Infracompetitive Privacy

Gregory Day & Abbey Stemler*

ABSTRACT: One of the chief anticompetitive effects of modern business lies in antitrust’s blind spot. Platform-based companies (“platforms”) have mastered a business model whereby they offer users “free” and low-priced services in exchange for their personal information. With this data, platforms can design products, target advertising, and sell user information to third parties. The problem is that platforms can inflict greater costs on users and markets in the form of lost privacy than the efficiencies generated from their low prices. As an example, users spend billions of dollars annually to remedy privacy breaches and, indirectly but alarmingly, many users participate without realization in experiments designed to manipulate their behaviors, compromising their agency. But because antitrust’s framework typically uses consumer prices to measure welfare, platforms and privacy injuries have largely avoided antitrust scrutiny.

We argue that insufficient competition enables platforms to capture the economic benefits of data while externalizing the costs of protecting it. 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, an increase of 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. 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.

I. INTRODUCTION

II. THE UNIQUE COMMERCIAL NATURE OF TECHNOLOGY PLATFORMS

A. THE DOMINANT PLATFORMS AND THEIR BUSINESSES

B. CAPTURING AND EXTRACTING VALUE FROM DATA

---

* Assistant Professor, University of Georgia, Terry College of Business, Courtesy Appointment, University of Georgia School of Law.

** Assistant Professor, Indiana University, Kelley School of Business; Faculty Associate, Berkman Klein Center for Internet and Society at Harvard University; Consultant, World Bank Group; Affiliate, Ostrom Workshop.
At first blush, Google’s acquisition of the “smart” thermostat manufacturer, Nest Labs, was as astonishing as it was perplexing. 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? It is hard to overstate the modern value of data. Platform-based technology firms ("platforms") thrive by attracting users with "free" and low-priced services, enabling these companies to mine, exploit, and market their users’ data to third parties. Google, for example, is able to capture personal information from Gmail accounts while Uber can, as reports indicate, track certain user activities even after one has deleted the company’s application ("app").

The deal offered by platforms is this: Individuals may enjoy "free" or 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.10

Platforms can, however, inflict a greater cost on users in the form of lost privacy, outweighing the efficiencies generated by low prices. 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 theft11 and data breaches.12 Enabled by inadequate security, hackers alone impose between $375 and $500 billion in damages per year.13 More subtly yet perhaps more importantly, platforms can manipulate their users’ behaviors, prompting observers to remark that technology firms are compromising human agency.14 In fact, this landscape may qualify as a market failure—a condition whereby the market systemically encourages actors to engage in inefficient behaviors15—as platforms have little incentive to bolster data security as long as they can avoid scrutiny.

We demonstrate that “infracompetitive privacy” is the root of the problem. The term “supracompetitve” almost always refers to supracompetitive pricing—defined as the high prices a monopolist charges in the absence of competition16—which is the primary injury that antitrust law condemns.17 We assert that, like prices, privacy relies on competition. Because


14. See infra Section III.B.4 (discussing the contours of decisional privacy).

15. 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.”).


17. 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,
an array of platforms compete in markets devoid of meaningful competition, they enjoy insulation from market forces which incentivizes them to pass the burdens of protecting privacy onto users. Disguising this market failure is the cheap or “free” price of platform services—i.e., low prices create the illusion of vigorous competition. If technology markets were sufficiently competitive, as we explain, firms would enhance their privacy safeguards to vie for users.

Given that insufficient competition may 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 so far 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. Because antitrust law is solely meant to promote the economic interests of consumers, antitrust courts have typically conditioned liability on evidence that the defendant raised prices (i.e., supracompetitive prices) or restricted output (which produces supracompetitive prices). 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. Perhaps but it is the ability to charge supracompetitive prices that is the sine qua non of market power.” (quoting FTC v. Actavis, Inc., 570 U.S. 136, 157 (2013)).


See David N. Cicilline & Terrell McSweeney, 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 [https://perma.cc/6C4D-TVKB].


23. 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 Peter Swire, Protecting Consumers: Privacy Matters in Antitrust Analysis, CTR. FOR AM. PROGRESS (Oct. 19, 2007, 9:00 AM), http://www.americanprogress.org/issues/regulation/news/2007/10/19/3554/pro...
antitrust’s architects never foresaw an era when firms could render anticompetitive effects without charging prices.

We assert that antitrust should condemn anticompetitive practices leading to inadequate privacy. 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 de facto antitrust immunity for lapses in privacy, we can expect them to externalize the costs of protecting data. To illustrate our case, data by IBM suggests a relationship between monopoly power and privacy breaches; consumers seem to punish firms for costly data breaches except in concentrated markets. We think that consumers do demand heightened privacy, yet firms in concentrated industries—e.g., most platform markets—are able to resist pressures to supply it. If monopolists can better survive a privacy breach, market power may encourage 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”), 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, politicians, and activists have begun to question whether the Sherman Act should be expanded beyond its dominant scope of promoting competitive prices—colloquially known as “hipster antitrust.”

antitrust-analysis [https://perma.cc/CKA3-YDMD] (“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.” (quoting Sen. Herb Kohl)).


