SUPRACOMPETITIVE PRIVACY

Gregory Day[1] & Abbey Stemler[2]

[1] Assistant Professor, University of Georgia, Terry College of Business, Courtesy Appoint, University of Georgia School of Law.
[2] Assistant Professor, Indiana University, Kelley School of Business; Consultant, World Bank Group; Affiliate, Ostrom Workshop.

The authors would like to thank those who contributed valuable comments and critiques at workshops hosted by the Fellows at the Berkman Klein Center for Internet & Society at Harvard University, the Northeast Privacy Scholars Workshop at Fordham University School of Law, the Law and Ethics of Big Data colloquium at Babson College, and Southeast Academy of Legal Studies in Business Conference. Specials thanks to Rory Van Loo, Devin Desai, Kevin Werbach, Mike Schuster, and Tim Samples. We would also like to thank our research assistants for their dutiful work including William Bush and Taylor Samuels of the University of Georgia School of Law, as well as Jonathan Stuart of the University of Georgia Terry College of Business. Further, we are pleased that an earlier version of the manuscript won MBAA International's Distinguished Paper Award on a blind peer review basis.

SUPRACOMPETITIVE PRIVACY

ABSTRACT

One of the chief anticompetitive effects of modern business lies in antitrust's blind spot. Platform-based companies ("platforms") have innovated a business model whereby they offer consumers "free" and low-priced services in exchange for their personal information. With this data, platforms can design products, target consumers, and sell such information to third parties. The problem is that platforms can inflict greater costs on users and markets in the form of lost privacy than efficiencies generated from their low prices. Consumers, as examples, spend billions of dollars annually to remedy privacy breaches and, alarmingly, participate unwittingly in experiments designed to manipulate their behaviors, compromising human agency. But because antitrust law uses consumer prices to measure welfare, platforms and privacy injuries have avoided antitrust scrutiny.

Using an original dataset and quantitative methods, we show that insufficient competition enables platforms to capture the economic benefits of data while externalizing the costs of protecting it. As we find, consumers demand privacy yet firms in monopolized markets have powerful incentives to shift the costs of protecting privacy onto society. To reduce the rate of privacy breaches, we show that increasing competition would 1) allow users to punish offending firms, 2) disseminate information about the true costs of privacy, and 3) introduce more secure services into the market. As such, because monopoly power encourages firms to disregard the privacy demands of users, antitrust must evolve to recognize that the costs of inadequate privacy can degrade consumer welfare more than artificially high prices.

****

Introduction

At first blush, Google's[3] acquisition of the "smart" thermostat manufacturer, Nest Labs, was astonishing as it was perplexing.[4] Observers were initially puzzled by Google's motivation. For a company synonymous with its search engine, email platform, and technology services, why had Google sought to enter the thermostat market?[5] Perhaps even more interesting, why did

[3] Now organized under the umbrella company Alphabet. Larry Page, *G Is for Google*, ALPHABET, https://abc.xyz/ (last visited Oct. 9, 2018). Throughout this Article we will refer Alphabet and its subsidiaries as "Google."

[4] *See generally* James Walker, *Google to Merge with Alphabet Smart Home Subsidiary Nest*, DIGITAL J. (Feb. 8, 2018), http://www.digitaljournal.com/tech-and-science/technology/google-to-merge-with-alphabet-smart-home-subsidiary-nest/article/514
340 (describing the acquisition).

[5] *See Google's Strategy Behind the $3.2 Billion of Acquisition of Nest Labs*, FORBES (Jan. 17, 2014, 2:57 PM), https://www.forbes.com/sites/greatspeculations
/2014/01/17/googles-strategy-behind-the-3-2-billion-acquisition-of-nest-labs/#4e42bef01
d45 (attempting to explain why Google purchased Nest).

Google spend *$3.2 billion* to do so?[6] The answers to both questions concern data and its collection.[7]

It is hard to over overstate the modern value of data. Platform-based technology firms ("platforms") thrive by attracting users with "free"[8] and low-priced services, enabling these companies to mine, exploit, and market their users' data to third parties.[9] Google, for example, captures personal information from Gmail accounts[10] while Uber can track a user's' activities even after one has *deleted* the company's application ("app").[11] The deal offered by platforms is this: individuals may enjoy cheap services in exchange for their personal information, which is turned into revenue. Google's acquisition of Nest thus makes sense considering the volumes of user data collected by Nest and purchased by Google.[12]

Platforms can, however, inflict greater costs on consumers in the form of lost privacy than efficiencies generated by low prices.[13] The issue is that platforms enjoy data's economic potential without bearing the full costs of protecting privacy. Society instead suffers deadweight loss, as consumers, companies, and governments spend billions of dollars annually to redress identity

---

[6] Lance Whitney, *Google Closes $3.2 Billion Purchase of Nest*, CNET (Feb. 12, 2014, 5:00 AM), https://www.cnet.com/news/google-closes-3-2-billion-purchase-of-nest/.

[7] Casey Johnston, *What Google Can Really Do with Nest, or Really, Nest's Data*, ARS TECHNICA (Jan. 15, 2014, 7:30 PM), https://arstechnica.com/information-technology/2014/01/what-google-can-really-do-with-nest-or-really-nests-data/; Leo Kelion, *Google-Nest Merger Raises Privacy Issues*, BBC NEWS (Feb. 8, 2018), https://www.bbc.com/news/technology-42989073; Rakesh Sharma, *Google's Acquisition of Nest and Your Privacy*, FORBES (Jan. 13, 2014, 9:07 PM), https://www.forbes.com/sites/rakeshsharma/2014/01/13/googles-acquisition-of-nest-and-your-privacy/#2e081a843c33.un.

[8] *See generally* John Newman, *The Myth of Free*, 86 GEO. WASH. L. REV. 513, 524-26 (2018) (explaining the economics of "free").

[9] *See generally* Agnieszka McPeak, *Disappearing Data*, 2018 WIS. L. REV. 17, 18–19 (2018) (explaining the use and exploitation of data by technology firms). *See also* Kevin Granville, *Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens*, N.Y. TIMES (Mar. 19, 2018), https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html.

[10] *See* Todd Haselton, *How to Find Out What Google Knows About You and Limit the Data It Collects*, CNBC (Nov. 20, 2017, 11:50 AM), https://www.cnbc.com/2017/11/20/what-does-google-know-about-me.html.

[11] Jefferson Graham, *Can an App Really Track You After You Delete It?*, USA TODAY (Apr. 26, 2017, 8:16 AM), https://www.usatoday.com/story/tech/talkingtech/2017/04/26/can-app-really-track-you-after-you-delete/100864168/.

[12] Bernard Marr, *Google's Nest: Big Data and the Internet of Things in the Connected Home*, FORBES (Aug. 5, 2015, 10:52 AM), https://www.forbes.com/sites/bernardmarr/2015/08/05/googles-nest-big-data-and-the-internet-of-things-in-the-connected-home/#2d675bf03bac.

[13] *See, e.g.*, Dan Kedmey, *Hackers Leak Explicit Photos of More Than 100 Celebrities*, TIME (Sept. 1, 2014), http://time.com/3246562/hackers-jennifer-lawrence-cloud-data/ (explaining data breaches severely embarrassed over a hundred celebrities); Tom Risen, *Study: Hackers Cost More Than $445 Billion Annually*, U.S. NEWS, https://www.usnews.com/news/articles/2014/06/09/study-hackers-cost-more-than-445-billion-annually (last visited July 15, 2018).

theft[14] and data breaches.[15] Enabled by inadequate security, hackers alone impose between $375 to $500 billions of damages per year.[16] More subtly yet perhaps more importantly, platforms are able to manipulate their users' behaviors, prompting observers to remark that technology firms are compromising human agency.[17] In fact, this landscape qualifies as market failure—a condition whereby the market systemically encourages actors to engage in inefficient behaviors[18]—as platforms have little incentive to bolster data security as long as they can avoid scrutiny.

We demonstrate that "supracompetitive privacy" is the root of the problem. The term "supracompetitive" almost always refers to supracompetitive pricing—defined as the high prices a monopolist can charge in the absence of competition[19]—which is the primary injury that antitrust law condemns.[20] Our research shows that, like prices, privacy relies on competition. Because many platforms such as Facebook and Google compete in markets devoid of meaningful competition,[21] they enjoy insulation from market forces which incentivizes them to pass the burdens of protecting privacy onto users. Disguising this market failure is the "free" price of platform services—i.e., the

[14] *See* Hunt Allcott & Matthew Gentzkow, *Social Media and Fake News in the 2016 Election*, 31 J. ECON. PERSPECTIVES 211 (2017); Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, GUARDIAN (Mar. 17, 2018, 6:03 PM), https://www.theguardian.com /news/2018/mar/17/cambridge-analytica-facebook-influence-us-election; Danielle Kurtzleben, *Did Fake News on Facebook Help Elect Trump? Here's What We Know*, NPR (Apr. 11, 2018, 7:00 AM), https://www.npr.org/2018/04/11/601323233/6-facts-we-know-about-fake-news-in-the-2016-election (quoting Facebook's CEO Mark Zuckerberg's statement at a joint Senate Committee: "[I]t's clear now that we didn't do enough to prevent these tools from being used for harm as well. That goes for fake news, foreign interference in elections, and hate speech, as well as developers and data privacy. We didn't take a broad enough view of our responsibility, and that was a big mistake. It was my mistake, and I'm sorry. I started Facebook, I run it, and I'm responsible for what happens here.").

[15] *See, e.g.*, Nate Lord, *Infographic: Is Security Spending Proportional to the Data Breach Problem?* DIGITAL GUARDIAN (July 27, 2017), https://digitalguardian.com /blog/infographic-security-spending-proportional-data-breach-problem.

[16] *See* Risen, *supra* note 13.

[17] *See infra* Part II.2.B (discussing the contours of decisional privacy).

[18] Market failure is an economic condition arising when market participants avoid paying the full costs of their conduct. Tamara R. Piety, *Market Failure in the Marketplace of Ideas: Commercial Speech and the Problem That Won't Go Away*, 41 LOY. L.A. L. REV. 181, 190, 203 (2007) ("Economists generally use the term "market failure" to describe conditions where the operation of the market fails to produce optimal (i.e., "efficient") distributions of goods, services, or outcomes.").

[19] CAE Inc. v. Gulfstream Aerospace Corp., No. CV 15-924-LPS, 2017 WL 3279122, at *6 (D. Del. July 28, 2017) (indicating that restricted output enables the monopolist to charge supracompetitive prices).

[20] *See In re* Aggrenox Antitrust Litig., 199 F. Supp. 3d 662, 664–65 (D. Conn. 2016) ("That 'power to charge prices higher than the competitive level' is market power, which is an essential element of antitrust cases… The exclusion of rivals will typically go hand-in-hand with market power, but it is the ability to charge supracompetitive prices that is the *sine qua non* of market power.").

[21] *See* Allison Schrager, *A Nobel-Winning Economist's Guide to Taming Tech Monopolies*, QUARTZ (June 27, 2018), https://qz.com/1310266/nobel-winning-economist-jean-tirole-on-how-to-regulate-tech-monopolies/ (discussing how tech monopolies naturally arise).

low prices create the illusion of vigorous competition.[22] If technology markets were sufficiently competitive, as we explain, firms would enhance their privacy safeguards to vie for users.[23]

Given that insufficient competition can enable privacy breaches, it is problematic that the laws meant to protect consumers from the ill effects of uncompetitive markets—i.e., the antitrust laws—are wholly unable to remedy privacy injuries. To explain this blind spot, platform and tech firms have abandoned retail prices as their chief means of competition, creating fundamental problems for antitrust enforcers.[24] Because antitrust law is solely meant to promote the economic interests of consumers,[25] antitrust courts have typically conditioned liability on evidence that the defendant raised prices (i.e., supracompetitive prices) or restricted output (which produces

---

[22] *See* David N. Cicilline & Terrell McSweeny, *Competition Is At the Heart of Facebook's Privacy Problem*, WIRED (Apr. 24, 2018, 8:00 AM), https://www.wired.com/story/competition-is-at-the-heart-of-facebooks-privacy-problem/.

[23] A review of the literature revealed limited scholarship on the intersection of privacy and antitrust. *See, e.g.*, ARIEL EZRACHI & MAURICE E. STUCKE, VIRTUAL COMPETITION: THE PROMISE AND PERILS OF THE ALGORITHM-DRIVEN ECONOMY (2016); MARK R. PATTERSON, ANTITRUST IN THE NEW ECONOMY: GOOGLE, YELP, LIBOR, AND THE CONTROL OF INFORMATION (2017); MAURICE E. STUCKE & ALLEN P. GRUNES, BIG DATA AND COMPETITION POLICY (2016); Pamela Jones Harbour & Tara Isa Koslov, *Section 2 in a Web 2.0 World: An Expanded Vision of Relevant Product Markets*, 76 ANTITRUST L.J. 769 (2010); Nathan Newman, *The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google*, 40 WILLIAM MITCHELL L. REV. 849 (2014); Frank Pasquale, *Privacy, Antitrust, and Power*, 20 GEO. MASON L. REV. 1009 (2013); Frank Pasquale, *When Antitrust Becomes Pro-Trust: The Digital Deformation of U.S. Competition Policy*, CPI ANTITRUST CHRON. 1 (May 2017), https://www.competitionpolicyinternational.com/wp-content/uploads/2017/05/CPI-Pasquale.pdf. It provides an overview of antitrust law in the context of data-driven industries and focuses in part on privacy implications. Most articles about the relationship between privacy and antitrust argue that antitrust law is not the appropriate vehicle for addressing privacy concerns. *See* James C. Cooper, *Privacy and Antitrust: Underpants Gnomes, the First Amendment, and Subjectivity*, 20 GEO. MASON L. REV. 1129 (2013) (arguing that privacy concerns are inappropriate for inclusion in an antitrust analysis); Geoffrey A. Manne & Raymond Sperry, *The Problems and Perils of Bootstrapping privacy and Data into an Antitrust Framework*, CPI ANTITRUST CHRON. 4 (May 29, 2015); Maureen K. Ohlhausen & Alexander P. Okuliar, *Competition, Consumer Protection, and The Right [Approach] to Privacy*, 80 ANTITRUST L.J. 121, 153 (2015) ("using the modern antitrust laws, which are empirically focused on economic efficiency, to remedy harms relating to normative concerns about information privacy contradicts the specialized nature of these laws and risks distorting them in ways that would leave both the law and consumers worse off"); Randal C. Picker, *Competition and Privacy in Web 2.0 and the Cloud*, 103 NW. U. L. REV. COLLOQUY 1 (2008) (arguing that limits on the sharing of user data would lead to increased market concentration of platforms); D. Daniel Sokol & Roisin E. Comerford, *Antitrust and Regulating Big Data*, 23 GEO. MASON L. REV. 1129 (2016) (arguing that antitrust law is "ill suited as the institutional choice" for addressing privacy concerns and that the "scholarly case for such harm has not yet been adequately established"); David S. Evans & Richard Schmalensee, *The Antitrust Analysis of Multi-Sided Platform Businesses*, (Nat'l Bureau of Econ. Research, Working Paper No. 18783 2013), http://www.nber.org/papers/w18783.pdf (discussing how traditional approaches to antitrust laws do not work for two-sided marketplaces, i.e. platforms). Several economists have written on the relationship between platforms and antitrust, but none have directly addressed the impacts on privacy. *See* Nicholas Economides, *Antitrust Issues in Network Industries*, *in* THE REFORM OF EC COMPETITION LAW 345 (Ioannis Lianos & Ioananis Kokkoris eds., 2008); Rob Frieden, *The Internet of Platforms and Two-Sided Markets: Implications for Competition and Consumers* (2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3051766; *see also* Kenneth A. Bamberger & Orly Lobel, *Platform Market Power*, 32 BERK. TECH. L.J. 1051 (2017).

[24] *See* Lina M. Khan, *Amazon's Antitrust Paradox* (note), 126 YALE L.J. 710 (2017).

[25] *Antitrust Laws and You*, DEP'T OF JUST. ANTITRUST DIV., https://www.justice.gov/atr/antitrust-laws-and-you (last accessed July, 16, 2018) ("Essentially, [the antitrust] laws prohibit business practices that unreasonably deprive consumers of the benefits of competition, resulting in higher prices for products and services."); *see also In re* Cardizem CD Antitrust Litig., 332 F.3d 896, 904 (6th Cir. 2003) ("[T]he very purpose of antitrust law is to ensure that the benefits of competition flow to purchasers of goods affected by the violation.").

supracompetitive prices).[26] The issue is that, since the courts have yet to recognize privacy as a quality that antitrust may protect, the cheap prices offered by platforms have insulated them from antitrust scrutiny.[27] Evidently, antitrust's architects never foresaw an era when firms could render anticompetitive effects without charging prices.

