and on a level playing field, unhampered by anticompetitive restraints. Competition also tests and hardens American companies at home, the better to succeed abroad." *Mission*, U.S. DEP'T OF JUST., https://www.justice.gov/atr/mission#:~:text=The%20goal%20of%20the%20antitrust,better%20quality%20and%20greater%20choice (July 20, 2015).

[82] *See supra* Sections I and II.

III. PRIVACY IN THE LAW

Privacy is no new concept to Americans or human rights law.[83] The "exact nature and extent of [privacy] protection," however, was challenged by technological advancements.[84] Advancements in information and communication technologies were seen as threats, and instead of advancing privacy law while technologies, too, were advancing, privacy laws took on a defensive reaction to growth.[85] This was unordinary because American law otherwise plays a much more enabling or even leveling role to achieve a "desired innovative or disruptive activity."[86] But this problem is hardly unique to the United States. Even entities like the European Union, with arguably stronger conceptions of where data protection and privacy stands on principle,[87] went through layers of reforms to achieve what the California Consumer Privacy Act (CCPA) seeks to embody: the General Data Protection Regulation (GDPR).[88]

---

[83] *See generally*, Brandeis & Warren, *supra* note 20.

[84] *Id. See also* Gasser, *supra* note 21. ("That the individual shall have full protection in person and in property is a principle as old as the common law" and has only been deemed necessary, "from time to time[,] to define anew the exact nature and extent of such protection.").

[85] Robert Gellman, Fair Information Practices: A Basic History 1 (June 17, 2016) (unpublished manuscript), http://bobgellman.com/rg-docs/rg-FIPShistory.pdf.

[86] *See* Gasser, *supra* note 21. The rise of Silicon Valley, for example, can be understood as a result of the law, specifically intellectual property and tort law, enabling desired innovation. *See* Anupam Chander, *How Law Made Silicon Valley*, 63 EMORY L. J. 639 (2014).

[87] The EU Charter of Fundamental Rights enshrines the right to "the protection of personal data concerning him or her" to everyone. Council Directive 2001/18, art. 8, 2001 O.J. (L 106) 1 (EC). "Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified." *Id.*

The Treaty on the Functioning of the European Union, additionally, obliges the EU to "lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data." Treaty on the Functioning of the European Union 326/47-326/390, art. 16, Mar. 25, 1957, O.J. L.

[88] The CCPA is California's Consumer Privacy Act, now amended and expanded by the California Privacy Rights Act (passed in the November 2020 ballot). It is unclear the exact ramifications of the California Privacy Rights Act. *Compare*, for example, Cameron F. Kerry & Caitlin Chin, *By Passing Proposition 24, California Voters Up the Ante on Federal Privacy Law*, BROOKINGS (Nov. 17, 2020), https://www.brookings.edu/blog/techtank/2020/11/17/by-passing-proposition-24-california-voters-up-the-ante-on-federal-privacy-law/, (arguing that the CPRA "raises the bar" because now, businesses are restricted in how they collect and process data and are required to "protect personal information") *with* Greg Bensinger, *A Privacy Measure that's Hard to Like*, N.Y. TIMES (Oct. 28, 2020) https://www.nytimes.com/2020/10/28/opinion/california-prop-24-privacy.html (maintaining that the CPRA will give Californians "the right to seek to prohibit sharing of their data," but falls short because there are too many loopholes. Notably, there is no opt-out default, so consumers would have to manually register their preferences in data protection among a wide swath of websites).

The proposition was quite contentious. Organizations committed to data privacy and protection, like the Electronic Frontiers Foundation, remained neutral because the Proposition was a "mixed bag of partial steps backwards and forwards." *See* Lee Tien, Adam Schwartz, & Hayler Tsukayama, *Why EFF Doesn't Support California's Proposition 24*, Electronic Frontiers Foundation (July 29, 2020), https://www.eff.org/deeplinks/2020/07/why-eff-doesnt-support-cal-prop-24. The American Civil Liberties Union and Public Citizen, however, opposed it outright, alleging it is wrought with pay-for-privacy schemes. *See* Press Release, ACLU of Southern California Proposition Endorsements for 2020 Election, ACLU (Oct. 5, 2020), https://www.aclu.org/press-releases/aclu-southern-california-proposition-endorsements-2020-election; *see also* Consumer Action Opposes California Proposition 24, Cision PR Newswire (Aug.

The GDPR gives EU citizens unprecedented control over how their personal information is collected, store, and used by organizations.[89] For that, it remains the strongest privacy protection act worldwide since its enactment in May 2018.[90] The GDPR protects consumer's names, addresses, pictures, DNA, IP addresses, and payment information.[91] Business owners must ask for permission *before* collecting each user's data using clear and simple language, notify users within 72-hours of a data breach, and, at each user's request, must explain what information is being collected, how it is being used, with whom it is being shared, and erase any information that may have been collected in the past.[92] The sheer reach of this legislation has invited criticism over how it could hurt business models or even encourage businesses to secretly collect and profit off of user information, but these criticisms have not gone far.[93] Rather, the GDPR has been, for the most part, successful in both protecting existing business models and protecting user privacy.[94] And this protection follows EU citizens wherever they are, protecting even European customers who purchase from US e-commerce merchants.[95]

19, 2020), https://www.prnewswire.com/news-releases/consumer-action-opposes-california-proposition-24-301115223.html.

The need for data protection and privacy legislation came after the development of "automatic data processings, which enables vast quantities of data to be transmitted within seconds across national frontiers." *See Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD, https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (last visited Jan. 18, 2021). When OECD Member countries began passing legislation in support of data protection and privacy, some were stronger than others. The General Data Protection Regulation currently stands as the toughest set of data protection rules, "enhanc[ing] how people can access information about them and plac[ing] limits on what organisations can do with personal data." Matt Burgess, *What is GDPR? The Summary Guide to GDPR Compliance in the UK*, WIRED (March 24, 2020), https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018. The regulation is what countries across the globe are looking to for inspiration. *See* Dan Simmons, *12 Countries with GDPR-Like Data Privacy Laws*, COMFORTE (Jan. 17, 2019), https://insights.comforte.com/12-countries-with-gdpr-like-data-privacy-laws.

What makes the GDPR so particularly strong is its consent model, which requires companies to post "clear notices for users and get their *unambiguous consent* to collect data, instead of burying an OK inside fine print and legal jargon." *GDPR: Why Privacy is Now Stronger in EU Than U.S.*, FORTUNE (May 25, 2018), https://fortune.com/2018/05/25/what-is-gdpr-compliance.

The CCPA, on the other hand, is an opt-out model, which means users must manually opt-out of the sale of their information by clicking, for example, a 'Do Not Sell My Personal Information' link. For a further discussion of the difference between these two models, see *infra* Section III.

[89] Regulation 2016/679 of the European Parliament and of the Council of Apr. 27, 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 4, 2016 O.J. (L 119) 33 (EU) [hereinafter GDPR].

[90] *Id.*

[91] *Id.*

[92] *Id.*

[93] *A Breakdown of CCPA, GDPR, HIPAA and Other Privacy Acts*, BLUEPAY, https://blog.bluepay.com/a-breakdown-of-ccpa-gdpr-hipaa-and-other-privacy-acts (last visited Jan. 18, 2021).

[94] Josephine Wolff, *How is the GDPR Doing?*, SLATE MAG. (Mar. 20, 2019), https://slate.com/technology/2019/03/gdpr-one-year-anniversary-breach-notification-fines.html; *Two Years of the GDPR: Questions and Answers*, EUROPEAN COMMISSION (June 24, 2020), https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1166.

[95] *Id*.

The CCPA aimed to follow suit, but the California Privacy Rights Act (CPRA), effective January 1, 2023, brings waves of uncertainty.[96] There is great debate over the nature of the CPRA and whether it expands the CCPA or reverses it.[97] Regardless, both steps towards better privacy regulation still do not resolve the question of data collection. Data collection may be constrained under these acts, but that would, arguably, *increase* the value of who has access to data and how much. The GDPR and CCPA are both simultaneously detailed and vague regulations, leading to a greater need for attorneys and significant compliance costs. Thereby exacerbating the antitrust problem if only a handful of companies have a stronghold over user data because they can afford it.