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 monopolists. We contribute to this literature by demonstrating that antitrust is poorly equipped to remedy the anticompetitive effects of modern business; privacy is a function of competition and that the resulting costs are economic. We also support the belief held by international authorities that antitrust’s relationship with privacy must be examined—e.g., the decision by the German competition authority to condemn Facebook’s use of data. So in shedding economic light on privacy, and given the obsolescence of conventional pricing, we contribute to the greater debate about whether privacy should fit into antitrust’s framework.

This Article proceeds in six parts. Following the introduction, Part II 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 III 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 IV asserts that the cost of inadequate privacy is attributable to uncompetitive markets in 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 V 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. Part VI concludes the Article.

II. 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, 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 can accrue and maintain monopoly power. This Part reviews the dominance of the leading platforms

[https://perma.cc/NQL5-852D] (explaining the term “hipster antitrust” and giving arguments both for and against it); see, e.g., Khan, supra note 20, at 737–39 (arguing that antitrust must acknowledge more anticompetitive effects that prices and output).
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 20 platforms—almost $6 trillion—exceeds a quarter of the U.S. economy, yet the scale of these platforms is far from their greatest distinguishing feature. 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 those of previous generations when competition pressured firms into lowering their goods’ prices to the marginal cost of production. To make the platforms’ model viable, they surveille users’ interactions with the platform and other users to generate data—recording every click, swipe, and choice—contrary to how conventional venues, such as a shopping mall, enabled people to purchase goods with relative anonymity. A platform can even, depending upon its privacy policy, observe users who have ceased engaging the platform, as software may continuously run in a device’s background. To provide context to “big tech,” 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. From this narrow focus, Amazon grew into the world’s largest store—worth more than Walmart, Target, Macy’s, Costco, and Kohls combined. Today, Amazon controls roughly 50 percent of the e-commerce market, claiming more Amazon Prime subscribers in the United States than gun owners. As this consumer base expands,

---


observers have remarked that Amazon has “deeper penetration into the private lives and desires of consumers than any other company.”

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 effectively than its rivals—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 personal, social, and political preferences of the over 35 million Americans who have purchased an Alexa.

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. 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.” 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 35 minutes per day on the platform (this number grows considerably if one includes the amount of time

32. Bob Pisano, We are Letting Amazon and Apple ‘Avoid Taxes, In invade Privacy, and Destroy Jobs,’ Says NYU Professor, CNBC (Oct. 3, 2017, 4:30 PM), https://www.cnbc.com/2017/10/02/scott-galloway-the-four-amazon-apple-google-facebook.html [https://perma.cc/4QZ6-BUT7].
36. Id.
spent on its subsidiaries, Instagram and WhatsApp).  

Embellishing Facebook’s market share, Facebook collects nuanced information about their users’ preferences, friends, and locations as they utilize the platform. Indeed, by exploiting data and network effects, Facebook has emerged as the dominant social network, generating over $40 billion of revenue in 2017 from advertising.

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. Google now accounts for around 90 percent of the world’s searches through its various portals (Google Search, Google Image Search, YouTube, and Google Maps). In 2016, Google earned profits of over $20 billion as well as boosted its cash flow by 23 percent. These revenue sources have enabled Google to not only acquire competitors but also to build an infrastructure featuring data centers and fiber optic cables connecting the world, furthering its market power. Indeed, Google has successfully integrated into its users’ daily lives by introducing lines of hardware including, Nest, Google Home, and Chromecast.

---


39. GA LLOWAY, supra note 30, at 96–109. Sometimes, Facebook tracks user information even after they log off the platform.

40. See infra Section II.C.


44. Ip, supra note 41.

45. GA LLOWAY, supra note 30, at 5.


Uber. Among ridesharing platforms, Uber reigns supreme with a 77 percent share of the market and valuation in the hundreds of billions.\textsuperscript{48} Although not the original ridesharing platform, Uber pioneered the prioritization of growth over profits model, making end-runs around regulations.\textsuperscript{49} 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 experience; one of its chief innovations includes the use of economic incentives in the form of “surge pricing” to nudge drivers toward high demand areas.\textsuperscript{50} With these techniques, Uber has accrued a critical mass of drivers and riders to draw even more users into the app.\textsuperscript{51} The result is an efficient transportation service enjoyed by consumers at lower costs than traditional ride services.