We employ novel empirical methods to demonstrate that antitrust law should condemn anticompetitive practices leading to inadequate privacy.[28] This is because heightened competition would 1) allow users to punish offenders, 2) disseminate information about the true costs of data breaches, and 3) introduce more secure products and services into the stream of commerce. But so long as tech firms enjoy antitrust immunity for lapses in privacy, we can expect them to continue to externalize the costs of protecting data. To make this case, we test the relationship between monopoly power (using data from the Herfindahl-Hirshman Index[29]) and privacy breaches (based on data provided by IBM). The results show that consumers punish firms for costly data breaches *except* in concentrated markets. Consumers do, it seems, demand heightened privacy yet firms in concentrated industries—e.g., most platform markets—are able to resist pressures to supply it. Because monopolists can better survive a privacy breach, we demonstrate that market power encourages firms to shift the economic costs of protecting privacy onto consumers, which *should* implicate antitrust enforcement. Our argument is not that all tech giants are violating the Sherman Antitrust Act ("Sherman Act"),[30] but rather that antitrust law should consider privacy lapses to entail an actionable injury, especially as firms abandon prices as their primary means of competition.

This Article also contributes to the burgeoning debate over antitrust's goals. Scholarship and activists[31] have begun to question whether the Sherman Act should be expanded beyond its

---

[26] Ginzburg v. Mem'l Healthcare Sys., Inc., 993 F. Supp. 998, 1026 (S.D. Tex. 1997) ("To determine the legality of a restraint under the rule of reason, the plaintiff must show that the defendant's actions amounted to a conspiracy against the market—a concerted attempt to reduce output and drive up prices or otherwise reduce consumer welfare.") (alterations in original).

[27] *See generally id.* (providing an exhaustive review and analysis of which types of effects are considered anticompetitive under the antitrust laws without once mentioning privacy). There are pockets of government where support for the proposition that privacy concerns should be, at least in part, be addressed by antitrust law. *See also* Senator Herb Kohl's comments ("The antitrust laws were written more than a century ago out of the concern with the effects [sic] of undue concentrations of economic power for our society as a whole, and not just merely their effects on consumers' pocketbooks. No one concerned with antitrust policy should stand idly by if industry consolidation jeopardizes the vital privacy interests of our citizens so essential to our democracy") in Behavioral Advertising: Tracking, Targeting, and Technology: Town Hall Before the FTC (Oct. 18, 2007) (testimony of Peter Swire, Professor, Moritz College of Law of the Ohio State University), http://www.americanprogress.org/issues/regulation/news/2007/10/19/3564/protecting-consumers-privacymattersin-antitrust-analysis/.

[28] John M. Newman, *Antitrust in Zero-Price Markets: Foundations*, 164 U. PA. L. REV. 149, 160 (2015) (explaining that courts and scholars have considered zero-price goods to be "de facto" immune from antitrust scrutiny because antitrust's focus concerns price competition and thus whether the challenged act has rendered above market pricing).

[29] Jennifer E. Gladieux, *Towards A Single Standard for Antitrust: The Federal Trade Commission's Evolving Rule of Reason*, 5 GEO. MASON L. REV. 471, 523 n.367 (1997) (explaining the Herfindahl-Hirshman Index).

[30] 15 U.S.C. §§ 1–7 (1890).

[31] Sandeep Vaheesan, *The Evolving Populisms of Antitrust*, 93 NEB. L. REV. 370, 409–10 (2014) (discussing the rise of antitrust's populism); *see also* Brian Beutler, *How Democrats Can Wage War on Monopolies—And Win*, NEW REPUBLIC (Sept. 16, 2017), https://newrepublic.com/article/144675/democrats-elizabeth-warren-can-wage-war-monopolies-and-win.

dominant scope of promoting competitive prices.[32] With the rise of breached privacy and other social harms, the debate has concerned whether enforcement should condemn practices that, as examples, lead to political injuries, social inequality, and other harms caused by powerful monopolists. We contribute to this literature by confirming that antitrust is poorly equipped to remedy the anticompetitive effects of modern business. In doing so, this Article is likely the first to offer evidence that privacy is a function of competition and that the resulting costs are economic. We also provide scholarly support for the belief held by certain authorities that antitrust's relationship with privacy must be examined—e.g., the decision in February 2019 by the German competition authority to condemn Facebook's use of data.[33] So in shedding economic light on privacy, and given the obsolescence of conventional pricing, we contribute to the greater debate by demonstrating the ways that mounting concerns such as privacy should fit into antitrust's framework.

This Article proceeds in four parts. The first Part explores the unique nature of platforms and other online technology services. It explains that tech firms have found innovative ways of commercializing data. Because platforms offer consumers low-priced goods while harvesting data within a web of networks, their monopoly power can expand without detection. Part II explores the extent to which the commercialization of user information generates economic and political costs in the form of lost privacy. This discussion canvasses the resources spent on protecting one's privacy before and following a breach, as well as the costs levied on decisional privacy.

Part III demonstrates that the cost of inadequate privacy is attributable to uncompetitive markets. Using a novel empirical treatment, it shows that consumers tend only to punish companies for privacy breaches when those firms exist in uncompetitive markets. In such a situation, the monopolist lacks incentives to use data cautiously. Since antitrust is the chief body of law intended to remedy market failure caused by uncompetitive markets, we assert that antitrust should take into account the costs of privacy rendered by the exploitation of data. Part IV discusses the greater implications of our research, including privacy invasions by technology companies when working for the government, merger policy, and avenues for future research.

I. The Unique Commercial Nature of Technology Platforms

Platform companies generate revenue in fundamentally different ways than traditional companies. Instead of charging retail prices for goods and services,[34] platforms facilitate exchanges between two or more groups, enabling them to harvest data from these interactions. The popularity of this business model is attributable to the ease by which platforms accrue and maintain

[32] *See, e.g.*, Khan *supra* note 24 at 126 (arguing that antitrust must acknowledge more anticompetitive effects that prices and output).

[33] Natasha Singer, *Germany Restricts Facebook's Data Gathering*, N.Y. TIMES (Feb. 7, 2019), https://www.nytimes.com/2019/02/07/technology/germany-facebook-data.html ("Authorities in Germany and some other European countries contend that Facebook has unfairly used its leverage to freely collect details about users on millions of third-party sites that use… Facebook Pixel. In doing so, the German agency's ruling is advancing a larger antitrust argument: that a tech company's abuse of its market dominance to amass information about and profile its users can amount to a kind of data coercion.").

[34] Alex Moazed, *Platform Business Model-Definition: What is it: Explanation*, APPLICO (May 1, 2016), https://www.applicoinc.com/blog/what-is-a-platform-business-model/.

monopoly power.[35] This Part reviews the dominance of the leading platforms and their business models in order to explain why platform technology is especially prone to monopolization.

A. The Dominant Platforms and Their Businesses

The market capitalization of the top twenty platforms—$6 trillion—exceeds a quarter of the U.S. economy,[36] yet the largeness of these platforms is far from their greatest distinguishing characteristic. Principally, platforms have revolutionized business by abandoning retail prices as their competition's lodestar in favor of data harvesting, which entails offering below-cost or even free services meant to gather the greatest number of users. This model contrasts with previous generations when the nature of competition pressured firms into lowering their goods' prices to the marginal cost of production. Making the platforms' model viable, they surveille their user's interactions with itself and other users to generate data—recording every click, swipe, and choice—contrary to how conventional venues such as shopping malls enabled people to purchase goods with relative anonymity.[37] A platform can even, depending upon its privacy policy, observe users who have ceased engaging the network, as software may continuously run in a device's background.[38] Platforms can also capture data after one has deleted the app from her device.[39]

To provide context to big data, consider the revenue, users, and business models of the leading platforms:

Amazon. When Jeff Bezos started Amazon in 1994, he sought to create a more convenient process to purchase books.[40] From this narrow focus, Amazon grew into the world's largest store—worth more than Walmart, Target, Macy's, Costco, and Kohls combined.[41] Today, Amazon controls roughly 50% of the e-commerce market, claiming more Amazon Prime subscribers in the

---

[35] For a discussion on data harvesting, *see* Julie E. Cohen, *Law for the Platform Economy*, 51 U.C. DAVIS L. REV. 133, 160 (2017).

[36] Jeff Desjardins, *Tech's 20 Largest Companies Are Based in 2 Countries*, BUSINESS INSIDER (July 9, 2018), https://www.businessinsider.com/techs-20-largest-companies-are-based-in-2-countries-2018-7.

[37] Ryan Calo & Alex Rosenblat, *The Taking Economy: Uber, Information, and Power*, 117 COLUM. L. REV. 1623 (2017); Charlie Warzel, *Facebook Has Had Countless Privacy Scandals. But This One Is Different*, BUZZFEED (Mar. 26, 2018, 5:46 PM), https://www.buzzfeed.com/charliewarzel/why-facebooks-data-scandal-just-wont-quit?utm_term=.sc0kmGLRae#.ubq95Ole3z ("Every movement you make online—and even where you move about in the world—is fastidiously catalogued, analyzed, and ultimately sold").

[38] Note there have also been many reported violations of privacy policies. *See generally* Fox Van Allen, *Study Finds Nearly Half of iOS Apps Violate Apple's Privacy Policy*, TIME (June 26, 2013), http://techland.time.com/2013/06/26/study-finds-nearly-half-of-ios-apps-violate-apples-privacy-policy/ (noting that almost half of iOS apps used Unique Device Identifiers (UDIDs) as a way of identifying users for advertisements in violation of Apple's privacy policy).

[39] *See* Kate Conger, *Uber Responds to Report That It Tracked Devices After Its App Was Deleted*, TECHCRUNCH (Apr. 23, 2017), https://techcrunch.com/2017/04/23/uber-responds-to-report-that-it-tracked-users-who-deleted-its-app/.

[40] Shah Mohammed, *How Did Amazon Build Its 'Sustainable Competitive Advantage'?* (May 28, 2018), https://medium.com/@shahmm/how-did-amazon-build-its-sustainable-competitive-advantage-88cfee7fe2c8.

[41] Jeff Bukhari, *Amazon Is Worth More Than Walmart, Costco, and Target Combined*, FORTUNE (Apr. 5, 2017), http://fortune.com/2017/04/05/amazon-walmart-costco-target-market-cap/.

United States than gun owners.[42] As this consumer base expands,[43] observers have remarked that Amazon has "deeper penetration into the private lives and desires of consumers than any other company."[44]

Explanations for Amazon's dominance include the seamless experience that Amazon provides consumers through its search functions, distribution system, and data analytics. Amazon has, perhaps more so than its rivals, effectively designed products to capture personal information so as to target products to consumers. For example, in addition to Amazon's knowledge of shopping habits gleaned from its online interface, Amazon created the electronic personal assistant, Alexa, which employs voice recognition technology to accommodate user requests ("Alexa, add butter to my shopping list," "Alexa, please play the most popular Elvis Presley song."). With this technology, Amazon captures and studies the personal, social, and political preferences[45] of the six million Americans who have purchased an Alexa.[46]

In fact, Amazon has introduced additional items to build off of Alexa's popularity, including the Echo Look. This product is equipped with a camera and microphone so that users may submit pictures of themselves to receive fashion advice—and shopping suggestions.[47] As one commentator opined, "[i]t seems absurd that people would bring a camera and microphone, connected to an online store, into their bedroom. The potential for abuse is unmistakable."[48] So among its other devices, Alexa and Echo Look demonstrate Amazon's ability to persuade consumers to feed their personal information into Amazon's devices and thus algorithms.

Facebook. In terms of social networking platforms, Facebook is without a peer. Roughly 1.5 billion of the earth's 7.5 billion people use the platform on a *daily* basis with the average person spending thirty-five minutes per day on the platform (this number grows considerably if one

---

[42] Ingrid Lunden, *Amazon's Share of the US E-Commerce Market Is Now 49%, or 5% of All Retail Spend*, TECHCRUNCH (2017), https://techcrunch.com/2018/07/13/amazons-share-of-the-us-e-commerce-market-is-now-49-or-5-of-all-retail-spend/. Roughly thirty percent of the US population owns a gun, and sixty-four percent have Amazon Prime. SCOTT GALLOWAY, THE FOUR: THE HIDDEN DNA OF AMAZON, APPLE, FACEBOOK, AND GOOGLE 4 (2018).

[43] Amazon's online business is growing at more than twenty percent each year. Louis Columbus, *10 Charts That Will Change Your Perspective on Amazon Prime's Growth*, FORBES (Mar. 4, 2018), https://www.forbes.com/sites/louiscolumbus/2018/03/04/10-charts-that-will-change-your-perspective-of-amazon-primes-growth/#54a3613c3fee. Eighty percent of online growth in the U.S. over the last few years can be attributed to Amazon. Shep Hyken, *Sixty- Four Percent of US Households Have Amazon Prime*, FORBES (Jun. 17, 2017), https://www.forbes.com/sites/shephyken/2017/06/17/sixty-four-percent-of-u-s-households-have-amazon-prime/#1971bb004586.

[44] GALLOWAY, *supra* note 42, at 30.

[45] Larry Greenmeier, Alexa, *What Are You Doing with My Family's Personal Information*, SCIENTIFIC AM. (Jan. 15, 2018), https://www.scientificamerican.com/article/alexa-what-are-you-doing-with-my-familys-personal-info/ (describing the information that Amazon can harvest from Alexa).

[46] Kevin Murname, *Reports Claim that 16% of Adults in the US Owns Amazon's Echo or Google's Home*, FORBES (Jan. 13, 2018, 8:00 AM), https://www.forbes.com/sites/kevinmurnane/2018/01/13/report-claims-that-16-of-adults-in-the-us-own-amazons-echo-or-googles-home/#7844419a78d8.

[47] Jon Markman, *Amazon Using AI, Big Data to Accelerate Profits*, FORBES (June 5, 2017, 9:39 AM), https://www.forbes.com/sites/jonmarkman/2017/06/05/amazon-using-ai-big-data-to-accelerate-profits/#769788c46d55.

[48] *Id.*

includes the amount of time spent on its subsidiaries, Instagram and WhatsApp).[49] Embellishing Facebook's market share, as users interact with the platform, it collects nuanced information about their preferences, friends, and locations.[50] Indeed, by exploiting data and network effects,[51] Facebook has emerged as the dominant social network,[52] generating over $40 billion of revenue in 2017.[53]

Google. Inspired by bibliometrics as well as its ranking system for academic articles, Larry Page and Sergey Brin created an algorithm to organize search results, PageRank.[54] From this start, Google now accounts for around ninety percent of the world's searches through its various portals (Google Search, Google Image Search, YouTube, and Google Maps).[55] In 2016, Google earned profits of over $20 billion as well boosted its cash flow by 23 percent.[56] These revenue sources have enabled Google to not only acquire competitors but also build an infrastructure featuring data centers and fiber optic cables connecting the world.[57] Furthering its market power, Google has successfully integrated into daily lives by introducing lines of hardware, including Nest, Google Home, and Chromecast.[58]

Uber. Among ridesharing platforms, Uber reigns supreme with a 77% share of the market and valuation in the hundreds of billions.[59] Although not the original ridesharing platform, Uber pioneered the prioritization of growth over profits, making end-runs around regulations.[60] Perhaps more salient is the manner in which Uber collects user data to perfect its interface as well as increase consumer satisfaction. For example, Uber experiments with drivers to enhance their

---

[49] David Cohen, *How Much Time Will the Average Person Spend on Social Media During their Life?*, ADWEEK (May 22, 2017), https://www.adweek.com/digital/mediakix-time-spent-social-media-infographic/.

[50] Sometimes, Facebook tracks user information even after they log off the platform. GALLOWAY, *supra* note 42, at 104.

[51] See *infra* Part II.3.

[52] Facebook along with Google absorbs 63% of all revenue from online advertising. Greg Ip, *The Antitrust Case Against Facebook, Google and Amazon*, WALL ST. J. (Jan. 16, 2018, 11:52 AM), https://www.wsj.com/articles/the-antitrust-case-against-facebook-google-amazon-and-apple-1516121561. *See also* John Dudovskiy, *Facebook Business Strategy and Competitive Advantage*, RESEARCH METHODOLOGY (Jan. 3, 2017), https://research-methodology.net/facebook-business-strategy-and-competitive-advantage/.

[53] *Facebook's Revenue and Net Income from 2007 to 2018 (in Millions of Dollars)*, STATISTA (2019), https://www.statista.com/statistics/277229/facebooks-annual-revenue-and-net-income/ (last visited Feb. 9, 2019).

[54] John Battelle, *The Birth of Google*, WIRED (Aug, 1, 2005, 12:00 PM), https://www.wired.com/2005/08/battelle/.

[55] Ip, *supra* note 52.