The CCPA was nonetheless the United States' most sweeping privacy act, granting citizens some degree of control over how their personal information is collected, stored, and used by organizations.[98] It did not apply to *all* businesses; rather, the law only applied to businesses that either generated $25 million annually, earned at least half of their revenue from selling personal information, or collected personal data from 50,000+ customers, devices, or households.[99] This generally implicated companies like Facebook, Amazon, and Google.[100] And it does not matter where the company is incorporated. Any businesses that have any physical presence, employees, or customers in California would have been at risk of penalty if they flouted the law.[101] Since the CCPA was enacted, some states, like New York, Nevada, and Maryland, have devised their own privacy regulations.[102]

Personal information under the CCPA means "any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked," with a particular consumer or household.[103] Businesses are thus required to disclose any personal information collected, sold, or disclosed for a business purpose about a consumer, delete any personal information in response to consumer requests, to not discriminate against any consumer who elects to exercise their rights under the CCPA, and to describe in its online privacy policy consumers'

[96] *See supra* note 88.
[97] *Id*.
[98] Assemb. B. 375, 2017–18 Reg. Sess. (Cal. 2018), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180AB375.
[99] *Id*.
[100] *Id*.
[101] *Id*.
[102] Rachel R. Marmor, Maryam Casbarro, Monder Khoury, & Nancy Libin, *"Copycat CCPA" Bills Introduced in States Across Country*, DAVIS WRIGHT TREMAINE LLP PRIV. & SEC. L. BLOG (Feb. 8, 2019), https://www.dwt.com/blogs/privacy--security-law-blog/2019/02/copycat-ccpa-bills-introduced-in-states-across-cou).
[103] *See supra* note 88.

rights under the CCPA.[104] The privacy policy must also include the methods for submitting consumer requests and a list of categories of personal information that the business has collected, sold, and disclosed about consumers in the past twelve months.[105] Now, the CCPA has been amended and expanded by the newly enacted California Privacy Rights Act, which is generously described as a delphic.[106]

Even before the CPRA was passed, however, there was a critical difference between the CCPA and the GDPR: their foundational models. The GDPR is grounded in a consent model, where 'consent' is "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."[107] Based on these four requirements for consent, browsewrap agreements and pre-checked boxes are no longer permitted, and users cannot be punished for refusing to consent with a given site's cookies or policies.[108]

This is in stark contrast with the CCPA, which, despite its ambitions to emulate the GDPR's reforms, is curbed by the opt-out model.[109] The CCPA does not, like the GDPR, require users to give affirmative, clear consent before any personal data is collected or processed.[110] Rather, it merely makes it possible for consumers to direct a business not to sell their personal information to a third party. Even that, with certain caveats.[111] A business under the CCPA must provide a "Do Not Sell My Personal Information" link on its homepage that links to another webpage enabling a consumer to opt-out of the sale of his/her personal information.[112] Otherwise, a business must only affirmatively *not* sell personal information of consumers if the business has "actual knowledge" that the consumer is less than 16 years of age and has not authorized the sale as either a 13-16 year old or through a parent or guardian.[113] This is an incredibly narrow circumstance since in nearly

[104] *Id*. Online privacy policies are difficult because they can generally be reduced to optics. In terms of contract law, it is very difficult to prove actual reliance on the policy. *See* In re Northwest Airlines Privacy Litigation *and* In re Jetblue Airways Corp. Privacy, *supra* note 37.
[105] *Id*.
[106] *See* Greg Bensinger, *A Privacy Measure That's Hard to Like*, N.Y. TIMES (Oct. 28, 2020), https://www.nytimes.com/2020/10/28/opinion/california-prop-24-privacy.html. The CPRA is discussed at length in *supra* note 88.
[107] *See generally* GDPR, *supra* note 89. For more information, *see GDPR FAQs: Frequently Asked Questions About GDPR*, EU GDPR.ORG, https://eugdpr.org/the-regulation/gdpr-faqs/.
[108] *Id*.
[109] CAL. CIV. CODE §§ 1798.100–199 (West 2019) [hereinafter CCPA].
[110] *Id.*
[111] The CCPA does not stop a business from distributing the data within the organization that collected it, even different business units, and does not stop transfers outside of personal information to third parties. *Id*.
[112] *Id.*
[113] *Id.*

every online interaction, as technology currently stands, it is almost impossible for a business to gauge the actual age of the consumer or require parent or guardian authorization.

It is also important to note what the CCPA does *not* do, which is restrict a business's ability to (1) collect, use, retain, sell, or disclose consumer information that is de-identified or in the aggregate consumer information and (2) collect or sell a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California.[114]

In effect, the CCPA's opt-out model provides legal recognition of a data harm by extending principles of torts and contracts,[115] which provides a notable cause of action, but reveals the limitation of privacy law.[116] There are privacy concerns everywhere — not just with Big Tech — and the core regulatory privacy approach has not changed from an inherently defensive stance.[117] Information and communication technologies have been rendered threats that we, as consumers, either in the European Union or the United States, must either consent to or hope that there is a cause of action to support our dissent.[118] Not only was there "always going to be a Cambridge Analytica" under these defensive stances, but there will likely be another one.[119]

IV. PRIVACY RECODING DEPENDS ON ANTITRUST RECODING

While privacy law can benefit from a holistic "recoding,"[120] its ramifications are too steeped in antitrust concerns to be reformed alone.[121] When one thinks of data protection and privacy, the

[114] The GDPR also allows the use of de-identification to reduce liability and/or risk. *See* GDPR.
[115] Leading privacy analysts Daniel Solove and Danielle Citron define harm as the "impairment, or set back, of a person, entity, or society's interests. People or enities suffer harm if they are in worse shape than they would be had the activity not occurred." Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. R. 737, 747 (2018). Data harm does this by increasing risk and anxiety, as companies collect "more and more personal data in inadequately secured data reservoirs." *See id*. at 745.
Solove and Citron identify a refusal to engage in activities that "depend on good credit, like house- and job-hunting, … [and searching for a] new home or employment," emotional distress, paranoia that "thieves may be using one's personal data for criminal ends" and more as potential consequences of data harm. *See id.* This harm has "confounded" courts, calling into question a plaintiff's standing. *See id*. at 737. For a further discussion on how to conceptualize data harms, see Joanna Redden, Jessica Brand, & Vanesa Terzieva, *Data Harm Record*, DATA JUST. LAB, https://datajusticelab.org/data-harm-record/#_ftn3 (updated Aug. 2020).
[116] *Id.*
[117] *See* Gasser, *supra* note 21.
[118] *Id*.
[119] In the Netflix documentary, *The Great Hack*, former Chief Operating Officer of Cambridge Analytica, Julian Wheatland, says "there was always going to be a Cambridge Analytica." *See* Eric Johnson, *Cambridge Analytica Made 'Ethical Mistakes' Because it was Too Focused on Regulation, Former COO Says*, VOX (Jul. 31, 2019), https://www.vox.com/recode/2019/7/31/20747874/cambridge-analytica-julian-wheatland-great-hack-netflix-documentary-kara-swisher-podcast-interview. And many believe there will be another one. *See* David Petersson, *Another Cambridge Analytica is Out There, and We Aren't Ready to Fight It*, VENTURE BEAT (Apr. 13, 2018), https://venturebeat.com/2018/04/13/another-cambridge-analytica-is-out-there-and-we-arent-ready-to-fight-it.
[120] *See* Gasser, *supra* note 21.
[121] *Id*.

platform-based companies that are collecting that data for algorithms, experimentation, and advertisement revenues come to mind. Apple, Facebook, Amazon, Microsoft, and Google are growing *through* mergers and acquisitions, which increase their market power by increasing their access to and control over user data. For that, the issue is inherently baked into merger reviews.