Other Players. Conventional firms have similarly embraced platform-business models. For example, a majority of Domino’s employees work in its data analytics section, shifting the company from a brick and mortar pizza chain into a tech firm that happens to sell pizzas.\textsuperscript{52} 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


\textsuperscript{49} Eric Biber et al., Regulating Business Innovation as Policy Disruption: From the Model T to Airbnb, 70 VAND. L. REV. 1561, 1563, 1581–82 (2017).


\textsuperscript{51} See generally DAVID S. EVANS & RICHARD SCHMALENSEE, MATCHMAKERS: THE NEW ECONOMICS OF MULTISIDED PLATFORMS 207 (2016) (discussing the concept of “critical mass,” which is necessary for a two or more-sided marketplace to “ignite” and have self-sustaining growth).

pizza retailer.\textsuperscript{53} Along the same lines, Netflix has 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.\textsuperscript{54} 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, 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.\textsuperscript{55} Airbnb tracks a consumer’s location and preferred devices to target listings.\textsuperscript{56} Uber’s data analytics have likewise enabled it to undersell the taxi industry as well as innovate a self-driving car program,\textsuperscript{57} generating $6.8 billion of revenue in the United States alone.\textsuperscript{58}

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.\textsuperscript{59}


\textsuperscript{54} Keegan Green, Evolution of Netflix, ENGADGET (Mar. 21, 2016), https://www.engadget.com/2016/03/21/evolution-of-netflix [https://perma.cc/N5C5-PDSM].


\textsuperscript{58} Peter Cohen et al., Using Big Data to Estimate Consumer Surplus: The Case of Uber 1 (Nat’l Bureau of Econ. Research, Working Paper No. 22627, 2016), http://www.nber.org/papers/w22627.pdf [https://perma.cc/5QTQ-UCCQ]. Remarkably, this study was based on Uber offering a data set of almost 50 million individual observations to researchers. Id.

Estimates show that social media advertising revenue in the United States exceeded $23 billion in 2018. Although Facebook’s CEO and founder, Mark Zuckerberg, claimed before Congress in 2018 that Facebook does not sell data, which mirrors Google’s position, Facebook generates revenue by profiling users and then assisting advertisers in targeting them—essentially commercializing users without necessarily “selling” their data.

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. The project provided a link for some users to find their polling places, accompanied by a clickable button indicating “I Voted,” and a snapshot of some of the user’s friends who had already voted. A second group of users were shown the link to polling places and the “I Voted” button, but excluded the profile pictures. Facebook found that users who received the added feature of their friends were 0.39% more likely to vote. 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.

Further animating data’s value, consider the prices paid for platforms in corporate mergers. Facebook bought WhatsApp, the messaging platform, for $20 billion when the platform had less than $10.5 million in revenue and only 50 employees. A sophisticated understanding of finance is unnecessary

---


64. Bond et al., supra note 63, at 295–96.


to realize that Facebook had primarily acquired WhatsApp for its 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 listeners’ music preferences.67

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, so that Google may commercialize data derived from seemingly mundane household behaviors.68 And 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 by 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)69—can enhance a platform’s market


68. Team, supra note 3.

power. The initial study of network effects focused on positive direct network externalities; that is, when a user joins a network, she benefits similar users on that network.\(^\text{70}\) 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.\(^\text{71}\)

Since all sides of the transaction benefit as the network grows, network effects magnify growth, furthering the platform’s size and popularity.\(^\text{72}\) 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.\(^\text{73}\)

Beyond traditional network effects, firms can also marshal \textit{data} network effects.\(^\text{74}\) 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.\(^\text{75}\) As Scott Galloway explained, “Google, unlike most products, ages in reverse, becoming more valuable with use.”\(^\text{76}\)

Then, upon gaining momentum, platforms can pursue complementary offerings to feed their algorithms with additional users and data. Google


\(^{72}\) We say “generally” because the Cambridge Analytica scandal revealed how easy it was for Facebook’s app developers to access large amounts of user data. See \textit{supra} notes 127–32 and accompanying text.


\(^{76}\) GALLOWAY, \textit{supra} note 30, at 5.
offers G Suite and Maps in addition to its search engine. Uber Eats has likewise surpassed competition in the market for food delivery with its understanding of maps and logistics gleaned from its parent, Uber. 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.

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. 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 of their investment.

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. 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.”

Further, akin to how Facebook allegedly pressured Six3Three to sell their company, critics assert that the leading platforms acquire potential rivals to prevent upstarts from threatening their market power. This is known as the Kronos effect after the Greek God who ate his offspring to protect his supremacy. For instance, Google took the lead in the video sharing market by acquiring its chief rival, YouTube. 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. Beyond Facebook, which bought competitors Instagram and WhatsApp among others, Amazon survived its price battle with Diapers.com by purchasing the company.