[56] GALLOWAY, *supra* note 42, at 4.

[57] DataCenter Knowledge, *Google Data Center FAQ, Part 1*, https://www.datacenterknowledge.com/google-data-center-faq (last visited Feb. 13, 2019).

[58] Nikhil Dandekar also outlines five ways Google became dominant: its search speed, deep indexing, PageRank algorithm, simple interface, and query-specific snippets. *How Did Google Surpass All Other Search Engines*, MEDIUM (Mar. 8, 2017), https://medium.com/@nikhilbd/how-did-google-surpass-all-the-other-search-engines-8a9fddc68631.

[59] GALLOWAY, *supra* note 42, at 30 (2018). It also has a valuation of around $120 billion. Liz Hoffman, Greg Bensinger & Maureen Farrel, *Uber Proposals Value Company at $120 Billion in a Possible IPO*, WALL ST. J. (Oct. 16, 2018, 1:28 PM), https://www.wsj.com/articles/uber-proposals-value-company-at-120-billion-in-a-possible-ipo-1539690343?mod=hp_lead_pos1.

[60] Eric Biber et al., *Regulating Business Innovation as Policy Disruption: From the Model T to Airbnb*, 70 VAND. L. REV. 1561 (2017).

experience; one of its chief innovations included the use of economic incentives in the form of "surge pricing" to nudge drivers toward high demand areas.[61] With these techniques, Uber has accrued a critical mass of drivers and riders to draw even more users into the app.[62] The result is an efficient transportation service enjoyed by consumers at lower costs than traditional ride services.[63]

Other Players. Conventional firms have similarly embraced platform-business models. For example, a majority of Domino's employees work in the company's data analytics section, shifting Dominos from a brick and mortar pizza chain into a tech firm that happens to sell pizzas.[64] From Domino's pizza tracker to Twitter-enabled ordering (one may order a pizza by tweeting a pizza emoji to @dominos), technology has elevated Domino's into the top grossing pizza retailer.[65] Along the same lines, Netflix pivoted from its former life as a mail-order DVD company into its current format as the ubiquitous streaming platform, relying on data algorithms to model offerings to consumers. The point is that conventional firms are incorporating platform technology to surpass their tech-stagnant rivals.

B. Capturing and Extracting Value from Data

To explain data's commercial nature, as a starting point, firms can efficiently design and deliver products to consumers from information derived from the monitoring of their behaviors. For example, Netflix studies consumer preferences gleaned from its interface so that Netflix may not only tailor media recommendations to individual users, but also inform the creative direction of its own original content.[66] Airbnb tracks a consumer's location and preferred devices to target listings.[67] Uber's data analytics have likewise enabled it to undersell the taxi industry as well as

---

[61] Alex Rosenblat & Luke Stark, *Algorithmic Labor and Information Asymmetries: A Case Study of Uber's Drivers*, 10 INT'L J. COMM. 3758 (2016).

[62] DAVID S. EVANS & RICHARD SCHMALENSEE, MATCH MAKERS: THE NEW ECONOMICS OF MULTISIDED PLATFORMS (2016).

[63] *See* Shankar Vedantam & Maggie Penman, *This Is Your Brain on Uber*, NPR (May 17, 2016, 12:01 AM), https://www.npr.org/2016/05/17/478266839/this-is-your-brain-on-uber. Andrew J. Hawkins, *Uber Is Trying to Make You Forget that Surge Pricing Exists*, VERGE (June 23, 2016), http://www.theverge.com/2016/6/23/12017002/uber-surge-pricing-upfront-fare-app-update-announcement; Calo & Rosenblat, *supra* note 37.

[64] Bernard Marr, *Big Data-Driven Decision-Marking at Domino's Pizza*, FORBES (Apr. 6, 2016), https://www.forbes.com/sites/bernardmarr/2016/04/06/big-data-driven-decision-making-at-dominos-pizza/#4a75db222b8e; *see also* Nathaniel Meyersohn, *Why Domino's Is Winning the Pizza War*, CNN (Mar. 6, 2018, 7:55 AM), https://money.cnn.com/2018/03/06/news/companies/dominos-pizza-hut-papa-johns/index.html (explaining Domino's dominance).

[65] Adario Strange, *Domino's Will Now Let You Order Pizza through Twitter Via Emoji*, MASHABLE (May 13, 2015), https://mashable.com/2015/05/13/dominos-twitter-pizza-emoji/#szfQvn0PQmqP.

[66] Enrique Dans, *How Analytics Has Given Netflix the Edge Over Hollywood*, FORBES (May 27, 2018, 3:17 PM), https://www.forbes.com/sites/enriquedans/2018/05/27/how-analytics-has-given-netflix-the-edge-over-hollywood/#2307c8766b23 (reviewing Netflix's many commercial uses for data).

[67] David Nield, *All the Ways Your Smartphone and Its Apps Can Track You*, GIZMODO (Jan. 4, 2018, 12:27 PM), https://fieldguide.gizmodo.com/all-the-ways-your-smartphone-and-its-apps-can-track-you-1821213704.

innovate a self-driving car program,[68] generating $6.8 billion of revenue in the United States alone.[69]

Taking this a step further, by offering free services meant to attract hordes of users—e.g., Facebook enlists 2.5 *billion* users, while Twitter, Fortnite, and Snapchat claim 300, 200, and 200 million users, respectively—platforms can sell access to their clienteles, most simply, via advertising.[70] Estimates show that social media advertising revenue in the United States exceeded $23 billion in 2018.[71] Although Facebook's CEO and founder, Mark Zuckerberg, claimed before Congress in 2018 that Facebook does not sell data, which mirrors Google's position,[72] Facebook generates revenue by profiling users and then assisting advertisers in targeting them—essentially commercializing users without necessarily "selling" their data.[73]

It is, in fact, inaccurate to describe platforms as passive voyeurs. Certain platforms run experiments designed to predict or even manipulate their users' behaviors. In a concealed experiment, Facebook augmented voting behaviors by displaying lists of friends who had voted in an election.[74] The project provided a link for some users to find their polling places, accompanied by a button indicating "I Voted," and a sampling of profile pictures of friends who had already voted. A second group of users were shown the link to polling places and the "I Voted" button, though excluded the profile pictures. It found that users who received the added feature of their friends were 0.39% more likely to vote.[75] While this increase is a small percentage of the population, in light of Facebook's 180 million active U.S. users, it illustrates the ease by which platforms can manipulate elections and also human behavior.

---

[68] Kia Kokalitcheva, *Not Everyone Agrees on the Future of Uber Drivers When Self-Driving Cars Arrive*, FORTUNE (Oct. 15, 2016), http://fortune.com/2016/10/14/uber-driver-future-self-driving-cars/ (quoting Douglas Rushkoff "Uber right now has drivers doing R&D for a robotic self-driving car.").

[69] Peter Cohen et. al., *Using Big Data to Estimate Consumer Surplus: The Case of Uber* (Nat'l Bureau of Econ. Research, Working Paper No. 22627, 2016), http://www.nber.org/papers/w22627.pdf. Remarkably, this study was based on Uber offering a data set of almost fifty million individual observations to researchers. *Id. But see* Philadelphia Taxi Ass'n, Inc v. Uber Techs., Inc., 886 F.3d 332 (3d Cir. 2018).

[70] Josh Constine, *2.5 Billion People Use at Least One of Facebook's Apps*, TECHCRUNCH (2018); Jon Fingas, *'Fornite' Now Has Over 200 Million Players*, ENGADGET (Nov. 27, 2018), https://www.engadget.com/2018/11/27/fortnite-200-million-players/; Sara Salinas, *Instagram Stories Has Twice As Many Daily Users as Snapchat's Service—and It Now Has Background Music*, CNBC (June 28, 2018, 3:00 PM), https://www.cnbc.com/2018/06/28/instagram-stories-daily-active-users-double-snapchats.h
tml; Hamza Shaban & Craig Timberg, *Twitter's Stock Plunges After Reporting Drop In User Numbers*, WASH. POST (July 27, 2018), https://www.washingtonpost.com/technology/2018/07/27/twitters-monthly-users-fell-by-million-second-quarter-following-purge-fake-suspicious-accounts/?utm_term=.ac2bc5d594c4.

[71] Social Network Advertising Revenues in the United States from 2015 to 2018, STATISTA (2018), https://www.statista.com/statistics/271259/advertising-revenue-of-social-networks-in-the-us/.

[72] Google, *We Do Not Sell Your Personal Information to Anyone*, https://privacy.google.com/how-ads-work.html (last visited Sept. 16, 2018).

[73] Kaleigh Rogers, *Let's Talk About Mark Zuckerberg's Claim that Facebook 'Doesn't Sell Data'*, MOTHERBOARD (Apr. 22, 2018, 11:12 AM), https://motherboard.vice.com/en_us/article/8xkdz4/does-facebook-sell-data.

[74] Robert M. Bond et al., *A 61-Million-Person Experiment in Social Influence and Political Mobilization*, 489 NATURE 7415 (2012), http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3834737. *See also* Jonathan Zittrain, *Engineering an Election*, 127 HARV. L. REV. F. 335, 335 (2014) (arguing that "digital gerrymandering" could easily flip an election).

[75] Bond, *supra* note 74.

Further animating data's value, consider the recent prices paid for platforms in corporate mergers. Facebook bought WhatsApp, the messaging platform, for $20 billion[76] when the platform had less than $10.5 million in revenue and only 50 employees.[77] A sophisticated understanding of finance is unnecessary to realize that Facebook had primarily acquired WhatsApp's users and their personal information. Likewise, Apple purchased Shazam (a platform that identifies song, artist and album information playing in the open air) for $400 million, not for its song identification technology, but mostly for Shazam's trove of data about listener's music preferences.[78] And to rehash the acquisition of Nest, Google sought to create networks connecting household items such as refrigerators and thermostats, known as the Internet of Things ("IoT"), so that Google may commercialize data derived from seemingly mundane household behaviors.[79]

Once a platform develops a profitable model for commercializing data, the operation's magnitude can bolster its dominance. As the next section describes, natural and artificial barriers to entry further a platform's market power, increasing data's profitability.

C. From Pieces to Power

The unique nature of data enables platforms to insulate their market power from competition. Some of these barriers to entry may naturally arise, including networks effects and data advantages, though critics charge that some platforms embellish their lead using anticompetitive means. The following discussion explores the ability of platforms to draw insights into consumers and impede competition as they collect data.

Network effects—defined as the process of connecting two or more different groups (i.e. buyers and sellers)[80]—can enhance a platform's market power. The initial study of network effects

---

[76] David Gelles, *Facebook's $21.8 Billion WhatsApp Acquisition Lost $138 Million Last Year*, N.Y. TIMES (Oct. 28, 2014, 5:46 PM), https://dealbook.nytimes.com/2014/10/28/facebooks-21-8-billion-acquisition-lost-138-million-last-year/; Jay Yarow, *WhatsApp, Facebook's $22 Billion Acquisition, Did $10.2 Million In Revenue Last Year*, BUS. INSIDER (Oct. 28, 2014, 4:46 PM), http://www.businessinsider.com/whatsapp-facebooks-22-billion-acquisition-did-102-million-in-revenue-last-year-2014-10.

[77] David Rowan, *The Inside Story of Jan Koum and How Facebook Bought WhatsApp*, WIRED (May 1, 2018), https://www.wired.co.uk/article/whats-app-owner-founder-jan-koum-facebook.

[78] Tripp Mickle, *Apple Acquires Shazam and Its Song-Recognition App*, WALL ST. J. (Dec. 11, 2017, 2:22 PM), https://www.wsj.com/articles/apple-acquires-shazam-and-its-song-recognition-app-1513019568; Adam Satariano & Lizette Chapman, *Apple Buys Shazam to Boost Apple Music*, BLOOMBERG (Dec. 11, 2017, 12:15 PM), https://www.bloomberg.com/news/articles/2017-12-11/apple-buys-early-iphone-app-hit-shazam-to-boost-apple-music.

[79] Trefis Team, *Google's Strategy Behind the $3.2 Billion Acquisition of Nest Labs*, FORBES (Jan 17, 2014, 2:57 PM), https://www.forbes.com/sites/greatspeculations/2014/01/17/googles-strategy-behind-the-3-2-billion-acquisition-of-nest-labs/#42e378e21d45

[80] These characteristics have been revealed by scholars, regulators, and industry leaders. NICK SRNICEK, PLATFORM CAPITALISM (2017); JOHNATHAN TAPLIN, MOVE FAST AND BREAK THINGS: HOW FACEBOOK, GOOGLE, AND AMAZON HAVE CORNERED CULTURE AND UNDERMINED DEMOCRACY (2017); Martin Kenney & John Zysman, *The Rise of the Platform Economy*, ISSUES IN SCI. & TECH. 61 (2016), http://www.brie.berkeley.edu/wp-content/uploads/2015/02/Kenney-Zysman-The-Rise-of-the-Platform-Economy-Spring-2016-ISTx.pdf (arguing that the U.S. economy is reorganizing into a "digital platform economy" as platform owners gain more power and control); Dirk Auer & Nicolas Petit, *Antitrust Versus the Press: Two Systems of Belief About Monopoly (*Jan. 29, 2018) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3112150 (arguing that mass media conflates the terms "monopoly" and "antitrust"); ULRICH DOLATA, APPLE, AMAZON, GOOGLE, FACEBOOK, MICROSOFT: MARKET CONCENTRATION—COMPETITION—INNOVATION STRATEGIES (2017),

focused on positive direct network externalities; that is, when a user joins a network, she benefits similar users on that network.[81] A clear example is bitcoin, the digital currency. The more users trading in bitcoin, the more valuable bitcoin becomes for every owner of the currency. When networks have two or more *groups* participating, indirect network externalities arise, which means that the more buyers of Barbra Streisand memorabilia who join eBay, the better off sellers of Streisand memorabilia become.[82]

Since all sides of the transaction benefit as the network grows, network effects create inertia furthering the platform's size and popularity.[83] Consider the number of connections keeping Facebook's rivals at bay. Given the size of Facebook's user base, upstart competitors cannot possibly offer consumers the same ability to connect with friends, family, and strangers—thus, Facebook's network advantage reinforces its monopoly power.[84]

Beyond traditional network effects, firms can also marshal *data* network effects.[85] Data network effects occur when a system becomes more efficient through machine-learning as more data is fed into it. Google's search engine is the ultimate example. Based on trillions of observations about searchers' intentions (their search query) and what they prefer (which link is selected), Google continuously gains intelligence so that it may, among other things, precisely direct advertising.[86] As Scott Galloway explained, "Google, unlike most products, ages in reverse, becom[ing] more valuable with use."[87] Then, upon gaining momentum, platforms can pursue complementary offerings to feed their algorithms with additional users and data. Google offers G Suite and Maps in addition to its search engine.[88] Uber Eats has likewise surpassed competition in

---

https://www.econstor.eu/bitstream/10419/152249/1/880328606.pdf; Nick Srnicek, *The Challenges of Platform Capitalism*, 23 JUNCTURE 254 (2017), https://rampages.us/goldstein2017capitalism/wp-content/uploads/sites/24780/2017/08/
Srnicek-2017-Juncture.pdf (arguing that "platform" businesses are driven to constantly expand and that in doing so, they disregard user's privacy and worker's rights); Jonathan Taplin, Opinion, *It is Time to Break Up Google?*, N.Y. TIMES (Apr. 22, 2017), https://www.nytimes.com/2017/04/22/opinion/sunday/is-it-time-to-break-up-google.html (arguing that Google has become a natural monopoly that needs to be regulated).

[81] *See* Michael L. Katz & Carl Shapiro, *Network Externalities, Competition, and Compatibility*, 75 AM. ECON. REV. 423 (1985); Arun Sundararajan, *Network Effects* (2006), http://oz.stern.nyu.edu/io/network.html (last visited Apr. 2, 2018).

[82] Justus Haucap & Ulrich Heimeshoff, *Google, Facebook, Amazon eBay: Is the Internet Driving Competition or Market Monopolization?*, DICE Discussion Paper, No. 83 (Jan. 2013); Evans & Schmalensee, *supra* note 62.

[83] We say "generally" because the Cambridge Analytica scandal revealed how easy it was Facebook's app developers to access large amounts of user data. *See supra* notes 134-38 and associated text. *But see* FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION (2015).

[84] We make no claim that is not *possible* for competition to enter into the marketplace *See*, *e.g.*, Facebook versus MySpace, and Ask Jeeves! versus Google) we just observe that it is unlikely. Stuart Dredge, *MySpace- What Went Wrong: "The Site Was a Massive Spaghetti-Ball Mess"*, GUARDIAN (Mar. 6, 2015, 4:04 AM), https://www.theguardian.com/technology/2015/mar/06/myspace-what-went-wrong-sean-percival-spotify; Kevin Ryan, *The Long, Sad Story of Ask.com,* ADAGE (Nov. 12, 2012), https://adage.com/article/digitalnext/long-sad-story-jeeves/147091/.