The Sherman Antitrust Act, the bedrock of antitrust law, was enacted to prohibit activities that discourage competition in the marketplace.[122] Senator John Sherman introduced the Act because "the law of selfishness, uncontrolled by competition, compels it to disregard the interests of the consumer."[123] He went onto delineate the evils that surface without this enforcement,

"If we will not endure a king as a political power we should not endure a king over the production, transportation, and sale of any of the necessaries of life. If we would not submit to an emperor we should not submit to an autocrat of trade, with power to prevent competition and to fix the price of any commodity."[124]

Antitrust enforcement, to Senator Sherman and the accompanying legislative intent for the Act, is thus necessary to conserve not just competition, but freedom in the marketplace.

Since its enactment, however, antitrust law has wrestled with delineating exactly what behaviors can be deemed anti-competitive and threaten freedom in the marketplace. In this regard, courts and regulatory agencies alike rely heavily on the presence or absence of market power to uproot an antitrust violation. But market power, understood as a company's "ability to raise price profitably above the competitive level,"[125] arguably stands without a clear definition because it is unclear what that *competitive level* of pricing is.[126] Courts thus assess elasticity facing a firm by defining the relevant market and calculating the defendant's market share within that market.[127] Some scholars propose that, instead, market power should be determined by evaluating whether the defendant's conduct has enabled the defendant "to raise price above the prevailing level or maintain price above the but for level (the level to which price would fall absent the challenged conduct)."[128]

---

[122] 15 U.S.C. §§ 1-2 (2012), [hereinafter "Sherman Act."]. The Sherman Act prohibits the abuse of a monopoly through anti-competitive conduct. *Id*.
[123] 21 CONG. REC. 2461 (1890) (statement of Sen. Sherman).
[124] *Id*.
[125] *See* John B. Kirkwood, *Market Power and Antitrust Enforcement*, 98 B.U. L. REV. 1169, 1170 (2018).
[126] *Id*. *See also* Louis Kaplow, *Market Definition and Merger Guidelines*, 39 REV. IND. ORG. 107, 123 (2017) ("The market definition/market share paradigm is not merely clumsy and sometimes misleading. Rather, it is entirely bankrupt.").
[127] *See Kirkwood, supra* note 125 at 1170.
[128] *Id*.

Regardless of the alternatives available, many scholars share a concern in the lack of a reliable definition for market power.[129]

Naturally, a stronger definition of market power will result in better antitrust enforcement altogether. Without a reliable definition, the grounds are fertile for heightened monopoly power and concentration. Antitrust law is also often *limited* by the market power analysis more often than it is enhanced by it. The issue here, for privacy, is that the traditional market power analysis is based on the control of prices, but data provides another means of excluding competitors without being tethered to prices. And in the context of this Comment, ignoring the element of data in a market power analysis leaves merger review all the muddier.

A. RECODING MERGER REVIEWS

The data acquired through mergers and acquisitions may not always be revelatory or unique, but does put mass amounts of commercially valuable data in the control of a few.[130] For that, merger review is of concern.

Much of the doctrine for merger review comes from the Clayton Act, which expanded upon the Sherman Act.[131] Mergers and acquisitions are particularly vulnerable to substantially lessening competition so, under Section 7 of the Clayton Act, the Federal Trade Commission (FTC) and Department of Justice (DOJ) must review and potentially enjoin mergers or attack anticompetitive businesses if they harm competition.[132] There are two types of mergers: horizontal and vertical. Horizontal mergers are mergers between firms operating in the same industry.[133] For example, a

---

[129] *See* 2B PHILLIP E. AREEDA, HERBERT HOVENKAMP & JOHN L. SOLOW, ANTITRUST LAW 114 (3d ed. 2007) ("Instead of trying to measure the degree by which a profit-maximizing monopoly price exceeds the competitive price, courts traditionally attempt to infer market power from the [defendant's] market share.").

[130] In a lot of mergers, especially horizontal mergers for companies that don't already have an ad-based model, the aquired data is unique. One example is the Sprint and T-Mobile merger, which was partially approved because each had completely different customer bases. *See* Nilay Patel, *The Court Let T-Mobile Buy Sprint Because Sprint Completely Sucks*, THE VERGE (Feb. 12, 2020, 10:19 AM) https://www.theverge.com/2020/2/12/21134278/sprint-tmobile-merger-court-ruling-opinion-decision-explainer-carriers-antitrust.

[131] The Clayton Act, Pub.L. 63–212, 38 Stat. 730 (1914) (codified at 15 U.S.C. §§ 12–27, 29 U.S.C. §§ 52–53).

[132] 15 U.S.C § 18 (2012) [hereinafter Clayton Act].

[133] U.S. Dep't Just. & Fed. Trade Comm'n, Horizontal Merger Guidelines 2 (2010), https://www.justice.gov/sites/default/files/atr/legacy/2010/08/19/hmg-2010.pdf.

The FTC's horizontal merger guidelines, too, have important implications for privacy. The evidentiary standard is steep — merger reviews must show that the resulting lack of competitive conditions would **both** prevent other companies from replicating the elements of a successful business model **and** meet the frustrated demands of people for whom other companies, for example, had more attractive privacy practices. *See* U.S. Dep't Just. & Fed. Trade Comm'n, Horizontal Merger Guidelines 2 (2010), https://www.justice.gov/sites/default/files/atr/legacy/2010/08/19/hmg-2010.pdf.

The FTC defines success for merger remedies as "maintaining or restoring competition [such that] competition in the relevant market remained at its pre-merger level or returned to that level within a short time (two to three years)." FED. TRADE COMM'N, THE FTC'S MERGER REMEDIES, 2006-2012 15 (Jan. 2017),

merger between Coca-Cola and Pepsi. Vertical mergers, on the other hand, are mergers between companies that provide different supply chain functions for a common good or service.

A principal question in merger analysis, then, is whether the proposed merger is likely to create, enhance, or facilitate market power.[134]

The antitrust revolution in the 1970s provides important background as to how this question is answered.[135] Price theory became the dominant lens with which to view anticompetition inquiries in the 1970s because "[w]hat exists is ultimately the best guide to what should exist."[136] That shift was premised on the theory that, without prices, there can be "no markets, and consequently, no market power."[137] Production, allocation, consumption, and pricing of goods and services thus took centerstage in antitrust enforcement and analyses under price theory.

Two consequences followed from the adoption of price theory. First, there was a "significant narrowing of the concept of entry barriers," which are costs borne by a firm seeking entry into the industry.[138] Second, "consumer prices became the dominant metric for assessing competition."[139] This metric is now understood as the consumer welfare standard, which originated with Robert

---

https://www.ftc.gov/system/files/documents/reports/ftcs-merger-remedies-2006-2012-report-bureaus-competition-economics/p143100_ftc_merger_remedies_2006-2012.pdf.
Even proposed reforms of merger enforcement do not change this focus on avoiding the lessening of competition, rather than enhancing it. *See, e.g.*, Consolidation Prevention and Competition Promotion Act of 2017, S. 1812, introduced by Senator Amy Klobuchar (D-MN), September 14, 2017, https://www.congress.gov/bill/115th-congress/senate-bill/1812 (changing the standard from "substantially lessening competition" to "materially lessens competition in more than a de minimis amount.").