Although some commentators assert that these tactics and transactions should violate antitrust, as they appear to suppress competition, it is difficult

84. GALLOWAY, supra note 30, at 4–5.
86. Victor Luckerson, A Decade Ago, Google Bought YouTube—and It Was the Best Tech Deal Ever, THE RINGER (Oct. 10, 2016, 8:30 AM), https://www.theringer.com/2016/10/10/16032554/google-youtube-acquisition-10-years-tech-deals-69fdebe18a6 [https://perma.cc/L35G-G5RF] (“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.”).
to construct an antitrust claim. This is because, as Part III explains, the typical antitrust analysis relies on evidence of artificially high prices or reduced output, which the free and cheap prices of platform services belies.

So in light of experimentation, machine learning, network effects, and corporate acquisitions, most leading platforms lack serious competition. 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). But because users pay for these services with personal information instead of money, platforms can generate privacy side effects borne by users without triggering antitrust scrutiny. The following Part explores the privacy externalities suffered by consumers, markets, and governments.

III. 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. 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”—the law has poorly established the boundaries of one’s privacy rights. In turn, platforms and other companies enjoy an almost unrestrained

---

89. Robert Reich, Break Up Facebook (and While We’re at It, Google, Apple and Amazon), GUARDIAN (Nov. 20, 2018, 3:00 AM), https://www.theguardian.com/commentisfree/2018/nov/20/facebook-google-antitrust-laws-gilded-age [https://perma.cc/H3FZ-PHF4].
90. Newman, supra note 24, at 160.
ability to observe and manipulate users, as the United States lacks a comprehensive set of privacy protections vis-à-vis companies and consumers.95

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).96 And while the Federal Trade Commission ("FTC") is tasked with protecting consumer privacy under § 5 of the FTC Act, the 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).97 Due to this landscape, the boundaries of one's privacy rights remain elusive and ill protected.98

Daniel Solove’s seminal taxonomy of privacy harms is, however, a useful starting point for discussing the privacy implications of technology.99 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.100 As privacy moves away from one’s control, individuals increasingly lose ability to prevent the collection, analysis, and dissemination of their data and more disturbingly, their ability to exercise free will when targeted via hidden means.101

---

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


100. Solove, supra note 99, at 489. Decisional privacy violations involve interfering with people’s ability to make their own decisions. Id. at 587.

101. Id. at 491–99.
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, Airbnb, Adobe, and Slack.103 Similarly, Facebook harvests locational data even when users are not using the app so as to help advertisers target them.104

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.”105 It is, however, unlikely that these efforts can obstruct all monitoring.106 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.107 This is partially because platforms bewilder

---

102. We broadly define privacy violations as “privacy harms;” however, the first three harms within Solove’s taxonomy are direct and indirect quantifiable costs on consumers. The fourth harm, is more amorphous, and we did not attempt to quantify it.


105. 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, TECHCRUNCH, https://techcrunch.com/2018/04/14/how-to-save-your-privacy-from-the-internets-clutches [https://perma.cc/NR2X-2AB].


consumers with complex privacy policies found in contracts of adhesion. Coupling this with 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 0.36% of the market share) which is presumed to lack Google’s quality (with 76.06% of the market).

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 smartphone to advertise businesses located in a close vicinity to that individual. Users are even tracked in stores via Bluetooth technology to tailor offers within the store’s own mobile app. In


110. 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 [https://perma.cc/73FG-YF9B] (“Snapchat introduced two new ways for marketers to reach target audiences based 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.”).

111. Michael Kwet, In Stores, Secret Surveillance Tracks Your Every Move, N.Y. TIMES (June 14, 2019), https://www.nytimes.com/interactive/2019/06/14/opinion/bluetooth-wireless-tracking-privacy.html [https://perma.cc/D49W-YL2W]; see 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 [https://perma.cc/ALF8-KPQ4] (”[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 . . . . [T]hey were able to easily identify the
fact, 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 swaying or is being held at an odd angle.\footnote{Arwa Mahdawi, Uber Developing Technology That Would Tell If You’re Drunk, \textit{GUARDIAN} (June 11, 2018, 12:27 PM), https://www.theguardian.com/technology/2018/jun/11/uber-drunk-technology-new-ai-feature-patent [https://perma.cc/522A-KZ9Q].}

While observers might assume that these programs analyze anonymized data and thus, it is benign, recent reporting suggests otherwise.\footnote{Jennifer Valentino-DeVries et al., \textit{Your Apps Know Where You Were Last Night, and They’re Not Keeping It Secret}, \textit{N.Y. TIMES} (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html [https://perma.cc/H8QG-JEYD].} When platforms analyze general data to discover broad patterns and preferences, evidence suggests that users may experience deep unease and other psychological issues based on eroding privacy.\footnote{Ian Tucker et al., \textit{Experiencing the Surveillance Society}, \textit{29 PSYCHOLOGIST} 682, 684–85 (2016).} Increased recognition of these “big brother” capabilities of platforms can alter behavior, again, at a cost.