[85] James Currier, *The Networks Effect Manual: 13 Different Network Effect (and Counting)*, MEDIUM, https://medium.com/@nfx/the-network-effects-manual-13-different-network-effects-and-counting-a3e07b23017d.

[86] Ardor Seo, *How Many Google Searches Per Day on Average in 2018*, https://ardorseo.com/blog/how-many-google-searches-per-day-2018/ (last visited Feb. 4, 2019); GALLOWAY, *supra* note 42, at 5 (2018).

[87] GALLOWAY, *supra* note 42, at 5.

[88] G Suite includes incredibly popular products like Gmail, Drive, Docs, and Sheets. Zia Zaidi, *The Numbers Are In: Google's G Suite Was. Roaring Success in 2018*, DIGITAL INFORMATION WORLD (Feb. 6, 2019), https://www.digitalinformationworld.com/2019/02/g-suite-5-million-users.html. Google Maps is also the number one

the market for food delivery with its understanding of maps and logistics gleaned from its parent, Uber.[89] From the troves of data mined from a network's connections, dominant platforms can thus generate a superior ability than their smaller rivals to discern trends, interpret markets, and unite consumers with sellers and advertisers.[90]

Notwithstanding the notion that network effects naturally arise, platforms can embellish their network advantage—in perhaps anticompetitive ways—to exclude competition. Case in point is Facebook's litigation with plaintiff Six4Three who Facebook hired to create an app for its platform. Six4Three alleged that Facebook restricted the developers' access to Facebook's data to pressure the developers into several agreements, which included 1) sharing their app's data with Facebook, 2) transferring their intellectual property to Facebook, and 3) selling Six4Three to Facebook for a below market fee.[91] According to the developers, Facebook's tactics were especially coercive because, without Facebook's data, it would be impossible for them to finish their app Pikini, resulting in a potential total loss investment.[92]

Likewise, game developers have asserted that Facebook prohibits them, as a condition of accessing Facebook's platform, from charging cheaper prices outside of Facebook's network.[93] The implication is that Facebook impedes competition by forcing rivals to maintain artificially high prices. In a letter to the FTC, a consumer advocacy group wrote: "By prohibiting game developers from offering lower prices to users outside the Facebook platform, Facebook has fixed prices and therefore stifled competition outside the Facebook platform because developers cannot provide the incentive of a discounted price on another social network or website that would draw players away from Facebook."[94]

Further, akin to how Facebook pressured Six4Three to sell their company, critics allege that the leading platforms acquire potential rivals to prevent upstarts from threatening their market power.[95] This is known as the Kronos effect after the Greek God who ate his offspring to protect

---

navigation app. Robert Williams, *Google Maps Rated as No. 1 Navigation App, Survey Says*, MOBILE MARKETER (July 11, 2018), https://www.mobilemarketer.com/news/google-maps-rated-as-no-1-navigation-app-survey-says/527525/.

[89] Ashley Sams, *Uber Eats is Using AI to Surpass its Competitors (And It's Working)* (Oct. 3, 2018), https://www.marketingaiinstitute.com/blog/uber-eats-artificial-intelligence.

[90] This is largely driven by machine learning. Alex Hern, *Google Says Machine Learning Is the Future. So I Tried it Myself* (June 28, 2016, 3:00 PM), https://www.theguardian.com/technology/2016/jun/28/google-says-machine-learning-is-the-future-so-i-tried-it-myself. *See also* Tim O'Reilly, *What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software*, 65 COMM. & STRATEGIES 17, 24 (2007) (Network effects from user contributions are the key to market dominance in the Web 2.0 era."); Howard A. Shelanski, *Information, Innovation, and Competition Policy for the Internet*, 161 U. PA. L. REV. 1663, 1679 (2013) (data is a "strategic asset that allows a platform to maintain a lead over rivals and to limit entry into its market.").

[91] Six4Three, LLC v. Facebook, Inc., No. CIV 533328, 2016 WL 3442328, at *1 (Cal.Super. June 15, 2016); Hannah Kuchler, *Facebook Accused of 'Anti-Competitive Behaviour*, FINANCIAL TIMES (May 24, 2018), https://www.ft.com/content/a383ab46-5f6b-11e8-9334-2218e7146b04.

[92] *See generally*, Issie Lapowsky, *Facebook's Bikini App Lawsuit is Getting Really Ugly*, WIRED (Nov. 29, 2018, 4:20 PM), https://www.wired.com/story/facebook-six4three-bikini-app-lawsuit/ (detailing the lawsuit).

[93] Pikini is an app that mines a Facebook user's photos for swimsuit pictures. Louise Naughton, *Facebook Accused of Anticompetitive Practices*, ELECT. PYMTS INT'L (July 1, 2011), https://www.verdict.co.uk/electronic-payments-international/news/facebook-accused-of-anticompetitive-practices/.

[94] Jamie Court, *Facebook Money? Will the Feds Stop Facebooks' Power Play for Online Currency?*, HUFFINGTON POST (Jun. 29, 2011, 11:09 AM), https://www.huffingtonpost.com/jamie-court/facebook-money-will-the-f_b_886846.html

[95] GALLOWAY, *supra* note 42.

his supremacy.[96] For instance, Google took the lead in the video sharing market by acquiring its chief rival, YouTube.[97] Consider Facebook's purchase of Onavo—a nascent app from Israel designed to help families track their data usage—which enabled Facebook, upon mining Onavo's data, to identify other emerging apps to acquire.[98] Beyond Facebook, which bought competitors Instagram and WhatsApp among others, Amazon survived its price battle with Diapers.com by purchasing the company.[99]

So in light of experimentation, machine learning, network effects, and corporate acquisitions, most leading platforms lack serious competition.[100] In fact, the chief rivals of most platforms tend to come from the other dominant platforms (*e.g.*, Google sought to create the social networking platform Google+ to challenge Facebook; Amazon and Google are now fighting in the smart speaker market).[101] But because users pay for these services with personal information instead of money, platforms can—without much attention—generate privacy side effects borne by users. The following Part explores the privacy externalities suffered by consumers, markets, and governments.

II. Privacy Vulnerability in the Age of Platforms

Recent media reports are replete with examples of consumers suffering privacy-related injuries from platform marketplaces. These injuries range from identify theft, location tracking, data blackmail to tampered elections. Observers have even remarked that technology's misuse has caused society's confidence in seminal institutions to erode.[102] This Part discusses the ways platforms externalize the costs of privacy onto consumers in both economic and political contexts; from this analysis, Part IV will argue that inadequate privacy should entail an anticompetitive effect under the antitrust laws.

A. The Legal Scope of Privacy

Despite efforts by scholars such as Ruth Gavison to define privacy—"[i]n its most suggestive sense, privacy is a limitation of others' access to an individual"[103]—the law has poorly

---

[96] TIM WU, THE MASTER SWITCH: THE RISE AND FALL OF INFORMATION EMPIRES (2011).

[97] Victor Luckerson, *A Decade Ago, Google Bought YouTube and It was the Best Deal Ever*, THE RINGER (Oct. 10, 2016), https://www.theringer.com/2016/10/10/16042354/google-youtube-acquisition-10-years-tech-deals-69fdbe1c8a06 ("In 2005 the web was in desperate need of a video hub, and Google tried to create one with the poorly named Google Videos... At the time of its acquisition, YouTube was one of the world's fastest-growing websites, and its executives had a clear understanding of what users wanted out of a video site. As the adage goes: If you can't beat them, buy them.").

[98] Erin Griffith, *Will Facebook Kill All Future Facebooks?*, WIRED (Oct. 25, 2017, 7:00 AM), https://www.wired.com/story/facebooks-aggressive-moves-on-startups-threaten-innovation/

[99] BRAD STONE, THE EVERYTHING STORE: JEFF BEZOS AND THE AGE OF AMAZON (2013).

[100] FRANKLIN FOER, WORLD WITHOUT MIND: THE EXISTENTIAL THREAT OF BIG TECH 30–31 (2017).

[101] GALLOWAY, *supra* note 42. *See* Canalys, *Global Smart Speaker Shipments Grew 187% Year on Year in Q2 2018, with China the Fastest Growing Market* (Aug. 16, 2018), https://www.canalys.com/newsroom/global-smart-speaker-shipments-grew-187-year-on-year-in-q2-2018-with-china-the-fastest-growing-market; Lisa Eadlicicco, *Why Google+ Failed, According to Google Insiders*, BUS. INSIDER (Apr. 26, 2015, 9:12 AM), https://www.businessinsider.com/what-happened-to-google-plus-2015-4.

[102] RACHEL BOTSMAN, WHO CAN YOU TRUST? HOW TECHNOLOGY BROUGHT US TOGETHER AND WHY IT MIGHT DRIVE US APART (2017).

[103] Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 428 (1980).

established the boundaries of one's privacy rights. In turn, platforms and other companies enjoy an almost unrestrained ability to observe and manipulate users, as the U.S. lacks a comprehensive set of privacy protections vis-à-vis companies and consumers.[104] Most privacy laws, for instance, pertain only to specific types of data collection and usages, including consumer credit (the Fair Credit Reporting Act) or health data (Health Insurance Portability and Accountability Act).[105] And while the Federal Trade Commission (FTC) is tasked with protecting consumer privacy under Section 5 of the FTC Act, ithe agency operates under a limited mandate focused on unfair and deceptive trade practices (e.g., a platform's failure to comply with its own privacy policies).[106] Due to this landscape, the boundaries of one's privacy rights remain elusive and ill protected.[107]

Daniel Solove's seminal taxonomy of privacy harms is, however, a useful starting point for discussing the privacy implications of technology.[108] For Solove, privacy harms originate from four types of activities: 1) collecting information about individuals, 2) processing that information to derive useful insights, 3) disseminating that information and those insights, and 4) influencing individuals based on those insights.[109] As privacy moves away from one's control, individuals increasing lose ability to prevent the collection, analysis, and dissemination of their data and more disturbingly, their ability to exercise freewill when targeted via hidden means.[110]

B. Privacy Harms

Using Solove's taxonomy, this section traces the ways a firm's activities may inflict quantifiable costs on individuals, markets, and governments as well as erode one's decisional privacy, as platforms can manipulate the behaviors of consumers using proprietary data about their tendencies.

1. Harms from Collecting Information

Platforms collect data from individuals from an incomprehensible number of sources. Amazon, for instance, gathers data from all companies using its cloud storage service, Amazon Web Services (AWS), which drives some of the world's largest platforms including Netflix,

---

[104] Various provisions in the U.S. Constitution and state constitutions of course operate to protect individuals from privacy invasion by the government.

[105] Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877, 881 (2003).

[106] 15 U.S.C. § 45(a)(1). *See generally*, *Big Data: A Tool for Inclusion or Exclusion?*, FTC (Jan. 6, 2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf (providing an overview of privacy law in the context of firms collecting and using large amounts of data). *See also*, Maureen K. Ohlhausen & Alexander P. Okuliar, *Competition, Consumer Protection, and The Right [Approach] to Privacy*, 80 ANTITRUST L.J. 121 (2015).

[107] Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131 (2011); Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1908 (2013) ("[P]rivacy is not a fixed condition, nor could it be, because the individual's relationship to social and cultural contexts is dynamic."); Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1090 (2002); Gavison, *supra* note 103.

[108] Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006). *See e.g.* Calo, *supra* note 107, 15 1139-1142 (describing the utility and limitations of Solove's approach).

[109] Solove, *supra* note 108, at 489. Decisional privacy violations involve interfering with people's ability to make their own decisions. *Id.*

[110] *Id.*

Airbnb, Adobe, and Slack.[111] Similarly, Facebook harvests locational data even when users are not using the app so as to help advertisers target them.[112]

To avoid surveillance, some consumers expend significant resources from the purchasing of webcam covers, installing software and browser extensions such as tracker blockers and ad blockers to the building of a virtual private network, known as a "VPN."[113] It is, however, unlikely that these efforts can obstruct all monitoring.[114] Users may even suffer indirect costs, especially related to employment opportunities—*e.g.*, if a job requires Adobe or Slack, one will inevitably be surveilled.

Nevertheless, despite the recent spate of high-profile breaches, evidence suggests that most consumers have yet to spend additional time or resources to protect their privacy.[115] This is partially because platforms bewilder consumers with complex privacy policies found in contracts of adhesion.[116] When adding the power of network effects, consumers lack a meaningfully secure alternative. After all, regardless of one's dissatisfaction with Uber, few would prefer a rival ride-share app with robust privacy protections but no cars. Individuals are, likewise, unlikely to search with the privacy-bastion DuckDuckGo, a tiny competitor (with 0.22% of the market share) which is presumed to lack Google's quality (with 73.73% of the market).[117] Furthermore, many DuckDuckGo users would probably be surprised to learn that the service is hosted on an AWS server.[118]

2. Harms from Analyzing Information

A step beyond data harvesting is analyzing the resulting information for insights about users. Consider that platforms such as Snapchat employ mapping technology from one's

---

[111] *Why AWS Dominates the Internet*, DIGG (Feb. 6, 2018, 12:45 PM), http://digg.com/2018/why-aws-dominates-the-internet. Amazingly, in 2017, AMS represented only 10% of the company's total revenue but 73% of its operating income. Therese Poletti, *The Engine for Amazon's Earnings Growth Has Nothing to Do with E-Commerce*, MARKETWATCH (Apr. 29, 2018, 11:51 AM), https://www.marketwatch.com/story/the-engine-for-amazon-earnings-growth-has-nothing-to-do-with-e-commerce-2018-04-26.

[112] Bennett Cyphers, *A Guided Tour of the Data Facebook Uses to Target Ads*, EFF, (Jan. 24, 2019), https://www.eff.org/deeplinks/2019/01/guided-tour-data-facebook-uses-target-ads.

[113] For a detailed explanation of these methods *see* Natasha Lomas & Romain Dillet, *How to Save Your Privacy from the Internet's Clutches: Practical Tips to Fight Surveillance Capitalism*, TECH CRUNCH, https://techcrunch.com/2018/04/14/how-to-save-your-privacy-from-the-internets-clutches/ (last visited Feb. 13, 2019).

[114] Kashmir Hill reported on how hard it is to quit the top five tech firms, Amazon, Facebook, Google, Microsoft, and Apple, all of which largely derive profits from their platform services. Kashmir Hill, *Life Without the Tech Giants*, GIZMODO (Jan. 22, 2019,11:45 PM) https://gizmodo.com/life-without-the-tech-giants-1830258056.

[115] *See* Christopher Koopman, *Is Data Privacy a Market Failure?*, MEDIUM (Jan. 10, 2019), https://medium.com/cgo-benchmark/is-data-privacy-a-market-failure-461f987874ac.

[116] Marcus Moretti & Michael Naughton, *Why Privacy Policies Are So Inscrutable*, THE ATLANTIC (Sept. 5, 2014), https://www.theatlantic.com/technology/archive/2014/09/why-privacy-policies-are-so-inscrutable/379615/; Chris Morran, *1-in-5 Internet Users Always Read Privacy Policies, But That Doesn't Mean They Understand What They're Reading*, CONSUMERIST (Nov. 28, 2012, 3:15 PM), https://consumerist.com/2012/11/28/1-in-5-internet-users-always-read-privacy-policies-but-that-doesnt-mean-they-understand-what-theyre-reading/.

[117] Karlijn Pots, *Deciphering Search Ranking Credibility and Quality: An Exploratory Analysis* 8 (Masters Thesis, University of Twente), https://pdfs.semanticscholar.org/addb/9960d8643e309afaaaa8d5d3efc6ee780945.pdf; *Search Engine Market Share*, NETAPPLICATIONS (2017), https://netmarketshare.com/search-engine-market-share.aspx (last visited Feb. 13, 2019). Interestingly, DuckDuckGo is hosted on Amazon Web Service described below.

[118] Hill, *supra* note 114.

smartphone to advertise businesses located in a close vicinity to that individual.[119] Users have, indeed, reported ads on their devices for stores in which they had physically visited despite never having performed an online search of those businesses.[120] Furthermore, Uber received a patent on technology designed to predict when a user is intoxicated based on typos, walking speed, as well as whether the user's phone is being held at an odd angle or swaying.[121] While observers might assume that such programs analyze anonymized data and is thus benign, recent reporting suggests otherwise.[122] When platforms analyze general data to discover broad patterns and preferences, evidence suggests that anxiety and other psychological issues can develop.[123] Increased recognition of these "big brother" capabilities of platforms can alter behavior, again, at a cost.