[134] *Id.*

[135] Before the antitrust revolution in the 1970s, economic structuralism dominated most antitrust analysis. *See e.g.*, Brown Shoe Co. v. United States, 370 U.S. 294, 328-34 (1962) (including the shoe industry's history and trend towards consolidation as part of its market share analysis when assessing a shoe manufacturing company's acquisition of a retail chain) *and* United States v. Phila. Nat'l Bank, 374 U.S. 321, 364-65 (1963) (halting a horizontal merger, under the *Brown Shoe* analysis, where the merged bank's market share was only 30% because other factors pointed to anticompetition). Under economic structuralism, court decisions embraced multifactor analyses that considered both size and potential conflicts of interest.
In *Brown Shoe*, for example, fairness and efficiency were traded off. *See* Brown Shoe Co., 370 U.S. at 344 ("It is competition, not competitors, which the Act protects. But we cannot fail to recognize Congress' desire to promote competition through the protection of viable, small, locally owned business. Congress appreciated that occasional higher costs and prices might result from the maintenance of fragmented industries and markets. It resolved these competing considerations in favor of decentralization. We must give effect to that decision.") This all changed with *Continental T.V. Inc. v. GTE Sylvania, Inc.*, where the Supreme Court applied a "rule of reason" approach in "deciding whether a restrictive practice should be prohibited as imposing an unreasonable restraint on competition." Continental T.V., Inc. v. GTE Sylvania, Inc., 433 U.S. 36, 49 (1977) (citing Chicago Bd of Trade, 246 U.S. at 238). Consumer welfare was deemed the goal of antitrust law and thereby constrained the discretion of federal courts. *Id*.

[136] *See* Eisner, *supra* note 20 at 104.

[137] *See generally* John M. Newman, *Antitrust in Zero-Price Markets: Foundations*, 164 U. PA. L. REV. 149 (2015). *Available at*: https://scholarship.law.upenn.edu/penn_law_review/vol164/iss1/4. There is tremendous scholarship criticizing the neoclassical model of price theory, and the potential to overlook harms that do not reflect positive pricing.

[138] *See* George J. Stigler, THE ORGANIZATION OF INDUSTRY 67 (1968). *See also* Khan, *supra* note 25.

[139] *See* Khan, *supra* note 25.

Bork but has been interpreted by courts as a measurement of consumer prices.[140] Many scholars today critique the consumer welfare standard and how it has potentially crippled antitrust law's capacity to confront big tech conglomerates. Antitrust attorney Lina Khan, especially, advocates for a reoriented approach, concentrated on *competition*, because consumer welfare is too narrow to capture the modern market characterized by a swath of companies offering free to low-cost services.[141]

In effect, price theory and the consumer welfare standard are fundamentally flawed when confronting Big Tech because they are not compatible with the outgrowths of technology and data. Predatory pricing, for example, becomes a highly rational endeavor for current market players under the price theory.[142] Existing business models also offer free to low-cost services in exchange for more valuable indicators of market power. Thus, price theory and the consumer welfare standard are especially ill-suited where is no way to quantify the loss to 'consumer welfare' after a loss of privacy and/or other non-monetary harm caused by market consolidation. Further, consumers care about more than just pricing. They care about quality, variety, innovation, and even privacy. Merger review is thus limited by a standard that companies like Facebook, Amazon, and Google could not successfully be scrutinized under.

The three main steps, now, in the United States' merger review are: (1) to define the product market, which involves analyzing the set of products that a monopolist could profitably raise the prices of; (2) to define the geographic market, which parallels the area that the monopolist is allegedly raising prices in; and (3) predict the merger's expected market share by determining the market share of the participants and any market concentration through the Herfindahl-Hirschman Index (HHI).[143] European competition law, similarly, employs the same tests but differs in some of its language.[144] The analysis is thus highly dependent on the definition of the market, and many

[140] *See generally* Herbert Hovenkamp, *On the Meaning of Antitrust's Consumer Welfare Principle*, Faculty Scholarship at Penn Law https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=3154&context=faculty_scholarship. For a critique of Bork's definition, *see* Robert H. Lande, *A Traditional and Textualist Analysis of the Goals of Antitrust: Efficiency, Preventing Theft from Consumers, and Consumer Choice*, 81 FORDHAM L. REV. 2349 (2013).
[141] *See* Khan, *supra* note 25.
[142] For a further discussion of the relationship between the consumer welfare standard and predatory pricing, *see* Lina M. Khan, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710 (2017).
[143] U.S. Dep't of Justice, *supra* note 133, at 18. The HHI is calculated by "summing the squares of the individual firms' market shares, and thus gives proportionately greater weight to the larger market shares." *Id*.
[144] Caleb Vesey, *Comparing EU and US Merger Guidelines*, EUROPEAN UNION COMPETITION LAW https://www.eucomplaw.com/merger-analysis/.

antitrust disputes are won and lost once the relevant market is defined.[145] This could cause problems if one is counting on antitrust law to police privacy issues.[146]

For example, imagine a merger between Facebook and Salesforce.com. Facebook's user base consists, almost entirely, of consumers. Salesforce's user base consists, almost entirely, of businesses. They play in entirely different markets and would therefore draw far less scrutiny. Yet, they both have detailed, and complementary and/or non-duplicative, data about people. The combination of that data would move a lot of information and power under one roof.

Thus, while the substantive inquiry is no easy task, that does not rid it of exposition or modification. The procedure for merger review would significantly benefit from a revamping that includes the acquisition and stronghold over data in its determination.

The FTC and DOJ are specifically of concern because they spearhead merger review. Companies are generally required to report any deal valued at more than $94 million for review and after doing so, the FTC and DOJ decide whether the merger warrants a preliminary review.[147] Under such a limited definition of "substantially lessening competition," however, merger reviews do not create or enhance competition, but preserve it.[148] When Google proposed to acquire DoubleClick, a company that developed and provided Internet ad serving services,[149] for example, the FTC closed its investigation because it is strictly concerned with "identify[ing] and remedy[ing] transactions

[145] *See* Walker Process Equip., Inc. v. Food Mach. & Chem. Corp., 382 U.S. 172, 177 (1965) ("Without a definition of [the relevant] market there is no way to measure [defendant's] ability to lessen or destroy competition."); McWane, Inc. v. FTC, 783 F.3d 814, 828 (11th Cir. 2015) ("Defining the market is a necessary step in any analysis of market power . . . ." (quoting U.S. Anchor Mfg., Inc. v. Rule Indus., Inc., 7 F.3d 986, 994 (11th Cir. 1993))).

[146] Even if one is not counting on antitrust law to resolve privacy concerns, Big Tech is still using privacy policies in a manner relevant to anticompetitive considerations. Professor Daniele Condorelli has identified a practice of *privacy-policy tying*, wherein privacy policies are bundled such that they apply across unrelated services. *See* Daniele Condorelli, *Data-Driven Platform Envelopment with Privacy-Policy Tying*, OECD ON THE LEVEL (Feb. 18, 2021), https://oecdonthelevel.com/2021/02/18/data-driven-platform-envelopment-with-privacy-policy-tying/. Facebook, for example, collects information from Facebook Messenger, Instagram, and any other features, apps, technologies, software, products, or services offered by Facebook. *Id*. This may result in short-term benefits to consumers in the form of a *better ad experience*, (which is arguably a small reward to reap), but will leave consumers worse off if the "end result is monopoly." *See id*.

[147] The Hart-Scott-Rodino Antitrust Improvements Act, [hereinafter Hard-Scott-Rodino Act], requires filing with the DOJ and FTC before any merger or acquisition occurs. That way, antitrust enforcement agencies can determine whether the merger or acquisition is in compliance with antitrust law and goals. *See* 15 U.S.C. § 18(a).

[148] "[T]]he Department seeks to avoid unnecessary interference with that larger universe of mergers. *See 1982 Merger Guidelines*, DEP'T OF JUST., https://www.justice.gov/archives/atr/1982-merger-guidelines (Aug. 4, 2015). For a further discussion on why this preservation may not be enough, *see generally* Khan, *supra* note 25.