3. Harms from Disseminating Information

breach exposed the personal information of over 100 million individuals worldwide.\footnote{117} 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.\footnote{118}

In fact, the prevalence of data breaches masks the \textit{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.\footnote{119} The cybersecurity market is, in turn, expected to eclipse $170 billion in revenue by 2022.\footnote{120}

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.\footnote{121} Similarly, in 2018, Amazon gave customers between $5 and $100 gift cards per complaint as an apology for exposing their email addresses.\footnote{122} These
numbers pale in comparisons, however, to the hundreds of millions of dollars platforms pay globally to regulatory bodies for data breaches.\(^{123}\)

4. Harms from Manipulation Based on Information and Insights

In addition to direct outlays, a troubling aspect of data commercialization is the hidden dangers to decisional privacy.\(^{124}\) Buttressed by society’s poor understanding of the ways tech firms exploit data, consumers can unwittingly participate in experiments resulting in their augmented behavior.\(^{125}\) The Facebook Cambridge Analytica scandal of 2018 is an unfortunate example. Russian-American professor, Aleksandr Kogan, developed a personality quiz app in 2014.\(^{126}\) With it, he received permission from 270,000 Facebook users to mine their data for academic purposes.\(^{127}\) Unbeknownst to those users, Kogan gathered the personal data of their friends, including roughly 71 million Americans.\(^{128}\) Kogan then sold that personalized data to Cambridge Analytica, a political firm hired by the Trump Campaign.\(^{129}\) 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 . . . .”\(^{130}\) The uproar incited by this
scandal prompted congressional inquiries and perhaps the future regulation of Facebook.131

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.132 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.133 Facebook has also confirmed that it collects data from non-Facebook users—a surprising admission to many, including the U.S. Congress.134

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... At some deep level we don’t even really understand how they’re producing the behavior we observe. This is the essence of their incomprehensibility.135

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. The next Part 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.

IV. ANTITRUST AND INFRACOMPETITIVE PRIVACY

The privacy injuries endemic to technology markets should, but do not currently, entail a harm that is recognized by antitrust law. We demonstrate that privacy is a product of competition; in this sense, increased competition would compel platforms (and other companies for that matter) to harvest and exploit data more securely. Although antitrust’s current form could seemingly remedy infracompetitive privacy—as antitrust’s purpose is to cure the effects 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, Section IV.A traces antitrust’s history to explain in Section IV.B why courts and administrative agencies have yet to recognize infracompetitive privacy as something that antitrust may remedy. Then, Section IV.C demonstrates the error in antitrust’s current framework; 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. Additional support is provided in Section IV.D. Given these results, Section IV.E explains that privacy, competition, and markets would benefit if antitrust enforcement condemned infracompetitive privacy.

A. ANTITRUST EXPLAINED THROUGH A HISTORICAL CONTEXT

Antitrust’s history explains 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 sought to reform antitrust law in the 1970s, the judiciary had a poor understanding of economics, causing antitrust to seek improper and unclear goals. 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.\textsuperscript{139} Compounding matters, Congress drafted the Sherman Act using broad language, providing few clues or methods to discern illegal conduct.\textsuperscript{140}

It was instead the courts’ task to define antitrust’s scope,\textsuperscript{141} which they labored to do.\textsuperscript{142} 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.\textsuperscript{143} 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.\textsuperscript{144} But as the Chicago School would argue, 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 efficient markets.\textsuperscript{145} 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


\textsuperscript{140} Vaheesan, supra note 27, at 374–75 (“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.”).

\textsuperscript{141} Nat’l Soc’y of Prof’l Eng’rs 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.”).

\textsuperscript{142} 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 maximand 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. While this view may not be entirely gone, it is certainly greatly diminished in modern antitrust jurisprudence.”).

\textsuperscript{143} Vaheesan, supra note 27, at 372.

\textsuperscript{144} See Wright, supra note 138, 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.”).

larger firms rather than many small businesses.\textsuperscript{146} It was misguided, as their theory insisted, to condemn companies that had obtained monopoly power or destroyed competition by virtue of offering superior products at cheaper prices; efficient markets are, after all, supposed to produce better goods at lower prices.\textsuperscript{147} To these economists, antitrust was diminishing consumer welfare by imposing liability on market enhancing behaviors.\textsuperscript{148}

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.\textsuperscript{149} In turn, because increased economic efficiency is the most reliable benefit of competition,\textsuperscript{150} the courts narrowed antitrust’s scope to promoting the economic interests of consumers as opposed to protecting individual competitors.\textsuperscript{151} To achieve this end today, almost all antitrust offenses require evidence that the challenged act harmed “consumer welfare,”\textsuperscript{152} typically in the form of increased prices or restricted output (as

\textsuperscript{146} Alan J. Meese, Monopolization, Exclusion, and the Theory of the Firm, 89 MINN. L. REV. 743, 772–93 (2005) (describing “price theory” which assumed that many firms acting in perfect competition created the lowest, most efficient prices).