3. Harms from Disseminating Information

The manner and scale in which platforms collect personal information raises the danger of unwanted dissemination, which is both common and costly. Over the last decade, the number of data breaches has risen sharply.[124] From 2012-2017, Amazon, Facebook, Google, and Uber suffered a series of breaches impacting almost one hundred million people.[125] Even Dominos's

---

[119] Robert Williams, *Snapchat Debuts 2 Ways to Target Ads by Location*, MOBILE MARKETER (Mar. 23, 2018), https://www.mobilemarketer.com/news/snapchat-debuts-2-ways-to-target-ads-by-location/519827/ ("Snapchat introduced two new ways for marketers to reach target audiences on the kind of location, the distance around a map point or foot traffic in an area, according to a company blog post. The image-messaging app with 187 million users wants to give businesses a way to reach customers who are in the right place at the right time.").

[120] *See id.* Andy Greenberg, *It Takes Just $1,000 to Track Someone's Location with Mobile Ads*, WIRED (Oct. 18, 2017; 7:00 AM), https://www.wired.com/story/track-location-with-mobile-ads-1000-dollars-study/ ("[T]he researchers had set on their grid of ad buys, the ad would appear on it, the researchers would be charged 2 cents, and they'd receive confirmation from the DSP of approximately where, when, and on which phone the ad had been shown. With that method, they were able to follow their test phones' locations within a range of about 25 feet… they were able to easily identify the person's home and work address, based on where their target stopped."); *Location-Based Mobile Advertising: A Step-By-Step Guide for Small Businesses*, MOBILE ADS BLOG (Dec. 22, 2016), https://www.mobileads.com/blog/location-based-mobile-advertising-small-business/.

[121] Arwa Mahdawi, *Uber Developing Technology That Would Tell If You're Drunk*, GUARDIAN (Jun. 11, 2018, 12:27 PM), https://www.theguardian.com/technology/2018/jun/11/uber-drunk-technology-new-ai-feature-patent.

[122] Jennifer Valentino, et al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), https://www.nytimes.com /interactive/2018/12/10/business/location-data-privacy-apps.html.

[123] Ian Tucker et al., *Experiencing the 'Surveillance Society'*, 29 PSYCHOLOGIST 682 (2016).

[124] Victor Reklaitis, *How the Number of Data Breaches is Soaring—In One* Chart, MARKETWATCH (May 25, 2018, 2:25 AM), https://www.marketwatch.com/story/how-the-number-of-data-breaches-is-soaring-in-one-chart-2018-02-26. For example, in 2017, data breaches nearly doubled from the previous year. *Data Breaches on the Rise*, EPIC.ORG (Jan. 25, 2018), https://epic.org/2018/01/data-breaches-on-the-rise.html.

[125] Amazon, 24.08 million users; Facebook, 6 million users; Google 5.93 million; Uber 57.05. Eliene Augenbraun, *Hackers Post Millions of Stolen Gmail Passwords on Russian Site*, CBS NEWS (Sept. 10, 2014, 6:31 PM), https://www.cbsnews.com/news/russian-hackers-steal-5-million-gmail-passwords/; Bloomberg, *Uber Data Breach Exposed Personal Information of 20 Million Users*, FORTUNE (April 12, 2018), http://fortune.com/2018/04/12/uber-data-breach-security/; Check Point, *More Than 1 Million Google Accounts Breached by Gooligan*, https://blog.checkpoint.com/2016/11/30/1-million-google-accounts-breached-gooligan/ (last visited Jan. 12, 2019); Alex Fitzpatrick, *Uber Data Breach Put 50,000 Drivers' Info at Risk*, TIME (Feb. 27, 2015), http://time.com/3726992/uber-data-breach/; Drew Guarini, *Facebook Leak of 6 Million Users' Data Larger Than We Thought*, HUFFINGTON POST (June 27, 2013, 1:26 PM), https://www.huffingtonpost.com/2013/06/27/facebook-leak-data_n_3510100.html; Mark Jones, *80,000 Logins Compromised in Amazon Server Breach*, KOMANDO (July 12, 2016), https://www.komando.com/happening-now/365611/80000-logins-compromised-in-ama

breach exposed the personal information of over half of a million individuals.[126] And since each victim of identity theft suffers an average loss of $1,000, the cumulative costs borne by consumers equate to billions of dollars each year.[127]

In fact, the prevalence of data breaches masks the *ex ante* costs incurred by consumers to guard against improper dissemination. Consider that a cottage industry of identity protection companies offers to prevent unwanted dissemination of data. Their services include the monitoring of the dark web, investigating of identity theft, and insuring against breaches.[128] The cyber security market is, in turn, expected to eclipse $170 billion in revenue by 2022.[129]

Platforms may also pass their internal costs derived from appeasing hackers and regulators onto users. For example, in 2016, Uber paid hackers $100,000 in hush money to destroy the private information of over 57 million users.[130] Similarly, in 2018, Amazon gave customers between $5 and $100 gift cards per complaint as an apology for exposing their email addresses.[131] These numbers pale in comparisons, however, to the hundreds of millions of dollars platforms pay globally to regulatory bodies for data breaches.[132]

4. Harms from Manipulation Based on Information and Insights

zon-server-breach; Emil Protalinski, *4.93 Million Gmail Usernames and Passwords Published, Google Says 'No Evidence' Its Systems Were Compromised*, THE NEXT WEB (Sep. 10, 2014), https://thenextweb.com/google/2014/09/10/4-93-million-gmail-usernames-passwords-published-google-says-evidence-systems-compromised/; Zack Whittaker, *Amazon's Zappos in Massive Data Breach; 24 Million Affected*, ZDNET (Jan. 16, 2012, 3:34 PM), https://www.zdnet.com/article/amazons-zappos-in-massive-data-breach-24-million-affected/.

[126] Jonathan Webb, *Domino's Pizza Blames Supplier for Data Breach: Hackers Are Probing Third-Party Weaknesses*, FORBES (Oct. 30, 2017, 11:00 AM), https://www.forbes.com/sites/jwebb/2017/10/30/dominos-pizza-blames-supplier-for-data-breach-hackers-are-probing-third-party-weaknesses/.

[127] *See also* Kelli B. Grant, *Identity Theft, Fraud Costs Consumers More Than $16 Billion*, CNBC (Feb. 1, 2017; 9:11 AM), https://www.cnbc.com/2017/02/01/consumers-lost-more-than-16b-to-fraud-and-identity-theft-last-year.html; Ellen Sirull, *The Hidden Costs of Identity Theft*, EXPERIAN (Jan. 19, 2018), https://www.experian.com/blogs/ask-experian/the-hidden-costs-of-identity-theft/.

[128] *See, e.g.*, Nate Lord, *Infographic: Is Security Spending Proportional to the Data Breach Problem?* DIGITAL GUARDIAN (July 27, 2017), https://digitalguardian.com/blog/infographic-security-spending-proportional-data-breach-problem.

[129] *Cyber Security Market to Touch US$ 170 Billion by 2022*, MARKETWATCH (Aug. 26, 2018, 11:00 PM), https://www.marketwatch.com/press-release/cyber-security-market-to-touch-us-170-billion-by-2022-2018-08-26.

[130] Lee Mathews, *Uber Pays $148 Million to Settle 2016 Data Breach Nightmare*, FORBES (Sep. 26, 2018, 3:18 PM), https://www.forbes.com/sites/leemathews/2018/09/26/uber-pays-148-million-to-settle-2016-data-breach-nightmare/#da6a01a78349. Uber also ended up paying a penalty of $148 million for the breach. *Id.*

[131] Catie Keck, *Amazon Is Offering Gift Cards to Customers Who Complain About Its Data Breach: Report*, GIZMODO (Nov. 29, 2018, 8:10 PM), https://gizmodo.com/amazon-is-offering-gift-cards-to-customers-who-complain-1830756650. Perhaps, the pinnacle example of technology enabling privacy disasters is a modern scam where criminals threaten to release one's hacked information unless the victim pays a ransom in bitcoin—due to the sophistication of blockchain technology, these blackmail payments are virtually impossible to track. *See* Jennifer Schlesinger & Andrea Day, *"I Know You Cheated on Your Wife"* CNBC, *Growing Blackmail Scan Demands Payment in Bitcoin*, CNBC (Jan. 22, 2018, 1:06 PM), https://www.cnbc.com/2018/01/22/growing-blackmail-scam-demands-payment-in-bitcoin.html (explaining the bitcoin scam).

[132] Anthony Wallace, *Fines and Lawsuits Are Adding to the Cost of Corporate Data Breaches* (Nov. 13, 2018, 10:00 PM), https://worldview.stratfor.com/article/fines-and-lawsuits-are-adding-cost-corporate-data-breaches.

In addition to direct outlays, a troubling aspect of data commercialization concerns the hidden dangers to *decisional privacy*.[133] Buttressed by society's poor understanding of the ways tech firms exploit data, consumers can unwittingly participate in experiments resulting in their augmented behavior.[134] The Facebook Cambridge Analytica scandal of 2018 is an unfortunate example. Russian-American professor, Aleksandr Kogan, developed a personality quiz app in 2014.[135] With it, he received permission from 270,000 Facebook users to mine their data for academic purposes.[136] Unbeknownst to those users, Kogan gathered the personal data of their friends, including roughly 71 million Americans. Kogan then sold that personalized data to Cambridge Analytica, a political consulting firm hired by the Trump Campaign.[137] As stated by Marc Rotenberg, the President of the Electronic Privacy Information Center: "No one could have known that their friends were disclosing their personal data on their behalf. It's entirely illogical."[138]

The uproar incited by this scandal prompted congressional inquiries and perhaps the future regulation of Facebook.[139] As the public would soon learn, the sharing of data with app developers (one of the many sides of Facebook's platform) was and is common practice.[140] In fact, Facebook and other platforms have for years harvested data from users in surprising ways. For instance, Ars Technica reported that Facebook scraped call and text data from Android phones.[141] Facebook has

---

[133] Aaron Smith, *Half of Online Americans Don't Know What a Privacy Policy Is*, PEW RESEARCH CENTER (Dec. 4, 2014), http://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is/ (finding that over 50% of Americans do not understand even the basics of privacy policies).

[134] *See, e.g*, PEOPLE, POWER, AND TECHNOLOGY: THE 2018 DIGITAL ATTITUDES REPORT DOTEVERYONE (2018), http://attitudes.doteveryone.org.uk/ (finding that only one-third of people are aware that their data is being collected and that half of people want to know how their data is used, but cannot find out); Natasha Singer, *What You Don't Know About How Facebook Uses Your Data*, N.Y. TIMES (Apr. 11, 2017), https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html.

[135] Matthew Rosenberg, Nicholas Confessore & Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. TIMES (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

[136] Granville, *supra* note 9.

[137] Craig Timberg & Tony Romm, *Facebook Could Face Record Fine, Say Former FTC Officials*, WASH. POST (Apr. 8, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/04/08/facebook-could-face-record-fine-say-former-ftc-officials/?noredirect
=on&utm_term=.c3da44e1f60a; Rosenberg, Confessore & Cadwalladr, *supra* note 135.

[138] Elizabeth Dwoskin & Tony Romm, *Facebook's Rules for Accessing User Data Lured More than Just Cambridge Analytica*, WASH. POST (Mar. 19, 2018), https://www.washingtonpost.com/business/economy/facebooks-rules-for-accessing-user-data-lured-more-than-just-cambridge-analytica/2018/03/19/31f6979c-658e-43d6-a71f-afdd8bf1308b_story.html?utm_term=.8caa59291a2f.

[139] *See* Katy Steinmetz, *Congress Never Wanted to Regulate Facebook. Until Now*, TIME (Apr. 12, 2018), http://time.com/5237432/congress-never-wanted-to-regulate-facebook-until-now/.

[140] Alexandra Samuel, *The Shady Data-Gathering Tactics Used by Cambridge Analytica Were an Open Secret to Online Marketers. I Know, Because I Was One*, THE VERGE (Mar. 25, 2018; 1:19 PM), https://www.theverge.com/2018/3/25/17161726/facebook-cambridge-analytica-data-online-marketers. A privacy consultant, Mary Hodder remarked: "I knew 10 years ago that Facebook's API allowed an entity to gather friend data," Hodder told me. "But I wasn't surprised that the 95 percent of the population that didn't understand this were shocked. They thought if Facebook was going to sell you out, it would just be you. They didn't know you would take all your friends with you." *Id.*

[141] Sean Gallagher, *Facebook Scraped Call, Text Message Data for Years from Android Phones*, ARS TECHNICA (Mar. 24, 2018, 6:20 PM), https://arstechnica.com/information-technology/2018/03/facebook-scraped-call-text-message-data-for-years-from-android-phones/.

also confirmed that it collects data from non-Facebook users—a surprising admission for many, including the U.S. Congress.[142]

Moreover, *developers* may have little understanding of how data is captured and utilized. This ignorance is because machine learning fuels many of the algorithms that modulate consumer behavior. As Jon Kleinberg and Sendhil Mullainathan write:

> "We have, perhaps for the first time ever, built machines we do not understand. We programmed them, so we understand each of the individual steps. But a machine takes billions of these steps and produces behaviors . . . that are not evident from the architecture of the program we wrote. . . . [A]t some deep level we don't even really understand how they're producing the behavior we observe. This is the essence of their incomprehensibility."[143]

In important part, even though platform companies may exploit data to accrue market dominance, they have largely evaded antitrust scrutiny by giving away or selling their services at low costs.[144] The next section explains why privacy is omitted from antitrust's framework, despite its potential link to anticompetitive conduct, as well as the reasons antitrust law should concern itself with the issues of data protection and privacy.

III. Antitrust and Supracompetitive Privacy

The privacy injuries endemic to technology markets should, but do not currently, entail a harm recognized by antitrust law. We use empirical methods to demonstrate that privacy is a product of competition; in this sense, increased competition would compel platforms (and other companies for that matter) to more securely harvest and exploit data. Although antitrust's current form could seemingly remedy supracompetitive privacy—as antitrust's purpose is to remedy the detriments of uncompetitive markets—the courts have narrowly interpreted enforcement's scope, never extending it to privacy harms. This Part argues that, as prices lose relevance in the modern marketplace, antitrust law must evolve in a manner accounting for the privacy harms stemming from uncompetitive markets and anticompetitive behaviors.

To do so, Part III.1 traces antitrust's history to explain in Part III.2 why the courts have yet to recognize supracompetitive privacy as something that antitrust may remedy. Then, Part III.3 demonstrates the error in antitrust's current framework. It employs empirical methods demonstrating that privacy breaches can be expected in uncompetitive markets, yet currently, platforms may suppress competition so long as the effects only diminish privacy and do not raise prices. Given these results, Part III.4 explains that privacy, competition, and markets would benefit if antitrust enforcement condemned supracompetitive privacy.

---

[142] April Glaser, *It's Your Data*, SLATE (Apr. 11, 2018; 9:25 PM), https://slate.com/technology/2018/04/facebook-collects-data-on-non-facebook-users-if-they-want-to-delete-it-they-have-to-sign-up.html; Kashmir Hill, *How Facebook Figures Out Everyone You've Ever Met*, GIZMODO (Nov. 7, 2017, 9:39 AM), https://gizmodo.com/how-facebook-figures-out-everyone-youve-ever-met-1819822691.

[143] Jon Kleinberg and Sendhil Mullainathan, *2015: What Do You Think About Machines That Think?*, EDGE (2015), https://www.edge.org/response-detail/26192 (last visited Feb. 13, 2019).

[144] Robert B. Reich, *Big Tech Has Become Way Too Powerful*, N.Y. TIMES (Sept. 18, 2015), https://www.nytimes.com/2015/09/20/opinion/is-big-tech-too-powerful-ask-google.html.

A. Antitrust Law Explained through a Historical Context

Antitrust's history reveals why the courts have limited the types of injuries that enforcement may redress, none of which including the costs of privacy. Before the Chicago School[145] sought to reform antitrust law in the 1970s, the judiciary had a poor understanding of economics, causing antitrust to seek improper and unclear goals.[146] This was predictable considering the difficulties of enforcing antitrust; since competition *should* destroy inefficient firms, the courts struggled to differentiate shrewd business practices from anticompetitive conduct.[147] Compounding matters, Congress drafted the Sherman Act using broad language, providing few clues or methods to discern illegal conduct.[148] It was instead the courts' task to define antitrust's scope,[149] which they labored to do.[150] Principally, the courts assumed that antitrust law should foster competition among many small businesses, which was errantly expected to produce lower prices as well as greater social and political equality.[151] Antitrust's early populism—i.e., protecting small businesses from their larger competitors—ostensibly justified condemning powerful companies that, in driving small firms out of business, diminished competition.[152] But as the Chicago School would identify, enforcement was mangling economic theory as well as harming markets and competition.