[149] Joanna Geary, *DoubleClick (Google): What is it and What Does it Do?*, THE GUARDIAN (Apr. 23, 2012), https://www.theguardian.com/technology/2012/apr/23/doubleclick-tracking-trackers-cookies-web-monitoring.

that *harm* competition."[150] A market can, therein, only be as good as it already is.[151] This presents difficulties when, for example, in the wake of COVID-19, the "only option" adopted by students, teachers, healthcare providers, therapists, and professionals across the board is Zoom, despite its neglect for data protection and privacy.[152] Or, for example, when platform-based companies have restructured the market with a new business model whereby users are offered free and/or low-cost services because the company's near-entire revenue is based off advertisements.[153] These behaviors have led to users bearing the cost of privacy breaches, at best.[154] At its worst, it leads companies to experiment on their users, without their consent, through algorithms designed to manipulate and predict consumer behavior that will, in turn, give companies an upper-hand in the market.[155] While the social concerns are salient, the task of antitrust law, as professed by Senator Sherman on the Senate floor, is clear: to prevent such abuses and preserve competition in the marketplace. Antitrust is a safeguard and check for democracy. Changing the methods of merger review such that the definitions of market power and consumer welfare are broadened to include modern indicators of economic growth and concentration would suture some of these wounds, and a look into two European Union Commission decisions on proposed mergers explains why.

---

[150] Statement Concerning Google/DoubleClick, Fed. Trade. Comm'n, File No. 071-0170, (emphasis added), https://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf. In a 4-1 decision, the FTC decided not to proceed with its investigation because the proposed merger did not substantially harm competition. The European Union, too, closed its investigation after concluding likewise. *See* EC, Regulation No 139/2004 Merger Procedure, Case No COMP/M.4731 – Google/DoubleClick, https://ec.europa.eu/competition/mergers/cases/decisions/m4731_20080311_20682_en.pdf.

[151] *See* Khan, *supra* note 25.

[152] Since the COVID-19 pandemic and the increased reliance on our computers, Zoom has become the app-of-choice for schools and workforces alike. *See* Natasha Mascarenhas, *Zoom's Earliest Investors are Betting Millions on a Better Zoom for Schools*, TECHCRUNCH (Sept. 23, 2020) (unwieldy URL); Lizzie Widdicombe, *The Great Zoom-School Experiment*, THE NEW YORKER (Apr. 2, 2020), https://www.newyorker.com/news/our-local-correspondents/the-great-zoom-school-experiment.

This is especially troubling when Zoom exhibits a neglect for data protection and privacy. *See* Khristopher J. Brooks, *Zoom Sued for Allegedly Sharing Users' Personal Data with Facebook*, CBS NEWS (Apr. 1, 2020) https://www.cbsnews.com/news/zoom-app-personal-data-selling-facebook-lawsuit-alleges/.

[153] WeChat, however, is an anomaly here because, despite its advertising revenue, "the majority of its money [is made] from gaming." *See WeChat's Owner is Rolling Out Tools for US Advertisers*, EMARKETER (Sept. 25, 2017), https://www.emarketer.com/Article/WeChats-Owner-Rolling-Tools-US-Advertisers/1016517. Ads are only about 20% of WeChat's revenue. *Id.* In fact, WeChat *limits* ads on WeChat Moments to less than 2 per user per day. *See* Connie Chan (@ConnieChan), TWITTER (Jan. 11, 2019, 7:30 AM), https://twitter.com/conniechan/status/1083748070032957443.

[154] Both consumers and companies have to pay the cost of data breaches. "It is posited that consumers as a whole incur costs that are comparable to those incurred by the provider as a result of data breaches." SIDDHARTH DONGRE, SUMITA MISHRA, CAROL ROMANOWSKI, & MANAN BUDDHADEV, QUANTIFYING THE COSTS OF DATA BREACHES, 13 (2019). Identity theft, credit card fraud, protection and monitoring, legal fees, and other intangible consequences, like difficulty securing credit cards, loans, jobs, home mortgages, and home rentals, high credit card interest rates, and psychological impacts all are part of the consumer cost of a data breach. *Id.* at 13–14.

[155] *See supra* note 52.

V. MERGING PRIVACY PROTECTIONS WITH A LACK THEREOF: THE FACEBOOK/WHATSAPP MERGER

Unlike WhatsApp, who built its business "around the goal of knowing as little about

[users] as possible," Facebook Messenger "enables Facebook to collect data regarding its users that it uses for the purposes of its advertising activities."[156] When the two decided to merge, then, there were tremendous privacy implications for WhatsApp users whose data was now being controlled by an entity that they either intended for a different use or wanted an escape from.[157]

The European Commission, in 2014, conducted its review and considered privacy of the proposed merger between Facebook and WhatsApp.[158] Facebook's Facebook Messenger already competed with WhatsApp, so the European Commission tailored its review to the possible loss of competition in the social media market,[159] the communications app market,[160] and in the online advertising market.[161] A premier question of the review was whether the merger would create a concentration of data and thus, create a "data monopoly."[162] The Commission answered no. In its approval of the merger, the Commission yielded that "regardless of whether the merged entity will start using WhatsApp user data to improve targeted advertising on Facebook's social network, there will continue to be a large amount of Internet user data that are valuable for advertising purposes and that are not within Facebook's exclusive control."[163]

---

[156] Commission Decision of Oct. 3, 2014, Case M.7217 Facebook/WhatsApp [hereinafter EU Commission Decision, Facebook/WhatsApp], http://ec.europa.eu/competition/mergers/cases/decisions/m7217_20141003_20310_3962132_EN.pdf.

[157] This decision was in 2014. Since, there has been great controversy over the extent to which WhatsApp would maintain an independent privacy policy. When, for example, a report suggested that WhatsApp may be sharing your data with Facebook and removed the opt-out option, app downloads for Signal and Telegram skyrocketed. *See* Chance Miller, *WhatsApp Clarifies Privacy Changes and Facebook Data Sharing as Signal and Telegram Soar*, 9TO5 MAC (Jan. 12, 2021), https://9to5mac.com/2021/01/12/whatsapp-privacy-facebook-integration/.
The clarification may not be enough, however. Elon Musk tweeted two words, "Use Signal," and caused a global outage for Signal because of the millions of new users. *See Signal Faced Outage Due to Millions of New Users and Elon Musk was Around to Troubleshoot*, NEWS18 (Jan. 16, 2021), https://www.news18.com/news/buzz/signal-faced-outage-due-to-millions-of-new-users-and-elon-musk-was-around-to-troubleshoot-3297191.html.
For more on the difference between Signal and WhatsApp's privacy policies, see Rani Molla, *What is Signal and Why is Everybody Downloading it Right Now?*, VOX (Jan. 15, 2021), https://www.vox.com/recode/22226618/what-is-signal-whatsapp-telegram-download-encrypted-messaging.

[158] *See* EU Commission Decision Facebook/WhatsApp, *supra* note 156. For the purposes of this Comment, the methods of review were not substantially different between European and American regulatory forces and thus, deserve equal analysis and deference.

[159] *Id.* at paragraphs 143–63.

[160] *Id.* at paragraphs 84–142.

[161] *Id.* at paragraphs 164–190.

[162] *Id.* at paragraph 164.

[163] *Id.* at paragraph 189.

Interestingly, however, the Commission spent a considerable amount of time looking at how consumer privacy choices may be implicated. The Commission specifically looked to different privacy policies available to consumers. For example, the Commission noted that many German users switched to Threema and Telegram — two existing communication apps — "in the 24 hours following the announcement of Facebook's acquisition of WhatsApp" for their greater privacy protections.[164] WhatsApp thus "disrupt[ed] the market conditions" by merging with a market incumbent and potentially creating "loss of actual or potential competition."[165] This was indication of healthy competition to the Commission, not threatened by the merger.

The Commission concluded that, generally, "the main drivers of the competitive interaction between consumer communications apps appears to be (i) the functionalities offered and (ii) the underlying network."[166] Both were of concern in this review and because "between [70-80]% and [80-90]% of WhatsApp users were Facebook users," WhatsApp users were not at odds with Facebook Messenger's users.[167] Immediately after, however, a high number of WhatsApp users immediately switched to Telegram.[168] Given Telegram's oscillating nature in the market, this, if anything, signals that people want the better design of WhatsApp *and* the better privacy of Telegram.[169] But rather than analyze this acquisition keenly, the Commission dodged the real data privacy implications inherent in this merger so to uphold a "pure" antitrust investigation. Even though a pure antitrust investigation *does* implicate data and privacy protection because, as here, valuable user data is now under the control of a company that those users specifically intended to escape by using another app, like WhatsApp.