\textsuperscript{147} 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.”).

\textsuperscript{148} Bork, supra note 139, at 405–07 (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).


\textsuperscript{151} Levine v. Cent. Fla. Med. Affiliates, Inc., 72 F.3d 1538, 1551 (11th Cir. 1996) (“The antitrust laws are intended to protect competition, not competitors . . . .”).

\textsuperscript{152} 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., FreeFreeHand Corp. v. Adobe Sys. Inc., 852 F. Supp. 2d 1171, 1185 (N.D. Cal. 2012) (declaring diminished innovation to entail an antitrust injury); HM Compounding Servs., Inc. v. Express Scripts, Inc., No. 4:14-CV-1858 JAR, 2015 WL 4162762, at *5–6 (E.D. Mo. July 9, 2015) (treat reduced consumer choice or variety as an anticompetitive effect under antitrust law).
diminished output should produce artificially high prices). 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 considered inappropriate. 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.

The primary test used to determine whether a restraint of trade violates antitrust law is known as the rule of reason test. Under this test, conduct deserves liability if its anticompetitive effect (e.g., high prices or restricted output) outweighs whatever procompetitive benefits resulted (e.g., increased innovation).

Given this framework, the next section discusses the reasons that platforms appear to enjoy antitrust immunity for the privacy harms discussed in Part III. 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. THE SALIENCY OF 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. The leading antitrust treatise lacks a discussion on the matter and the word “privacy” does not appear once in a preeminent law review article examining

153. Peritz, supra note 147, at 106.
156. See In re Loestrin 24 Fe Antitrust Litig., 814 F.3d 535, 544–45 (1st Cir. 2016).
157. Cal. Dental Ass’n v. FTC, 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.” (quotations omitted) (citations omitted)).
158. But see U.S. DEP’T OF JUSTICE & THE FED. TRADE COMM’N, HORIZONTAL MERGER GUIDELINES 2 (2010) (explaining that anticompetitive effects can “be manifested in non-price terms and conditions that adversely affect customers”).
anticompetitive effects.\textsuperscript{160} As a leading scholar in the field noted, antitrust is simply unconcerned with the costs of privacy.\textsuperscript{161}

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 likely conclude that tech markets reflect sufficient consumer welfare.\textsuperscript{162} So even if one could link a privacy injury to anticompetitive behavior—which we argue in the following Section—a court would be unlikely to impose antitrust liability without evidence of supracompetitive prices.

Perhaps antitrust could promote privacy if the courts or scholarship gave primacy to the privacy costs suffered by consumers, including those who had not even used the culprit technology. Although 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,\textsuperscript{163} For instance, academics have suggested that privacy injuries could entail a type of non-price injury, but have cautioned against this framework because

\textsuperscript{160} See generally Richard D. Cudahy & Alan Devlin, Anticompetitive Effect, 95 MINN. L. REV. 59 (2010) (omitting any discussion on privacy injuries). 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.


\textsuperscript{161} Newman, supra note 24, 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.").


equating privacy to quality would make enforcement overly subjective and unprincipled.\textsuperscript{164}

A couple works have sought to fit tech businesses into antitrust’s current framework by suggesting that a platform could violate antitrust law if it used monopoly power to underpay for data, though dismissing the costs of privacy.\textsuperscript{165} 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 degree, individuals value their privacy vis-a-vis low-priced services.\textsuperscript{166}

For these reasons, the few works exploring antitrust’s treatment of platforms have largely avoided 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 infracompetitive privacy creates measurable economic costs suffered by consumers akin to monopoly prices.

\section*{C. \textit{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 is that inadequately protected data can derive from a lack of competition, and that more competition would help alleviate this harm. To make this case, notice that privacy injuries constitute a form of market failure.\textsuperscript{167} 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


\textsuperscript{166} 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, 782 (2010). Furthermore, as Manne and Sperry 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, \textit{supra} note 163, at 4.

\textsuperscript{167} 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, \textit{Achieving Efficiency Through Collusion: A Market Failure Defense to Horizontal Price-Fixing}, 51 CALIF. L. REV. 243, 269–71 (1963) (discussing negative externalities as a form of market failure).
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 their 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.168 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.

2. Information

A chief problem explaining the prevalence of infracompetitive 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.169 Consumers could also base their decisions 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 infracompetitive privacy given their inability to punish offending firms.\textsuperscript{170}

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 to advertise this fact to consumers, raising the attention paid by users to privacy matters.\textsuperscript{171}

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, incentives 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.

\textsuperscript{170} Consumers become impervious to data breaches as it becomes the norm; therefore, will be 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.”