The Chicago School relied on a combination of legislative history and economic theory to identify the erroneous assumptions underlying enforcement. According to Robert Bork, Congress's sole purpose in enacting the Sherman Act was to promote "consumer welfare" via

---

[145] *See generally* Richard Posner, *The Chicago School of Antitrust Analysis*, 127 U. PA. L. REV. 925, 926 (1979) (describing the "Chicago School" as well as its intellectual rivalry with the "Harvard School" of economics); George L. Priest, *Bork's Strategy and the Influence of the Chicago School on Modern Antitrust Law*, 57 J.L. & ECON. S1 (2014) (explaining the Chicago's influence on antitrust).

[146] *See* Joshua D. Wright, *The Antitrust/Consumer Protection Paradox: Two Policies at War with Each Other*, 121 YALE L.J. 2216, 2233 (2012) ("The first half-century of decisions interpreting the antitrust laws suffered from what might be charitably called internal inconsistencies").

[147] ROBERT BORK, THE ANTITRUST PARADOX: A POLICY AT WAR WITH ITSELF (1978).

[148] Vaheesan, *supra* note 31, at 372 ("In the first four decades of the new law, the Supreme Court gave voice to the popular antimonopoly sentiment of the period--preserving small producers in the new economic environment. Its solicitude was directed at farmers and small firms. The Court's focus on small producers and general neglect of consumers may not be surprising because the idea of consumers as a distinct constituency was still in its infancy").

[149] Nat'l Soc. of Prof'l Engineers v. United States, 435 U.S. 679, 688 (1978) ("Congress, however, did not intend the text of the Sherman Act to delineate the full meaning of the statute or its application in concrete situations. The legislative history makes it perfectly clear that it expected the courts to give shape to the statute's broad mandate by drawing on common-law tradition.").

[150] *See* Geoffrey A. Manne & E. Marcellus Williamson, *Hot Docs vs. Cold Economics: The Use and Misuse of Business Documents in Antitrust Enforcement and Adjudication*, 47 ARIZ. L. REV. 609, 613–14 (2005) ("The historical maxim in antitrust law has been some conception of small-business protection or other variant of social welfare rooted in the populism of the era that spawned our federal antitrust statutes.[19] While this view may not be entirely gone, it is certainly greatly diminished in modern antitrust jurisprudence.").

[151] Vaheesan, *supra* note 31, at 372.

[152] *See* Wright, *supra* note 146, at 2234 ("The 1950s-1970s' structure-conduct-performance paradigm that dominated mid-century industrial organization literature postulated that market structure influenced firm conduct, which in turn influenced market performance, or market power, within a given industry. This theory led the U.S. government to apply inflexible criteria in challenging mergers that nearly all modern economists would recognize as procompetitive.").

efficient markets.[153] Then, using economic theory, Bork and the Chicago School dispelled the belief that less concentrated markets were always more desirable. They found that some markets offered consumers lower prices when dominated by a few larger firms rather than many small businesses.[154] It was misguided, as their theory insisted, to condemn companies that had obtained monopoly power or destroyed competition by virtue of offering superior products for cheaper prices; efficient markets are, after all, supposed to produce better goods at lower prices.[155] To these economists, antitrust was diminishing consumer welfare by imposing liability on market enhancing behaviors.[156]

The Chicago School eventually persuaded the courts that, not only had populist goals led antitrust law astray, but also economic principles should guide its reform.[157] Because increased economic efficiency is the most reliable benefit of competition,[158] the courts narrowed antitrust's scope to promoting the economic interests of *consumers* as opposed to protecting individual competitors.[159] To achieve this end, today, almost all antitrust offenses require evidence that the challenged act harmed "consumer welfare,"[160] typically in the form of increased prices or restricted output (as diminished output should produce artificially high prices).[161] And elevated prices alone are not dispositive. Since markets are expected to self-correct, economists note that one who charges unreasonably high prices invites competition; so without evidence the monopolist used anticompetitive means to prevent rivals from challenging their high prices, antitrust liability is

---

[153] Daniel A. Crane, *The Tempting of Antitrust: Robert Bork and the Goals of Antitrust Policy*, 79 ANTITRUST L.J. 835 (2014).

[154] Alan J. Meese, *Monopolization, Exclusion, and the Theory of the Firm*, 89 MINN. L. REV. 743, 773–93 (2005) (describing "price theory" which assumed that many firms acting in perfect competition created the lowest, most efficient prices).

[155] *See, e.g.*, Rudolph J.R. Peritz, *Toward A Dynamic Antitrust Analysis of Strategic Market Behavior*, 47 N.Y.L. SCH. L. REV. 101, 106 (2003) (explaining how enforcing price theory condemned procompetitive behaviors: "Chicago Schoolmen such as Robert Bork and Richard Posner insisted that antitrust policy should rest on the single value of efficiency, in particular that restraints should be judged solely by their effects on price and output. In this light, the per se illegality of minimum resale price maintenance seemed to make good sense. After all, orthodox price theory told us that those restraints raised prices and lowered output. But the Chicago Schoolmen found virtue in the practice. Taking instruction from Chamberlin's work, they argued that manufacturers should be permitted to restrain their dealers' pricing practices as part of strategies to compete against other manufacturers. These strategies benefitted consumers, according to the new Chicago Schoolmen, because manufacturers set resale prices only high enough to allow dealers to spend on promotional efforts at the levels that manufacturers wanted.").

[156] BORK, *supra* note 147 (explaining that antitrust law is meant to promote consumer welfare, yet antitrust's tendency to condemn procompetitive practices that has the opposite effect of diminishing consumer welfare).

[157] *See* Michael E. DeBow, *The Social Costs of Populist Antitrust: A Public Choice Perspective*, 14 HARV. J.L. & PUB. POL'Y 205, 206 (1991) (discussing the harm of populism in antitrust enforcement).

[158] Kenneth G. Elzinga & David E. Mills, *Antitrust Predation and the Antitrust Paradox*, 57 J.L. & ECON. S181, S183–84 (2014) (discussing the importance of understanding the economics of market structure).

[159] Levine v. Cent. Florida Med. Affiliates, Inc., 72 F.3d 1538, 1551 (11th Cir. 1996) ("The antitrust laws are intended to protect competition, not competitors").

[160] In some instances, circuit courts interpret antitrust's consumer welfare scope to include non-price harms such as promoting innovation and quality of goods. *See, e.g.*, Free FreeHand Corp. v. Adobe Systems Inc., 852 F.Supp.2d 1171 (N.D. Cal. 2012) (declaring diminished innovation to entail an antitrust injury); HM Compounding Services, Inc. v. Express Scripts, Inc., 2015 WL 4162762 (E.D. Miss. July 9, 2015) (treating reduced consumer choice or variety as an anticompetitive effect under antitrust law).

[161] Peritz, *supra* note 155, at 106.

inappropriate.[162] Antitrust is thus described as a remedy for market failure since it intervenes when the market's structure prevents efficient behavior—i.e. the market has failed[163]—notwithstanding the debate over antitrust's consumer welfare standard.[164]

Given this framework, the next section discusses the reasons that platforms enjoy antitrust immunity for the privacy harms discussed in Part II. It explains that the low and zero-prices of platform services, combined with the ostensible non-price nature of privacy, exist in antitrust's blind spot.

B. Prices, Not Privacy, in Antitrust's Framework

Antitrust enforcement has never condemned anticompetitive conduct resulting in a privacy injury. Our review of case law uncovered zero instances of antitrust liability premised on remedying privacy injuries.[165] The leading antitrust treatise lacks a discussion on the matter[166] and the word "privacy" does not appear once in a preeminent law review article examining

---

[162] Andrew I. Gavil, *Exclusionary Distribution Strategies by Dominant Firms: Striking a Better Balance*, 72 ANTITRUST L.J. 3, 38 (2004) (discussing the need for exclusionary conduct since markets should otherwise self-correct).

[163] Retina Assocs., P.A. v. S. Baptist Hosp. of Fla., Inc., 105 F.3d 1376, 1384 (11th Cir. 1997) (describing the necessary relationship between market power and exclusionary behavior in rendering anticompetitive effects).

[164] In important part, the test established by the Supreme Court to determine whether conduct violates antitrust law, known as the rule of reason test, *see In re* Loestrin 24 Fe Antitrust Litig., 814 F.3d 538, 544–45 (1st Cir. 2016), has engendered a much greater debate about how to identify illegal conduct. Maurice E. Stucke, *Looking at the Monopsony in the Mirror*, 62 EMORY L.J. 1509, 1562 (2013) ("Scholars . . . continue to debate after Robert H. Bork's influential book, THE ANTITRUST PARADOX: A POLICY AT WAR WITH ITSELF (1978), over antitrust's goals. Even among those who advocate an economic welfare objective, it is unsettled whether welfare should reflect consumer welfare or total welfare, what those terms mean, and the extent to which it makes any difference."). Under the rule of reason test, conduct deserves liability if its anticompetitive effect (*e.g.*, high prices or restricted output) outweighs whatever procompetitive benefits resulted (*e.g.*, increased innovation). California Dental Ass'n v. F.T.C., 224 F.3d 942, 947 (9th Cir. 2000) ("In particular, we must determine whether, on balance, CDA's restrictions on advertising are procompetitive or anticompetitive. The restrictions qualify as anticompetitive only if they harm both allocative efficiency and raise the prices of goods above competitive levels or diminish their quality. Such analysis is rigorous, requiring "a detailed depiction of circumstances and the most careful weighing of alleged dangers and potential benefits.") (alterations in original). To most courts and scholars, conduct violates antitrust if *consumers* suffered a net welfare reduction—this is known as the consumer welfare standard. Clayton J. Masterman, *The Customer Is Not Always Right: Balancing Worker and Customer Welfare in Antitrust Law*, 69 VAND. L. REV. 1387, 1398 (2016). Although consumer welfare is the majority approach, it was certainly not what Judge Bork meant. Khan *supra* note 24, at 720 (noting that courts and scholars have misunderstood what Bork meant by "consumer welfare."). His theory—which is commonly known as the "total welfare" standard—concerned the market's overall efficiency; in his view, if exclusionary conduct inures $10 of benefit onto the monopolist while consumers lose $9 of benefit, the act should avoid liability since it produced more total welfare than lost. The key element differentiating these approaches is *not* whether antitrust's chief concern lies with market prices, but whether antitrust should scrutinize the welfare of just consumers or the entire market.

[165] *But see* U.S. DEPT. OF JUSTICE & FEDERAL TRADE COMMISSION, HORIZONTAL MERGER GUIDELINES (2010) (anticompetitive effects "be manifested in non-price terms and conditions that adversely affect customers").

[166] PHILLIP E. AREEDA & HERBERT HOVENKAMP, ANTITRUST LAW (2000).

anticompetitive effects.[167] As a leading scholar in the field noted, antitrust is simply unconcerned with the costs of privacy.[168]

To explain why privacy injuries *and* platform companies have evaded antitrust scrutiny, modern enforcement presumes that competitive prices are the primary benefit conferred to consumers by efficient markets. However, since most platforms offer low-priced (or zero-priced) goods and services, the typical antitrust analysis would conclude that this market reflects sufficient consumer welfare.[169] So even if one could link a privacy injury to anticompetitive behavior—which we argue in the following section—a court would be highly unlikely to impose antitrust liability without evidence of supracompetitive prices.

Perhaps antitrust *could* promote privacy if the courts or scholarship recognized the privacy costs suffered by consumers, including those who had not even used the culprit technology. However, the few articles connecting privacy and antitrust laws have generally concluded that, given the supposedly non-economic nature of privacy, competition law is ill-suited for the task.[170] For instance, academics have suggested that privacy injuries could entail a type of *non-price* injury, but have cautioned against this framework because linking privacy to quality would make enforcement overly subjective and unprincipled.[171]

A couple works have sought to fit platform business models into antitrust's current framework by suggesting that a platform could violate antitrust law if it used monopoly power to underpay for data, though ignoring the costs of privacy.[172] This theory has the advantage of retaining antitrust's modern form—in the sense that it uses prices to measure consumer welfare—but it ignores the costs incurred by the greater market. Moreover, focusing on whether users receive sufficient consideration for their data raises the near impossible question of whether, or to which

---

[167] Richard D. Cudahy & Alan Devlin, *Anticompetitive Effect*, 95 MINN. L. REV. 59 (2010). The FTC reticence to incorporate privacy considerations into merger review is clear:

> Although such issues may present important policy questions for the Nation, the sole purpose of federal antitrust review of mergers and acquisitions is to identify and remedy transactions that harm competition. Not only does the Commission lack legal authority to require conditions to this merger that do not relate to antitrust, regulating the privacy requirements of just one company could itself pose a serious detriment to competition in this vast and rapidly evolving industry. That said, we investigated the possibility that this transaction could adversely affect non-price attributes of competition, such as consumer privacy. We have concluded that the evidence does not support a conclusion that it would do so. We have therefore concluded that privacy considerations, as such, do not provide a basis to challenge this transaction. Statement of Federal Trade Commission Concerning Google/DoubleClick, FTC File No. 071-0170, at 2—3 (2007), https://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf [hereinafter Doubleclick].

[168] Newman, *supra* note 28, at 205 ("[P]rivacy law is concerned with ensuring that individuals' information remains confidential when its release or use was not bargained for as part of a voluntary exchange. Antitrust law does not concern itself with such harm.").

[169] *See infra* Part II. *See also* David S. Evans, The Antitrust Economics of Free, 7 COMPETITION POL'Y INT'L 71 (2011) (describing how price and quality are disguised by zero-price goods creating "conundrums and confusion in antitrust analysis").

[170] *See* James C. Cooper, *Privacy and Antitrust: Underpants Gnomes, the First Amendment, and Subjectivity*, 20 GEO. MASON L. REV. 1129 (2013); Geoffrey A. Manne & Raymond Sperry, *The Problems and Perils of Bootstrapping Privacy and Data into an Antitrust Framework*, CPI ANTITRUST CHRON. (May 29, 2015), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2617685.

[171] Kenneth A. Bamberger & Orly Lobel, *Platform Market Power*, 32 BERK. TECH. L.J. 1051 (2017); STUCKE & GRUNES, *supra* note 23.

[172] Nathan Newman, *Search, Antitrust, and the Economics of the Control of User Data*, 31 YALE J. ON REG. 401, 449 (2014); Pasquale, *supra* note 23, at 1009-10.

degree, individuals value their privacy vis-a-vis low-priced services.[173] For these reasons, the few works exploring antitrust's treatment of platforms have largely ignored the economic nature of privacy breaches on the greater market, dismissing this would-be cause of action. We explain in the next section that antitrust enforcement should promote privacy, as supracompetitive privacy creates measurable economic costs suffered by consumers akin to monopoly prices.

C. Competition, Privacy, and Market Failure

Privacy injuries should incur antitrust scrutiny in markets where the costs spent by consumers to prevent or remedy a privacy breach are greater than what would have occurred if not for the anticompetitive behavior. Key to our stance—which we empirically demonstrate in the following section—is that inadequately protected data is attributable to a lack of competition, and that more competition would remedy this harm. To make this case, notice that privacy injuries are a form of market failure.[174] If a tech company could generate $10 of revenue from exploiting data, creating $8 of costs for the company and $15 of costs borne to the public, the company is likely to do the deal—despite the net level of societal harm—because enough costs are externalized to make the transaction profitable (for the company, that is). We think that, instead of externalizing privacy costs, platforms would increase spending on data protection if sufficient market forces existed. This is because added competition would 1) punish the culprits of a data breach, 2) disclose information about data collection and privacy breaches, and 3) provide consumers with products designed to protect privacy.

1. Punishment

To begin, if technology markets were competitive, consumers could respond to a company's data breach by giving one's business to a rival firm, punishing the offender. Currently, without competing options, monopolists are more capable of surviving a privacy breach—although some consumers may quit the platform, a lack of competition enables the platform to retain users who would otherwise switch to a rival. This is why, for example, Facebook's stock price rallied to pre-Cambridge Analytica levels soon after the scandal.[175] Consumers may even harbor the belief that the few firms in a monopolized market are all effectively the same. This dynamic is akin to monopoly pricing in a concentrated market; even though consumers may detect that the monopolist's prices are abnormally high, they lack a meaningful alternative, causing them to patronize the monopolist anyway. As a result, increasing competition would not only enable consumers to boycott firms that improperly protect data, but it would also create incentives for platforms to protect their users' personal information *before* a breach occurs.

---

[173] *See id.*; Harbour & Koslov, *supra* note 23. Furthermore, as Manne and Perry argue, some consumers may even view dissemination of data to third-party advertisers as a good thing because it provides better targeted advertising. Manne & Sperry, *supra* note 170.