Further, while privacy was not at the forefront of the Commission's review, it was of enough importance to propel and substantiate its argument.[170] Instead of trusting the instinct to adapt its analysis of competition to the modern economy, however, the Commission cut its analysis too short, and sacrificed thousands of users' data and future privacy protections in the process.[171]

---

[164] *Id.* at paragraph 90, 128.
[165] DOJ 2010 Merger Guidelines, *supra* note 133.
[166] EU Commission Decision Facebook/WhatsApp, *supra* note 156 at paragraph 86.
[167] *Id.*
[168] Turner Wright, *Crypto Telegram and Tweet Numbers are Down, But There's Hope Yet*, COINTELEGRAPH (Apr. 17, 2020), https://cointelegraph.com/news/crypto-telegram-and-tweet-numbers-are-down-but-theres-hope-yet.
[169] *See supra* note 157.
[170] EU Commission Decision, Facebook/WhatsApp, *supra* note 156 at paragraph 86.
[171] Notwithstanding the privacy implications, the review's economic justifications also failed to consider that using Facebook is not the same as using Facebook Messenger. This assumption is twofold. First, that Facebook is a singular platform who, when committed to, receives an undivided share in the attention economy, as opposed to a multi-faceted conglomerate with a variety of features for consumer choice. Second, that consumer choice is an even layer, as opposed to a marble cake of possibilities. Take Apple, for example. Apple has a strong command of the marketplace, but

Despite Facebook and WhatsApp's merger resulting in an increase in market share to nearly 40%, the Commission found that the substantial overlap of their user base meant Facebook and WhatsApp "were more like providers of complementary services than close competitors."[172] This analysis falls short in recognizing that an overlap or duplication of data from a particular user base does not preclude antitrust violation. That overlap may not be dangerous under a strict consumer welfare standard, but it is dangerous when one considers market power, a company's ability to raise prices above the competitive level, and that data may be an indicator of it. The Commission went on to conclude that, after the merger, there would be alternative providers for users to easily choose from, no significant barriers to entry, and network effects would not seriously hinder competitor expansion or entry, even if Facebook integrated its Messenger service with WhatsApp.[173] But this power to choose was inevitably limited by this decision, which gave Facebook more power to tailor its advertisements to users through data collection, and by extension, gives Facebook more revenue and market share.

The privilege of hindsight also disfavors the Commission's decision that the merger would not significantly impede competition in the communications market. When merging, the United States FTC sent a letter to WhatsApp:

> WhatsApp has made a number of promises about the limited nature of the data it collects, maintains, and shares with third parties – promises that exceed the protections currently promised to Facebook users. We want to make clear that, regardless of the acquisition, WhatsApp must continue to honor these promises to consumers. Further, if the acquisition is completed and WhatsApp fails to honor these promises, both companies could be in violation of Section 5 of the Federal Trade Commission (FTC) Act and, potentially, the FTC's order against Facebook.[174]

iPhone screens are still decorated with a range of rounded communications apps for when iMessage, Apple's messaging system, falls short, either for international messages, media capacity, or GIFs.

[172] EU Commission Decision, Facebook/WhatsApp, *supra* note 156 at paragraph 86.

[173] *Id.* at paragraphs 109, 117, 135.

[174] *See* Letter from Jessica L. Rich, Bureau of Consumer Protection Director, FTC, to Erin Egan, Chief Privacy Officer, Facebook, and Anne Hoge, General Counsel, WhatsApp Inc. (Apr. 10, 2014), https://www.ftc.gov/public-statements/2014/04/letter-jessica-l-rich-director-federal-trade-commission-bureau-consumer.

Yet, in 2016, WhatsApp began sharing user's phone numbers, last seen data, operating systems, mobile country codes, mobile carrier codes, screen resolutions, and device identifiers with Facebook.[175] In 2018, Facebook unapologetically informed WhatsApp that its functions would now be the same as those of Facebook, Instagram, and Messenger: to help advertisements reach their intended audiences. Shortly thereafter, WhatsApp founders resigned from Facebook.[176] Although this may be reduced to a breach of contract, the Commission can prevent such consequences. They can do a more detailed privacy analysis *and* issue greater penalties for not keeping promises made to antitrust regulators.

This is all notwithstanding Facebook's decision to intentionally withhold its ability to automatically match users who both had the Facebook and WhatsApp apps installed, given it was already doing so for those with both Facebook and Instagram.[177] Facebook's misleading information cost it 110 million in fines,[178] but this did not change the Commission's decision.[179] The proposed transaction was lawful regardless of Facebook's misconduct because the integration of Facebook and WhatsApp data did not, at the end of the day, significantly impede competition in the communications market.[180]

Internationally, this decision undermined the credibility of antitrust enforcement. The Commission applied the consumer welfare standard for substantially lessening competition and thus, deprived its review of how data privacy *and* competition would be compromised.

VI. THE MICROSOFT/LINKEDIN MERGER

The European Commission was put to the test again in 2016, when Microsoft's proposed merger with LinkedIn invited another review of a potential data monopoly.[181] The Commission, again, landed on the negative, that "the combination of their respective datasets does not appear to result in raising the barriers to entry/expansion for other plays in this space, as there will continue to be a

[175] Natasha Lomas, *WhatsApp to Share User Data with Facebook for Ad Targeting*, TECHCRUNCH (Aug. 25, 2016), https://techcrunch.com/2016/08/25/whatsapp-to-share-user-data-with-facebook-for-ad-targeting-heres-how-to-opt-out/.
[176] Deepa Seetharaman, *Facebook's New Message to WhatsApp: Make Money*, WALL ST. J. (Aug. 1, 2018) (unwieldy URL).
[177] European Commission, press release of Dec. 6, 2016, Case M.8124, Microsoft/LinkedIn, (Microsoft Press release), https://ec.europa.eu/commission/presscorner/detail/en/IP_16_4284.
[178] European Commission, press release of May 18, 2017, *Mergers: Commission Fines Facebook 110 Million for Providing Misleading Information about WhatsApp Takeover*, https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1369.
[179] Commission Decision of Dec. 6, 2016, Case M. 8124 Microsoft/LinkedIn [hereinafter EU Commission Decision, Microsoft/LinkedIn], paragraph 108, http://ec.europa.eu/competition/mergers/cases/decisions/m8124_1349_5.pdf.
[180] *Id.*
[181] *Id.*

large amount of internet user data that are valuable for advertising purposes … not within Microsoft's exclusive control."[182] But privacy, again, ended up in its review despite privacy related concerns purportedly falling outside "the scope of EU competition law."[183]

The Commission was mainly concerned that Microsoft could use certain integration and pre-installment practices in connection with the LinkedIn app to foreclose competition in the market for professional social networks.[184]

[T]o the extent that these foreclosure effects would lead to the marginalization of an existing competitor which offers a greater degree of privacy protection to users than LinkedIn (or make the entry of any such competitor more difficult), the Transaction would also restrict consumer choice in relation to this important parameter of competition when choosing a [professional social network].[185]

As the Commission notes, this foreclosing of competition would not only reduce a consumer's ability to choose their preferred social network, but also, prevent them from exercising a choice that would protect or, at least, to some extent, alleviate their privacy concerns.[186] As a remedy, Microsoft was to restrict its conduct in connection with integrating and pre-installing the LinkedIn app, but otherwise, the merger was approved.[187] Microsoft also agreed not to increase the difficulty for other professional social networks to work within the Microsoft system.[188]

It is difficult to understand how the Commission deemed privacy as a parameter for Microsoft's potential integration and/or pre-installation of the Linked-In app. Certainly, the Commission could have signed off on those restrictions without identifying privacy as a parameter.[189]

[I]n *Facebook/WhatsApp*, in 2014, the Commission found that, while an increasing number of users valued privacy and security, at that time the majority of consumer communications apps (e.g. Facebook Messenger, Skype, WeChat, Line, etc.) did not (*mainly*) compete on privacy