D. ADDITIONAL SUPPORT

We, in fact, ran regressions supporting the existence of a relationship between privacy and competition, though we warn against relying too heavily on the results due to data and analysis limitations, as we will explain shortly. Consumers do seem to prefer privacy, yet the nature of market power enables platforms to ignore this demand. This suggests 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. Our hope is that the following illustrations may inspire other researchers to devise empirical methods to study this subject, given the paucity of current data.

We analyzed data provided by IBM regarding the costs of a data breach, as well as other publicly available sources, to suggest that companies wielding market power have incentives to externalize privacy costs. The dependent variable, \textit{Abnormal Churn Rate}, refers to the rate at which customers quit utilizing a company beyond the expected level. Our independent variable is an industry’s level of \textit{Market Concentration}, derived from the Herfindahl–Hirschman Index ("HHI").\footnote{We calculated HHI statistics from Compustat data. HHI data is computed by squaring the market share of each firm competing in an industry and then adding the resulting figures. The Index ranges from 10,000 to 0, with the former number indicating a perfect monopoly, whereas the latter designates perfect competition. \textit{FEC 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.").} The other key independent variable is the \textit{Cost of a Data Breach per Capita}, measuring the cost of a privacy lapse in an industry per record breached. Because consumers are likely to take notice of a costly breach—an assumption supported by IBM—industries in which a costly data breach occurs may experience a lower \textit{Abnormal Churn Rate}, except when it lacks competition.\footnote{\textit{PONEMAN INST.}, 2015 COST OF DATA BREACH STUDY: GLOBAL ANALYSIS 14 (2015), \url{https://nhlearningsolutions.com/Portals/0/Documents/2015Cost-of-Data-BreachStudy.PDF} [https://perma.cc/89fCB-UVDK].} To control for intervention factors: (1) a proxy of the level of \textit{Intangible Property} collected by an industry was added since a firm that collects little consumer information is unlikely to levy significant costs;\footnote{From Compustat data, we identified the top 20 firms holding intangible property per industry and year, and then created a variable for the average of their holdings.} and (2) we also accounted for economic changes per year via GDP data. We analyzed this data using an Ordinary Least Squares ("OLS") analysis, which tracks the hypothesized relationship as a linear function.

We should note that our analysis suffers from structural limitations and thus should serve as an illustration rather than as strong evidence. The primary issue is the paucity of data on this subject; for instance, this is a “small n” study, meaning that we could derive better results if more observations were available. Second, we used Compustat data which canvasses only publicly
traded companies, meaning that we omitted private companies from our Market Concentration and control measures. Because public firms account for only a small subset of relevant firms, and since the choice to go public is far from random, the analysis suffers from a selection effect which could alter the results. Third, the industry types used by IBM are not neatly defined NAICS categories so we hand-coded and merged the Compustat data with the IBM categories; this was an imperfect process as it required many judgment calls. Fourth, HHI data is typically used to analyze more discrete markets than our purposes. While the mechanics of HHI should logically apply to broader industries, this quirk is worth highlighting. Although these shortcomings must be kept in mind, our theory may still reflect a snapshot of reality.

For our results, the variables Breach Cost and Market Concentration were both statistically significant: Breach Cost is positively correlated with Churn Rate while Market Concentration is negatively associated, indicating that firms lose customers as the costs of a breach mount, except when the firm controls a greater share of the market. In this latter situation, consumers seem to remain with firms lacking competition despite the costs of a breach. This may shed light on why platform companies have emphasized data collection over price competition: not only does the strategy appear to enable firms to build monopoly power using network effects, but it also helps them to evade antitrust scrutiny. Since modern antitrust is chiefly concerned about consumer prices while ignoring privacy, platforms can avoid scrutiny when exploiting big data—despite the real harms of anticompetitive practices. Indeed, it seems that consumers and markets bear much of privacy’s costs, generating incentives to offload the costs of privacy whether done intentionally or negligently. In other words, even if platforms suffer costs and embarrassment, firms in concentrated markets might be making the rational, yet socially deleterious, decision of offloading privacy costs onto society. The next Section reunites competition with antitrust policy.
Table 1. OLS Regression