[174] For example, if a chemical company could legally dump waste in a stream polluting the town downstream, this would incentivize the company to externalize its costs, causing market failure. Christopher R. Leslie, *Achieving Efficiency Through Collusion: A Market Failure Defense to Horizontal Price-Fixing*, 81 CAL. L. REV. 243, 269 (1993) (discussing negative externalities as a form of market failure).

[175] Prachi Bhardwaj, *Eight Weeks After the Cambridge Analytical Scandal, Facebook's Stock Price Bounces Back to Where it Was Before the Controversy*, BUS. INSIDER (May 11, 2018, 5:29 PM), https://www.businessinsider.com/facebooks-stock-back-up-cambridge-analytica-charts-2018-5.

2. Information

A chief problem explaining the prevalence of supracompetitive privacy is the lack of consumer awareness for the issue. Consider that many costs derived from privacy harms are unseen. In contrast to how consumers tend to *overreact* to slight increases in retail prices—e.g., the act of driving across town to purchase nominally cheaper gasoline or purchasing a modestly cheaper yet more inconvenient airplane ticket—consumers seem to underestimate the harms levied on their decisional privacy or even accept the monetary costs of privacy breaches. This is perhaps because users enjoy obvious short-run benefits in the form of zero-priced services while cognitively disassociated from speculative long-term costs.[176] Consumers could also be making decisions based on incomplete information in the sense that their ability to make a rational choice is limited by inadequate market signals. Consumers might further ignore information about the costs of supracompetitive privacy given their inability to punish offending firms.[177]

In light of this market failure, a chief benefit of increased competition is *information*. Since most platforms already offer zero-price or low-price services, and thus cannot further reduce prices, heightened competition would compel firms to distinguish themselves using non-price signals in the form of enhanced privacy. As firms vie for users, they would likely disseminate information about the value of privacy and the costs of failing to protect one's information in order to promote their services. In this sense, concentrated markets have enabled tech firms to ignore privacy concerns as few rivals exist to shed light on the problems borne from their treatment of personal information. Increased competition would therefore cause firms to not only improve the quality of their services, but also advertise this fact to consumers, raising the attention paid by users to privacy matters.

3. Consumer Choice & Quality

An offshoot of diminished price signals is that platforms must find other grounds to compete. To challenge a monopolist offering zero-priced products, a firm must provide a different, improved product. In a landscape where a monopolist inadequately or unethically protects data, incentivizes exist for rivals to innovate a more secure product to compete. In other words, market forces would naturally nudge firms toward better data collection methods even if consumers value this characteristic less than low prices—after all, prices are increasingly obsolete.

D. Empirical Analysis

---

[176] *Quality Considerations in Digital Zero-Price Markets,* ORG. ECON. COOPERATION & DEV. at 8 (Oct. 9, 2018), http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DAF/COMP(2018)14&docLanguage=En.

[177] Consumers become impervious to data breaches as the norm; therefore, less likely to punish businesses.

"A major objection is that the current requirement for customer notice generates too many breach disclosure letters. Critics focus on the disclosure trigger in the California statute and related legislation which requires the sending of notification letters whenever there is a reasonable likelihood that an unauthorized party has "acquired" personal information. These critics point to Aesop's fable, "The Boy who Cried Wolf." As Fred Cate writes, 'if the California law were adopted nationally, like the boy who cried wolf, the flood of notices would soon teach consumers to ignore them. When real danger threatened, who would listen?' The Washington Post has joined this chorus in editorializing against these laws as creating 'tedious warnings' that will cause people to 'ignore the whole lot.'" Paul Schwartz and Edward Janger, "Notification of Data Security Breaches," (2007) 105 MICH. L. REV. 913

To move from theory to evidence, we designed empirical research to illustrate privacy's relationship with competition. Our theory is that the lack of market forces in a monopolized market empowers and incentivizes platforms to externalize the costs of privacy onto consumers. Interjecting competition, as our theory follows, would 1) enable consumers to punish offending firms, 2) spread information about privacy, and 3) generate increasingly secure products. To prove these points, our research uses an original quantitative treatment to show that insufficiently protected data is attributable to inadequate competition. We analyzed data provided by IBM regarding the costs of data breaches, as well as other publicly available sources, to show that companies wielding market power have strong incentives to externalize the costs of privacy.

1. Data

IBM conducts an annual survey of firms across many industries regarding the costs of a data breach. We tracked data from IBM's reports from the years 2013 to 2017. Our unit of analysis is thus industry-year, meaning that our dataset includes a unique observation for each industry among the surveyed years. We also created our dependent variable, *Abnormal Churn Rate*, from IBM's reports. A company's churn rate is the rate at which customers quit utilizing that company. *Abnormal Churn Rate* measures the degree to which customers leave the studied company beyond the expected level. We included both variables in our analyses.

One of our key independent variables measures an industry's level of *Market Concentration*. Since we hypothesize that concentrated markets incentivize data breaches, we calculated a variable known as the Herfindah-Hirschman Index ("HHI" or "Index") to reflect the level of competition in each of the industries studied by IBM per year. HHI is the principal means used by scholars and courts to measure market concentration—especially in antitrust analyses.[178] HHI data is computed by squaring the market share of each firm competing in an industry and then adding the resulting figures.[179] The Index ranges from 10,000 to 0, with the former number indicating a perfect monopoly whereas the latter designates perfect competition.[180] We calculated HHI statistics from CompuStat data.

The other key independent variable is the *Cost of a Data Breach per Capita* in each industry. This measures the cost of the privacy lapse per recorded breach. The expectation is that consumers take notice of costly breaches, which is supported by regressions performed by IBM.[181] Thus, we expect that industries in which costly data breaches occur are more likely to experience a greater *Abnormal Churn Rate* except when the market lacks sufficient competition.

We also found it important to control for certain intervening factors. First, we added a proxy variable accounting for the amounts of consumer information held by companies in an industry. If a monopolist collects little consumer information, it would be illogical for a significant privacy disaster to result despite the firm's market power. To control for this, we added a variable from CompuStat concerning the level of *Intangible Property* held by companies in an industry, as data is recorded as intangible property. We identified the top twenty firms holding intangible

---

[178] *See supra* note 29 and accompanying text.

[179] Fed. Trade Comm'n v. Penn State Hershey Med. Ctr., 838 F.3d 327, 346–47 (3d Cir. 2016) ("Market concentration is measured by the Herfindahl–Hirschman Index ('HHI'). The HHI is calculated by summing the squares of the individual firms' market shares. In determining whether the HHI demonstrates a high market concentration, we consider both the post-merger HHI number and the increase in the HHI resulting from the merger.").

[180] *Id.*

[181] *2015 Cost of Data Breach Study: Global Analysis*, IBM, at 14 (2015).

property per industry and year, and then created a variable for the average of their holdings. Next, we created a variable controlling for economic changes per year.

We analyzed our data using an Ordinary Least Squares (OLS). This tracks the relationship between the independent and dependent variables as a linear function.

2. Results

The variables *Breach Cost* and *Market Concentration* were both statistically significant, but *Breach Cost* is positively correlated with Churn Rate while *Market Concentration* is negatively, meaning that firms lose customers as the cost of a breach mounts *except* when the firm controls a greater share of the market. In this latter situation, consumers tend to remain with firms lacking competition despite the costs of a breach. This indicates that consumers do demand heightened privacy, though the nature of market power enables platforms to ignore this demand. We can thus deduce that, as long as platforms and tech companies can externalize the costs of privacy protection without a corresponding punishment, they have incentives to do so. Even if platforms suffer some costs and embarrassment, our empirical results indicate that firms in concentrated markets are making the rational, yet socially deleterious, decision of offloading privacy costs onto society.

Moreover, our results have significant implications for the business models chosen by platform and technology companies. It explains the economic logic of emphasizing data collection over price competition. Not only does this strategy enable firms to build monopoly power using network effects, but it also helps them to evade antitrust scrutiny. Because modern antitrust is chiefly concerned about consumer prices while ignoring privacy, platforms can avoid antitrust scrutiny when exploiting big data—despite the real harms of anticompetitive practices. Indeed, consumers and markets bear much of privacy's costs, giving platforms powerful incentives to offload the costs of privacy whether done intentionally or negligently. The next section reunites competition with antitrust policy.

Table 2.

OLS Regression

	Model 1	Model 2
Abnormal Churn Rate		
Breach Cost	**.0122378*** **	**.0122074****
	(.0023827)	(.0023648)
Market Concentration	**-.0005884***	**-.0005916 ***
	(.0003146)	(.0003122)
Intangible Holdings	**.0000239****	**.0000238****
	(.00000986)	(.00000979)
GDP Control	.1960728	
	(.3894989)	
Time Control	**-.2859058***	**-.3280497****
	(.163019)	.1388719
Constant	1.849823	**2.459286*****
	(1.452212)	**(.7961745**)

Prob > F	**0.0000*** **	**0.0000*** **
R-Squared	0.0437	0.5198
No. of Observations	149438	149337

*p<0.10, **p<0.05, ***p<0.01

E. What Does This All Mean

Given our findings that platforms (and conventional firms for that matter) would better protect privacy if they faced increased competition, we argue that antitrust could provide a remedy for privacy injuries while continuing to ground liability in purely economic terms. The solution is to measure the costs spent by society, markets, and *consumers* to prevent and cure privacy lapses. In other words, the economic costs incurred by consumers to remedy a privacy breach are analogous to supracompetitive pricing, especially in markets lacking prices. Key to our argument is that, 1) uncompetitive technology markets enable firms to offload their privacy costs, creating market failure 2) platform companies use anticompetitive practices to bolster their market supremacy, and 3) increased levels of competition would diminish the incentives to externalize privacy's costs. So to construct an antitrust claim, we think that consumers should be able to approximate the actual costs spent by consumers to *ex ante* and *ex post* guard one's data in excess of what would be expended in a competitive market. Although a difficult calculus, it is no less abstract than the typical antitrust analysis in which the plaintiff must show evidence that monopoly prices are elevated above the competitive level.

To do so, a plaintiff could compare the privacy economics of the challenged market to a more competitive market. Key would be evidence of costs not incurred in the competitive market to protect one's personal information. For instance, if plaintiffs can trace their injury to a monopolist whose privacy policy provided inadequate protection, then evidence of superior privacy regimes found in comparable yet more a competitive market would indicate an antitrust violation. For an effective argument, the plaintiff could demonstrate that added competition would have likely incentivized rivals to offer a more secure regime, yet the nature of the platform's market power enabled it to withhold adequate privacy. Or, upon a data breach, consumers could indicate the economic costs to remedy the breach in excesses of comparable breaches in more competitive markets. So to initiate such a claim, a plaintiff should first show evidence of the defendant's anticompetitive conduct to implicate a violation of Section 1 or 2 of the Sherman Act; then the complaint should provide evidence that, as a result of anticompetitive practices, the costs incurred to protect privacy or remedy a breach surpassed the competitive level.

A plaintiff could also demonstrate that increased competition would have produced a greater array of products or services on the market to secure one's privacy. But due to the platform's monopoly power, the platform resisted demands for those products. Consider for example the heightened levels of privacy available in more competitive technology sectors, such as the email market. With email, not only do companies offer email accounts designed to protect privacy, but such markets have also avoided the privacy disasters arising out of less competitive technology markets.[182] Although more secure products might come at a greater price than services lacking comparable safeguards, the point is that competitive markets are more likely to offer consumers a choice. So if consumers can demonstrate that supracompetitive privacy resulted from

[182] *See, e.g.*, *About FastMail*, FASTMAIL, https://www.fastmail.com/about/company.html (last visited Feb. 13, 2019).

a monopolist's ability to erect barriers to competition, limiting the security of products available, this should implicate antitrust's framework.

We think the benefits of instituting a cause of action for supracompetitive privacy under the Sherman Act are intuitive. First, as outlined in Part II, because the current privacy regimes are targeted to specific types of data, they fail to protect consumer welfare on either a broad or significant level. Further, considering the difficulty of asking Congress to enact compressive privacy regulations, we the think that the best answer lies in current law. Antitrust is particularly well-suited for the task, as one of its chief advantages lies in its restraint. Because enforcement would only target companies that shifted the burdens of protecting privacy onto consumers beyond a competitive level, this framework would resist condemning firms that genuinely sought to protect privacy yet were overcome by sophisticated hackers. Indeed, since antitrust liability requires anticompetitive behavior or an unreasonable attempt to generate monopoly power (per Section 1 and 2, respectively), enforcement of supracompetitive privacy would only condemn antisocial conduct—e.g., anticompetitive practices. This enforcement would also, instead of being punitive, encourage firms to protect privacy *ex ante*, that is, it would incentivize platforms and technology to protect privacy before a breach occurs. Antitrust law is thus not only capable but the preferable body of law to foster privacy in the modern economy.

IV. Implications

This Part briefly discusses the implications of our research. Given that monopoly power enables platforms to protect data in haphazard fashions, this recognition bears consequences for the relationship between technology firms and the government, behavioral economics, and merger policy. We also discuss how our approach for identifying privacy's relationship with competition may inform future research in this space.

A. When Monopoly Power, Technology and the Government Meet

The power wielded by platforms and tech firms to safeguard privacy is especially problematic when considering the potential for these companies to combine forces with governments. After World War II, the legal community enforced a loose interpretation of antitrust law, condemning a vaster array of activities than today. Driving this approach was the dark reminders of collusion between cartels in Nazi Germany and U.S. firms; Congress not only sought to prevent concentrated economic power among dominant trusts, but it also feared such market power could threaten social values.[183] These misgivings included the possibility that monopolists could unravel seminal institutions, thereby increasing autocratic tendencies.[184] Today, in a similar fashion, a chorus of politicians and citizens have expressed concerns for the power marshalled by platforms to influence social institutions.[185]

---

[183] Brown Shoe Co. v. United States, 370 U.S. 294, 316 (1962); Maurice E. Stucke, *Reconsidering Antitrust's Goals*, 53 B.C.L. REV. 551, 560 (2012).

[184] Robert Pitofsky, *The Political Content of Antitrust*, 127 U. PA. L. REV. 1051, 1051–52, (1979)

[185] TIM WU, THE CURSE OF BIGNESS (2018); Jeff Stein, *Warren's 2020 Agenda: Break Up Monopolies, Give Workers Control Over Corporations, Fight Drug Companies*, WASH. POST (Dec. 31, 2018), https://www.washingtonpost.com/business/2018/12/31/warrens-agenda-break-up-monopolies-give-workers-control-over-corporations-fight-big-pharma/?utm_term=.95efea1fc166.

A majority of this anxiety extends beyond the extensive resources of platforms[186] to include their ability to mobilize users politically.[187] Through this capacity to manipulate decisional privacy, they can trigger users to act in malleable and predictable ways.[188] While such power in the hands of private companies may seemingly alarm governments, their capacity to influence political behavior—as evidenced by the Cambridge Analytica Scandal—can be *attractive* to governments.[189]

Indeed, as platforms generate insights about populaces, as well as devised sophisticated ways to alter behaviors, governments have established strong bonds with technology companies in hopes of benefitting from their capabilities. For instance, Google representatives held 427 meetings with the Obama White House, averaging more than one meeting per week.[190] While we can only speculate about the meetings' contents, more concrete evidence exists. For instance, AT&T's infrastructure permitted the George W. Bush Administration to spy on the U.S. public.[191] The *New York Times* reported that AT&T expressed an "extreme willingness to help" the government uncover information about private citizens—without a warrant.[192] Via this collaboration, AT&T supplied the Bush White House with emails found on its servers, offered technical support to wiretap information flowing through the internet, and even "installed surveillance equipment in at least 17 of its Internet hubs on American soil… And its engineers were the first to try out new surveillance technologies invented by the [National Security Agency]."[193] In light of this and other events, activists have grown especially concerned about, as examples, Facebook's relationship with the U.S. government[194] as well as WeChat's connection with the China—as it appears the Chinese government spies on its people via this app.[195] So the

---

[186] Cecilia Kang, *Google, Post-Obama Era, Aggressively Woos Republicans*, N.Y. TIMES (Jan. 27, 2017), https://www.nytimes.com/2017/01/27/technology/google-in-post-obama-era-aggressively-woos-republicans.html.

[187] *See* Abbey Stemler, *Platform Advocacy and the Threat to Deliberative Democracy*, 78 MD. L.R. 105 (2018).

[188] *Id.*

[189] *Id.*

[190] *Revealed: Google Staffers Have Had At Least 427 Meetings at the White House over Course of Obama Presidency—Averaging More Than One a Week*, DAILY MAIL (Apr. 23, 2016), https://www.dailymail.co.uk/news/article-3554953/Google-staffers-meetings-White-House-staggering-427-times-course-Obama-presidency-averaging-week.html.