[182] *Id.* at paragraph 180.
[183] European Commission, press release of Dec. 6, 2016, Case M.8124, Microsoft/LinkedIn, (Microsoft Press release), https://ec.europa.eu/commission/presscorner/detail/en/IP_16_4284.
[184] EU Commission Decision, Microsoft/LinkedIn, *supra* note 179 at paragraph 350.
[185] *Id.*
[186] *Id.*
[187] *Id.* at paragraph 470.
[188] *Id.*
[189] Eleonora Ocello & Cristina Sjodin, *Digital Markets in EU Merger Control: Key Features and Implications*, COMPETITION POL'Y INT'L (Feb. 19, 2018), https://www.competitionpolicyinternational.com/digital-markets-in-eu-merger-control-key-features-and-implications/.

features. When reviewing *Microsoft/LinkedIn* in 2016, the Commission found that privacy was an *important* parameter of competition among professional social networks, in particular in certain EU Member States, such as Germany.[190]

The decision not to indicates that antitrust review and regulation for tech and data companies has, at the least, a residual privacy component. At its heights, privacy steeps itself into antitrust concerns, with the potential to either exacerbate the lack of consumer choice or reconceptualize consumer choice and freedom.

The Commission here, for example, did not shy away from discussing Xing, a professional social network that "seem[ed] to offer a greater degree of privacy protection than LinkedIn" in Germany and Austria.[191] While LinkedIn users automatically accept its privacy policy upon pressing the 'join now' button and consent is otherwise assumed,[192] Xing has a separate box to tick in order to accept its privacy policy,[193] seeks active user consent for new policies,[194] and allows users to use the service regardless of their consent to those policies.[195] The contrast between LinkedIn and Xing's privacy policies, tangentially, are excellent examples of what a consent model under the GDPR looks like as opposed to opt-in or opt-out models.[196]

At large, the Commission was not concerned about privacy, understood as the right to keep information from others, but instead okayed the merger because others have this information too. The collection of large amounts of data leads to serious privacy concerns *and* serious market power concerns, but these were deemed two very different concerns in the Commission's review of both the Facebook/WhatsApp merger and the Microsoft/LinkedIn merger. The market power issues with collecting swaths of data were mitigated by the existence of even more data somewhere else. Yet, the privacy issues with collecting swaths of data are exacerbated, not mitigated, by the existence of even more data somewhere else. In both cases, and even more-so in the Microsoft/LinkedIn merger, the Commission seemed somewhat concerned with the economic effects of data collection, but not at all concerned with the *privacy* effects of data collection.

---

[190] *Id.*
[191] EU Commission Decision, Microsoft/LinkedIn, *supra* note 179 at paragraph 360.
[192] *Id.*
[193] *Id.*
[194] *Id.* at paragraph 390.
[195] *Id.*
[196] At this time, the CCPA had not been enacted yet, and this Comment does not intend to suggest that the CCPA did not change LinkedIn's behavior.

That renders the Commision's discussion as only the *first step* in addressing privacy concerns. The Commission needs to not only prioritize and analyze the availability of consumer choice for privacy policies, but also, the potential to have that choice overridden by accumulating enough data. The accumulation of commercially valuable user data is what increases — and at, the least, should indicate — market power. So, it is not surprising that the Commission's decision does not bode well with user privacy concerns because the idea of a competitive marketplace has devolved into four technology companies trading off, for the most part, the same data.

VII. WHAT DO THESE DECISIONS ENTAIL FOR PRIVACY? WHY ISN'T PRIVACY REGULATION, ON ITS OWN, ENOUGH?

Privacy regulation is both with and without foundation in the United States. On one hand, it is the right "to be let alone" that the late Justice Brandeis protected in his article, *The Right to Privacy*.[197] On the other, most privacy causes of action rely on other doctrines of law to receive defense, protection, and/or remedy, and this remedy, if granted, is often inadequate.[198]

This is inherently limiting. At its most basic level, the character of the common law both requires and relies on heavy doctrinal support to produce and guarantee strong, favorable outcomes to wronged citizens.[199] On an even more basic level, the character of the common law is to move slowly, which does not have much hope in matching the massive scale technology operates on.

State regulation would ideally provide a counterpart to the disadvantages of having little doctrinal support for modern notions of privacy in the common law. Yet, statutory remedies have only proven feeble against big tech companies.[200] The CCPA is mainly equipped to address the actual selling and transferring of data that connects to a user, but Big Tech only shares user data to third-parties with an attached pseudonym before placing the user in a targeting bucket. Google, for example, knows what users think because they tell it.[201] Every search is a communication in a two-

[197] *See generally* Brandeis & Warren, *supra* note 20.
[198] *See* Gasser, *supra* note 21.
[199] A problem with this when it comes to data protection and privacy, for example, is in data harm. *See supra* Section III and note 115 for a discussion on how data harm is not formally recognized, thereby calling a plaintiff's standing for a cause of action into question. The CCPA, too, may also limit a plaintiff's ability to bring forth a cause of action. *See supra* notes 37 and 88 and accompanying text.
[200] The CCPA is the strongest legislation protecting data privacy and regulation, but it has not resulted in major changes in the way that big tech companies conduct, control, or collect data. *See, e.g.*, Patience Haggin, *Facebook Won't Change Web Tracking in Response to California Privacy Law*, WALL ST. J. (Dec. 12, 2019), https://www.wsj.com/articles/facebook-wont-change-web-tracking-in-response-to-california-privacy-law-11576175345.
[201] *See* Caitlin Dewey, *Everything Google Knows About You (and How it Knows it)*, WASH. POST (Nov. 19, 2014, 4:07 AM), https://www.washingtonpost.com/news/the-intersect/wp/2014/11/19/everything-google-knows-about-you-and-how-it-knows-it/. *See also supra* Sections I and II.

way mirror that users are maybe only marginally aware of. And Google does with this information what every other *big* company does: it uses it to wield unprecedented power both in the market and in a citizen's daily life.[202] In addition to monopolizing ad revenue, it rewrites the freedom of press, governs the internet to the point where news agencies must collaborate with Google to have any traction, and bullies anybody who does not comply with their conditions, by providing subscriber and reader data, out of sight and out of search.[203] Google's share of the market is so large that it could even be argued AT&T acquired Time Warner as a defense to Google's increasing market power.[204]

VIII. DOJ AND FTC MERGER REVIEW CAN IMPLEMENT THIS CHANGE

If regulatory agencies were to recognize data as an indicator of market power, antitrust enforcement would be better off against the modern economy. Antitrust law is a rather recent phenomena that can and does deserve some level of restructuring in response to changes in the market, market structure, or consumer behavior.[205] No one assessment can survive the test of time when it comes to consumer behavior. Regulatory agencies are better off recognizing this. Congress is beginning to, since its recent Investigation of Competition in Digital Markets is one of the first in tens of years to address the magnitude of the concentration crisis.[206]

---

[202] "If you know who is looking at an ad, that ad space becomes more valuable." Dina Srinivasan, *How Digital Advertising Markets Really Work*, THE AM. PROSPECT (June 24, 2019), https://prospect.org/economy/digital-advertising-markets-really-work/.

Google's current market share in the search engine market is 92.47%. *See* Joseph Johnson, *Worldwide Desktop Market Share of Leading Search Engines from January 2010 to January 2021*, STATISTA (Feb. 10, 2021) https://www.statista.com/statistics/216573/worldwide-market-share-of-search-engines/#:~:text=Google%20has%20dominated%20the%20search,mobile%20devices%20and%20other%20ventures.

[203] When WSJ didn't comply with some Google regulations, it stopped showing WSJ articles in search results which significantly decreased WSJ's traffic. *See* Gerry Smith, *WSJ Ends Google Users' Free Ride, Then Fades in Search Results*, BLOOMBERG (June 5, 2017), https://www.bloomberg.com/news/articles/2017-06-05/wsj-ends-google-users-free-ride-then-fades-in-search-results.

[204] Stephen Moore, *Why the AT&T-Time Warner Merger Is a Win For Consumers*, N.Y. TIMES (June 13, 2018), https://www.nytimes.com/2018/06/13/opinion/att-time-warner-merger-good-consumers-antitrust.html.

[205] For a detailed look at the proposed methods of restructuring, *see supra* note 20.

[206] Press Release, H. Comm. on the Judiciary, House Judiciary Committee Launches Bipartisan Investigation into Competition in Digital Markets (June 3, 2019), https://judiciary.house.gov/news/press-releases/house-judiciary-committeelaunches-bipartisan-investigation-competition-digital. For the full report *see* H.R. Rep No. 117 (2020) https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf?utm_campaign=4493-519. Chairman David Cicilline spearheaded the investigation and continues to be a force against Big Tech in Congress. Press Release, Congressman David Cicilline (July 29, 2020) https://cicilline.house.gov/press-release/cicilline-opening-statement-big-tech-antitrust-hearing.

The investigation fully understands how data sways the market. As part of his opening statement on a series for 'Reviving Competition,' Chairman Cicilline noted that,

"Dominant platforms exploit their gatekeeper power to charge exorbitant fees, advantage their own products and services, impose oppressive contract terms, and *extract valuable data from the people and businesses that rely on them*.

In the meantime, what the DOJ and FTC can do is twofold. First, they can adopt new standards for measuring competition that reflect the modern marketplace. The amount of free to low-cost services provided by the biggest companies in the world should signal that no standard can be *solely and exclusively* based on pricing. By doing so, the DOJ and FTC invite more holistic and potentially multifactor investigations that would consider data and privacy concerns, and provide an answer to the zero-price market.[207]

Second, both agencies can understand data as an indicator of market power. Zero-price services are not free.[208] If they were, then there would be no harm to assess under a consumer welfare standard. These services are instead paid for by collecting, using, manipulating, and restructuring data.[209] This makes data a materialized social relation — potentially more valuable than a market good or natural resource. Tech companies have been able to multiply their revenue and share of the market because of an asset that antitrust agencies simply have not been equipped to understand or enforce, and that must be stopped. Considering data an indicator of market power would then reinvent consumer choice by repositioning tech companies that have taken advantage of this antitrust loophole.

It is no understatement to say the FTC alone has the potential to reshape the United States economy. Its broad jurisdiction over privacy, consumer protection, and antitrust laws gives it strong legal authority to define what unfair methods of competition are and how corporations should go

Over and over and over again, words like fear and hardship permeated concerns of businesses across the economic spectrum — app developers, innovators, and locally owned companies alike."
House Committee on the Judiciary, Subcommittee on Antitrust, Commercial, and Administrative Law, *Reviving Competition, Part 1: Proposals to Address Gatekeeper Power and Lower Barriers to Entry Online*, YouTube (Feb. 25, 2021), https://www.youtube.com/watch?v=eyvfYlxELv4&feature=emb_title.

[207] *See, e.g.*, LAWRENCE LESSIG, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD 12 (2001) ("[W]henever one says a resource is 'free,' most believe that a price is being quoted—free, that is, as in zero cost.").

[208] *See supra* note 24 and accompanying text.

[209] *Id.*

about their daily business.[210] Instead of being tougher on corporations, however, the FTC has privileged settlements and consent decrees over policy.[211]

Data protection and privacy are important, but are often seen as policy concerns that are too big to tackle. Many of their core issues, however, need not be resolved directly. A competitive marketplace is meant to insure against monopolists, encourage innovation, underpin middle-class growth, and protect consumers. Part of protecting consumers is protecting privacy, especially amidst merger reviews that result in both a less competitive marketplace by putting more data in the hands of a few and even more compromised consumer privacy. With proper antitrust enforcement, the problem will not go away, but it may, at the least, lose to the market.

[210] The FTC is the only regulatory agency currently enforcing privacy protections predominantly because "no other regulator had clear authority in the area." WILLIAM MCGEVERAN, PRIVACY AND DATA PROTECTION LAW 205 (2016). The majority of its authority comes from Section 5 of the FTC Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45(a)(1). "[Congress] explicitly considered, and rejected, the notion that it reduce the ambiguity of the phrase 'unfair methods of competition' by enumerating the particular practices to which it was intended to apply." FTC v. Sperry & Hutchinson Co., 405 U.S. 233, 239-40 (1972) (citing S. Rep. No. 63-597, at 13 (1914)).
The FTC, for example, can take action against predatory lending through almost the click of a button. It did so with merchant cash advances. *See* Press Release, Fed Trade Comm'n, FTC Alleges Merchant Cash Advance Provider Overcharged Small Businesses Millions (Aug. 3, 2020) (on file with author), https://www.ftc.gov/news-events/press-releases/2020/08/ftc-alleges-merchant-cash-advance-provider-overcharged-small.
The FTC brings a majority of its cases under deception and typically settles with the company in question through a "consent decree," wherein the defendant's unfair or deceptive practices in its privacy policy, for example, are outlined and settled. *See, e.g.*, In re Snapchat, Inc., FTC Docket No. C–4501 (Dec. 23, 2014) (settling many issues regarding Snapchat's privacy policy, including its deceptive communication to users that their snaps "disappear forever," over a 20-year period). In order to preserve its resources, however, the FTC only brings these cases when the matter is arguably airtight. The Snapchat case, for example, ticked all the boxes because it involved a large company with millions of users and more serious harms since the app was often used to send sensitive materials like nudity, alcohol, or drugs. *See* MCGEVERAN at 225. But the FTC cannot afford to bring these cases anytime a user's privacy is compromised.

[211] Zoom, for example, was caught lying about its security practices and the FTC chose not to fine Zoom. *See* Susan Heavey & Nandita Bose, *Zoom to Enhance Security as Part of Proposed U.S. Settlement with Zoom*, REUTERS (Nov. 9, 2020), https://www.reuters.com/article/zoom-ftc/zoom-to-enhance-security-as-part-of-proposed-u-s-settlement-with-ftc-idUSKBN27P28I. Rohit Chopra, a Democrat on the Federal Trade Commission, vehemently dissented to this. *Dissenting Statement of Commissioner Rohit Chopra*, Regarding Zoom Video Communications Inc., Comm. File No. 1923167 (Nov. 6, 2020) https://www.ftc.gov/system/files/documents/public_statements/1582914/final_commissioner_chopra_dissenting_statement_on_zoom.pdf. Chopra has consistently pushed for more FTC enforcement — even attacking the addictiveness of Facebook's products — because "all too often, the government is too captured by those incumbents that use their power to dictate their preferred policies." *See also Dissenting Statement of Rohit Chopra*, In re Facebook Inc., Comm. File No. 1823109, at 2. ("Behavioral advertising generates profits by turning users into products, their activity into assets, their communities into targets, and social media platforms into weapons of mass manipulation.") https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf.

CONCLUSION

At this point of the Comment, it is clear why antitrust and privacy are not only related, but also, inseparable. Privacy regulation depends, to some extent, on the working relationship between agencies, the judiciary, and antitrust enforcement. Further, privacy regulation is inadequate without properly internalizing and embodying antitrust values and principles.

Antitrust law, then, must reflect the modern marketplace. The DOJ and FTC must allow for broader interpretations of 'substantially lessening competition' so to account for the influx of zero-pricing and concomitant data grabs. This is done by broadening or abandoning the price theory central to a consumer welfare analysis. When the analysis for competition is (1) broadened to accommodate for the new levers of the marketplace, which do not necessarily include prices, and (2) data is considered an indicator of market power, antitrust enforcement can begin a robust response to the new characters and behaviors of the modern economy.

Without data protection and privacy enshrined as a human right, privacy laws existentially rely on statutory causes of action and remedies. And while legislation can provide notable privacy protections, they cannot go far without attacking the problem at the root: the companies that are compromising individual privacy, and thus, economic freedom, competition, and innovation. That is where antitrust enforcement must step in to protect competition, consumer privacy, and consumer choice.