[191] Julia Angwin et al., *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. See also Ryan Singel, Bush Spy Revelations Anticipated when
Obama is Sworn in, Wired (Nov. 11, 2003), https://www.wired.com/2008/11/bush-spy-revelations-anticipated-when-obama-is-sworn-in/

[194] Kalev Leetaru, *Facebook as the Ultimate Government Surveillance Tool?*, FORBES (July 20, 2018, 3:15 PM), https://www.forbes.com/sites/kalevleetaru/2018/07/20/facebook-as-the-ultimate-government-surveillance-tool/#598da3c12909 ("much of the governmental use of Facebook's ad targeting tools revolves around using its publicly accessible targeting and reporting tools to understand things like which neighborhoods have the highest density of persons in a particular demographic that also have a particular interest of concern to the government. By running large numbers of parallel campaigns covering all of the permutations of a set of demographics and interests, governments can even learn which demographics are most associated with particular interests and which interests are most strongly correlated with particular demographics. Geographic reporting tools allow neighborhood-level identification of where those demographics and interests coincide, allowing surveillance resources to be increased in those areas."

[195] Eva Dou, *Jailed for a Text: China's Censors Are Spying on Mobile Chat Groups*, WALL ST. J. (Dec. 8, 2017, 7:40 AM), https://www.wsj.com/articles/jailed-for-a-text-chinas-censors-are-spying-on-mobile-chat-groups-1512665007?ns=prod/accounts-wsj ("In China's swiftly evolving new world of state surveillance, there are fewer and fewer private spaces. Authorities who once had to use informants to find out what people said in private now rely on

question is not whether governments have used private technology and data collection efforts to surveil individuals, or even whether this has happened in the United States, but to what extent.

We think that imposing antitrust liability for supracompetitive privacy could provide relief against political abuses of privacy. While autonomy of choice is a key feature of the political system,[196] as demonstrated earlier, market forces have yet to promote this quality. But because increased competition would force firms to consider consumers and users in crafting privacy policies, firms would likely display less willingness to perpetrate abuses on behalf, and in collaboration with, governments. Consider that state actors can reward platforms for their willingness to surveil users while consumers can impose costs once the program is detected—so long as the benefits exceed the costs, the firm is likely to comply with the government's request. However, as competition increases, the ability of consumers to impose costs on platforms mounts as well; at some level of competition, the expectation is that private companies would refuse to enable the government's efforts to spy. So given the Sherman Act's goals, we think that, privacy should be incorporated into antitrust law to ensure that "the fortunes of the people will not be dependent on the whim or caprice, the political prejudice, [or] the emotional stability of a few self-appointed men."[197]

B. Merger Policy

The volume of acquisitions by the dominant platforms is astonishing. For example, Google has made almost 200 acquisitions since 2001, spending billions in the process.[198] Finding an appropriate conceptualization of privacy within the consumer welfare analysis will thus impact merger analysis. In particular, as large platforms acquire smaller firms, principal questions include what data are they acquiring? How might that data surplus increase the comprehensiveness of user profiling? How much does the risk of data dissemination increase for consumers? Nevertheless, as with litigation under the Sherman Act, merger enforcement under the Clayton Act has given primacy to the manner in which a proposed merger affects prices.[199] So while debate exists about the proper framework for U.S. enforcement, merger policy should take the approaches used in other countries into account.[200]

Traditionally, the US and Europe's view on antitrust and privacy were in concert.[201] Europe, which too was influenced by the Chicago School, believed that monopolies were not

---

a vast web of new technology. They can identify citizens as they walk down the street, monitor their online behavior and snoop on cellphone messaging apps to identify suspected malcontents.").

[196] *Id.*; Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1911 (2013) (writing that privacy "enables situated subjects to navigate within preexisting cultural and social matrices, creating spaces for the play and the work of self-making").

[197] United States v. Columbia Steel Co., 334 U.S. 495, 536 (1948) (Douglas, J., dissenting); Khan *supra* note 24, at 742.

[198] *The Google Acquisition Tracker*, CB INSIGHTS, https://www.cbinsights.com/research-google-acquisitions (last visited Feb. 13, 2019).

[199] Clayton Act § 7, 15 U.S.C. § 18 (2012).

[200] STUCKE & GRUNES, *supra* note 23.

[201] *See* Giuseppe Colangelo & Mariatersa Maggiolino, *Big Data, Data Protection and Antitrust in the Wake of the Bunderskartellamt Case Against Facebook*, 1 ITALIAN ANTITRUST REV. 104 (2017), available at http://iar.agcm.it/article/viewFile/12608/11414.

intrinsically bad.[202] However, European officials have since begun to question the utility of isolating issues related to big data and privacy to the consumer protection sphere and away from the antitrust's scope. In 2016, the French Autorité de la Concurrence and the German Bundeskartellamt ("Federal Cartel Office") released a report explaining their views on privacy's relationship with antitrust law.[203]

> [E]ven if data protection and competition laws serve different goals, privacy issues cannot be excluded from consideration under competition law simply by virtue of their nature . . . . [T]here may be a close link between the dominance of the company, its data collection processes and competition on the relevant markets, which could justify the consideration of privacy policies and regulations in competition proceedings.[204]

In particular, the report argued that data can entail a source of market power when it creates barriers to entry.[205] While data is non-rivalrous—that is it can be copied at little to no cost—platforms can tightly control their data, as a strategic asset to maintain their lead over rivals.[206] As such, firms with the most data can exclusively reap the benefits of predicting user behavior and discerning trends before others. In order to compete with a dominant platform, a competitor must undertake the costly process of recreating massive amounts of data.

We can also begin to find evidence of this thinking from American enforcers. FTC Commissioner Pamela Jones Harbour raised privacy concerns during the Google and DoubleClick merger debates. While DoubleClick and Google were not direct competitors—one was an ad serving company, the other a search engine—Commissioner Harbour worried that the ultimately successful merger would "create[] a firm with vast knowledge of consumer preferences, subject to very little accountability."[207] Harbour also raised the issue of network effects which could destroy consumer choice among platforms since "achieving a dominant market position might change the

---

[202] Giovanni Buttarelli, *Strange Bedfellows: Data Protection, Privacy, and Competition*, 34 COMPUTER & INTERNET LAW. 1, 2 (2017).

[203] Autorité de la concurrence and Bundeskartellamt, *Competition Law and Data* (2016), http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf.

[204] *Id*. at 23—24.

[205] Furthermore, in 2018, the European Commissioner for Competition, Margrethe Vestager, stated "[i]n some areas, these data are extremely valuable . . . . They can foreclose the market—they can give the parties that have them immense business opportunities that are not available to others." Natalia Drozdiak, *EU Asks: Does Control of 'Big Data' Kill Competition?*, WALL ST. J. (Jan. 2, 2018, 9:34 AM), https://www.wsj.com/articles/eu-competition-chief-tracks-how-companies-use-big-data-1514889000. In 2016 Margrethe Vestager also stated that the "European Commission might start considering the impact of data also on mergers involving smaller companies, especially in cases when a firm snaps up another just to get hold of its data." Natalia Drozdiak, *Big Data to Play a Bigger Role in Future Merger Reviews, Says EU Antitrust Watchdog*, WALL ST. J. (Sep. 29, 2016, 10:34 AM), https://blogs.wsj.com/brussels/2016/09/29/big-data-to-play-a-bigger-role-in-future-merger-reviews-says-eu-antitrust-watchdog/?mod=WSJBlog.

[206] Howard A. Shelanski, *Information, Innovation, and Competition Policy for the Internet*, 161 U. PA. L. REV. 1663, 1679 (2013).

[207] Buttarelli, *supra* note 200; In the matter of Google/DoubleClick, F.T.C. File No. 071-0170, at 10, https://www.ftc.gov/sites/default/files/documents/public_statements/statement-matter-google/doubleclick/071220harbour_0.pdf(Dissenting Statement of Commissioner Pamela Jones Harbour) (internal citations omitted).

firm's incentives to compete on privacy dimensions."[208] The FTC echoed this sentiment when it reminded Facebook and WhatsApp about their duties to uphold privacy commitments and forebear from consolidating data after their merger.[209]

In turn, our research—while primarily focused on antitrust's prohibition of trade restraints and monopolies—contributes insights to merger policy. Keeping in mind that the HHI Index entails the primary means by which the courts gauge market concentration, our empirical treatment measures market concentration using this tool. Given the results, there is strong evidence that government enforcers should, in balancing whether to bless a merger, consider supracompetitive privacy as a potential ground for actionable harm. After all, we demonstrate that the costs of privacy arising in concentrated market are greater than in a more competitive market, which is the very injury sought to be prevented in merger enforcement. This, in turn, provides support for Commissioner Harbour's dissent to Google's acquisition of DoubleClick as discussed earlier.[210]

C. Rationality, Bounded Rationality, and Irrational Behavior

One of the most important discussions in both business law as well economics concerns whether people can be expected to act rationally. For instance, the laws of insider trading assume that individuals, in the aggregate, act rationally as they invest; in doing so, rational actors measure the costs and benefits of the possible strategies, selecting the option providing the greatest utility.[211] While reports suggest that people care about privacy,[212] our research questions whether consumers are indeed acting rationally when they accept the privacy costs of using platform technology. These observations implicate the field of behavioral economics, which rejects

---

[208] Harbour & Koslov, *supra* note 23. *Contra* Alessandro Acquisti, *From Economics of Privacy to the Economics of Big Data, in* PRIVACY, BIG DATA, AND THE PUBLIC GOOD: FRAMEWORKS FOR ENGAGEMENT 91 (Stefan Bender et al. eds, 2014) (arguing that Harbour and Koslov's views are overly simplistic).

[209] Letter From Jessica L. Rich, Dir. of the Fed. Trade Comm'n Bureau of Consumer Prot., to Erin Egan, Chief Privacy Officer, Facebook, and to Anne Hoge, General Counsel, WhatsApp Inc. (Apr. 10, 2014). Former FTC Commissioner, J. Thomas Rosch, has also argued that "Google has told consumers that everything it is doing in terms of gathering information about their shopping habits et cetera was for the benefit of consumers. In fact, this is wrong—that is a classic half-truth. Because everything they have done in that regard, in my judgment, was for the benefit of Google, and more specifically, in favor of Google search, over which they have monopoly power. And I think that is to some extent, in whole or in part, related to their position in respect to search. That's valuable to them, incredibly valuable to them, to attract advertisers." Ron Knox, *An Interview with Tom Rosh*, 16 GLOBAL COMPETITION REV. (Feb. 2013), https://globalcompetitionreview.

[210] In the matter of Google/DoubleClick, F.T.C. File No. 071-0170, at 10, https://www.ftc.gov/sites/default/files/documents/public_statements/statement-matter-google/doubleclick/071220harbour_0.pdf (Dissenting Statement of Commissioner Pamela Jones Harbour) (internal citations omitted).

[211] *See, e.g.*, Tom C.W. Lin, *Reasonable Investor(s)*, 95 B.U. L. REV. 461, 467 (2015) ("[T]he reasonable investor is generally understood to be the idealized, perfectly rational actor of neoclassical economics. The reasonable investor is presumed to operate rationally to maximize returns in the marketplace. Prior to making investment decisions, the reasonable investor is capable of reading and comprehending all the noise and signals in the marketplace that encapsulate formal disclosures, economic data, market trends, senseless speculation, and irresponsible rumors. As such, when given the requisite information, reasonable investors are able to properly price the risks and rewards of an investment.").

[212] Buttarelli, *supra* note 200; Elec. Privacy Info. Cntr., Complaint and Request for Injunction, Google & DoubleClick, Inc. (Apr. 20, 2007), epic.org/privacy.ftc.google.epic_complaint.pdf; DoubleClick, at 10 (dissenting statement of Commissioner Pamela Jones Harbour) (internal citations omitted).

neoclassical ideas of rationality[213] in favor of a paradigm that incorporates psychology and economics to investigate "what happens in markets in which some of the agents display human limitations and complications."[214] The basic tasks of behavioral economics are thus to determine, first, the ways in which the brain is hard wired to make poor decisions and, second, strategies to improve our decision making calculus. The "nudge" revolution, for example, stems from this field.[215]

Perhaps consumers underestimate or ignore the costs of privacy, causing individuals to adopt behaviors that a rational actor would not.[216] In this sense, any number of heuristics could explain why individuals bear the costs of lost privacy. Perhaps the zero-priced services of platforms prove so tempting that individuals may comprehend their lost privacy entails a greater cost, yet the immediate benefits of platform services generate irrational behavior. This is akin to spending recklessly with a credit card: even though consumers might understand the long term costs of their purchases exceed the benefits, the joy of immediate gratification leads to irrationality. If so, the paucity of secure platforms on the market might be attributable to consumers who irrationally fail to value such a product. In other words, the prevailing lack of privacy might be the market's response to irrational actors.

Actors could also be laboring under bounded rationality, limited by incomplete information.[217] An essential quality of market efficiency is adequate information to make a decision.[218] The term bounded rationality means that actors have, in the aggregate, the faculties to make effective decisions, yet their lack of information prevents them from doing so. Recall the Cambridge Analytica scandal made possible by society's ignorance that Facebook could and would use personal information in such a manner. Perhaps users would have acted differently if better information existed to guide their choices. In turn, this market failure raises questions of whether consumers *would* have demanded greater privacy if only they had better information about the attendant costs and benefits.

The last option is that consumers are rational and informed. In light of the obvious benefits of free or low-priced services, yet the speculative harm of privacy, the decision to use a platform may be completely rational. Indeed, few consumers are likely to pinpoint an exact harm caused by Uber, for example, yet they can calculate the economic and personal benefits of using Uber versus a taxi. The point is that, considering the costs and benefits of all available options, it could be rational for individuals to prefer free and low-cost platform services, discounting the speculative dangers.

---

[213] Neoclassical economics is grounded in rationality, meaning that groups of people tend to select the behavior offering the most benefits with the least costs. *See generally* John Cirace, *When Are Law and Economics Isomorphic?*, 39 GOLDEN GATE U. L. REV. 183, 189 (2009) (explaining the role of rationality in the study of economics).

[214] Sendhil Mullainathan & Richard H. Thaler, *Behavioral Economics* (Nat'l Bureau of Econ. Research, Working Paper No. 7948 2001). *See also* Amitai Etzioni, *Behavioral Economics: Toward a New Paradigm*, 55 AM. BEHAV. SCIENTIST 1099, 1099 (2011).

[215] *See, e.g.*, Todd Haugh, *Nudging Corporate Compliance*, 54 AM. BUS. L.J. 68 (2017) (using behavioral economics to explain aspects of corporate compliance).

[216] *See generally*, Nathan Newman, *The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google*, 40 WILLIAM MITCHELL L. REV. 849 (2014)

[217] *See generally* Russell Korobkin, *Bounded Rationality, Standard Form Contracts, and Unconscionability*, 70 U. Chi. L. Rev. 1203, 1216–17 (2003) (explaining bounded rationality and information); Herbert A. Simon, *A Behavioral Model of Rational Choice*, 69 Q.J. ECON 99 (1955) (introducing and defining bounded rationality).

[218] *See* Roger J. Dennis, *Materiality and the Efficient Capital Market Model: A Recipe for the Total Mix*, 25 WM. & MARY L. REV. 373, 374-75 (1984).

Nevertheless, considering the importance of rationality to the law as well as economic theory, our research contributes to the behavioral economics literature by posing questions about whether consumer's rationally understand the costs and benefits of privacy.[219] We hope that future projects will build off this Article's research to study consumer rationality within platform markets.

D. Future Research

We invite future research to improve our methods. The lack of quantitative data about the causes of privacy injuries is likely due to the difficulty of designing such a study. In this sense, our treatment is one this Article's most significant contributions. That said, we hope that our attempt to measure privacy costs relative to market concentration may inspire other academics to devise additional, and perhaps, better methods. Beyond quantitative treatments, we think that case studies could illustrate our theory by delving into specific examples of platforms failing to protect privacy due to a lack of competition. One could also study the costs borne to platforms after a data breach relative to the costs incurred by society.

Conclusion

Antitrust is principally concerned with prices and output, yet tech giants offer goods and services for below-market prices. In turn, antitrust is generally agnostic about the business of tech giants as well as their responsibility for privacy injuries. Given that the commercialization of data and the attendant privacy injuries reflect the modern nature of business—as opposed to classical price competition—antitrust must modernize to address the dangers that inadequately protected data pose to consumers.

[219] The European Competition Commissioner, Margrethe Vestager, stated that "[v]ery few people realize that, if you tick the box, your information can be exchanged with others . . . . actually, you are paying, a price, an extra price for the product that you are purchasing. You give away something that was valuable. I think that point is underestimated as a factor as to how competition works." *Interview with Margrethe Vestager*, MLEX MARKET INSIGHT (Jan. 2015), https://mlexmarketinsight.com/insights-center/reports/interview-with-margrethe-vestager; STUCKE & GRUNES, *supra* note 23, at 9—10.