<table>
<thead>
<tr>
<th></th>
<th>Model 1</th>
<th>Model 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abnormal Churn Rate</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Breach Cost</td>
<td>(0.0122378***)</td>
<td>(0.0122074***)</td>
</tr>
<tr>
<td></td>
<td>((0.0023827))</td>
<td>((0.0023648))</td>
</tr>
<tr>
<td>Market Concentration</td>
<td>(-0.0005884^*)</td>
<td>(-0.0005916^*)</td>
</tr>
<tr>
<td></td>
<td>((0.0003146))</td>
<td>((0.0003122))</td>
</tr>
<tr>
<td>Intangible Holdings</td>
<td>(0.0000239^{**})</td>
<td>(0.0000238^{**})</td>
</tr>
<tr>
<td></td>
<td>((0.00000986))</td>
<td>((0.00000979))</td>
</tr>
<tr>
<td>GDP Control</td>
<td>0.1960728</td>
<td>-0.0005916*</td>
</tr>
<tr>
<td></td>
<td>((0.3894989))</td>
<td>((0.381222))</td>
</tr>
<tr>
<td>Time Control</td>
<td>(-0.2859058^*)</td>
<td>(-0.3280497^{**})</td>
</tr>
<tr>
<td></td>
<td>((0.163019))</td>
<td>((0.1388719))</td>
</tr>
<tr>
<td>Constant</td>
<td>1.849823</td>
<td>2.459286^{***}</td>
</tr>
<tr>
<td></td>
<td>((1.452212))</td>
<td>((0.7961745))</td>
</tr>
<tr>
<td>Prob &gt; F</td>
<td>(0.0000^{***})</td>
<td>(0.0000^{***})</td>
</tr>
<tr>
<td>R-Squared</td>
<td>0.437</td>
<td>0.5198</td>
</tr>
<tr>
<td>No. of Observations</td>
<td>61</td>
<td>61</td>
</tr>
</tbody>
</table>

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

E. WHAT DOES THIS ALL MEAN

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 have risen above the competitive level.175

To do so, a plaintiff could compare the privacy economics of the challenged market to a more competitive market. Key would entail evidence of costs not incurred in the competitive market to protect one’s personal information. For instance, if plaintiffs could trace their injury to a monopolist whose privacy policy provided inadequate protection, then evidence of superior privacy regimes found in a comparable yet more 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 excess 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 § 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. 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 infracompetitive privacy resulted from 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 infracompetitive privacy under the Sherman Act are intuitive. First, as outlined in Part III, 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. And considering the difficulty of asking Congress to enact comprehensive privacy

---

176. For a survey of the leading hosted email providers suggests broad competition, including on privacy dimensions, see Daniel Brame, The Best Hosted Email Providers for 2019, PC MAG (Apr. 25, 2019, 9:52 AM), https://www.pcmag.com/roundup/360593/the-best-hosted-email-providers [https://perma.cc/KjU5-MBP]. See also, e.g., About FastMail, FastMail, https://www.fastmail.com/about/company.html [https://perma.cc/PHY9-AKSL] (“While other companies ask users to give up their privacy in exchange for email, we believe in treating our customers like people, not products.”).

177. See also supra Part IV (arguing that antitrust law must evolve to protect consumers from privacy harms).
regulations, the best answer lies in current law. In fact, antitrust is particularly well-suited for this 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 a) monopoly (per § 1 and § 2, respectively), enforcement of infracompetitive 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.

V. BROADER 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 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. These misgivings included the possibility that monopolists could unravel seminal institutions, thereby increasing autocratic tendencies. Today, in a similar fashion, a chorus of politicians and citizens have expressed concerns for the power marshalled by platforms to influence social institutions.

181. Pitofsky, supra note 179, at 1051–52.
Much of this anxiety extends beyond the extensive resources of platforms\textsuperscript{183} to include their ability to mobilize users politically.\textsuperscript{184} Through this capacity to manipulate decisional privacy, they can trigger users to act in malleable and predictable ways.\textsuperscript{185} 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.\textsuperscript{186}

Indeed, as platforms generate insights about populates, as well as sophisticated ways to alter behaviors, governments have established strong bonds with technology companies in hopes of benefitting from their capabilities.\textsuperscript{187} For instance, Google representatives held 427 meetings with the Obama White House, averaging more than one meeting per week.\textsuperscript{188} While we can only speculative 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.\textsuperscript{189} The \textit{New York Times} reported that AT&T expressed an “extreme willingness to help” the government uncover information about private citizens—without a warrant.\textsuperscript{189} 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

\begin{thebibliography}{18}
\bibitem{184} See generally Abbey Stemler, \textit{Platform Advocacy and the Threat to Deliberative Democracy}, 78 MD. L. REV. 105 (2018) (discussing the political implications of social media companies’ direct contact with their users).
\bibitem{185} Id. at 109–13.
\bibitem{186} See id. at 115 (“For example, during the 2012 Mexican election, the Institutional Revolutionary Party used bots to create Twitter trends that fired up public interest about irrelevant issues and controversies in order to distract people from stories that were harmful to the party.”).
\end{thebibliography}
new surveillance technologies invented by the [National Security Agency].”191
In light of this and other events, activists have grown especially concerned
about, as examples, Facebook’s relationship with the U.S. government192 as
well as WeChat’s connection with China—as it appears the Chinese
government spies on its people via this app.193
So the 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 infracompetitive privacy
could provide relief against political abuses of privacy. While autonomy of
choice is a key feature of the political system,194 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

191. Angwin et al., supra note 189.
192. 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 [https://perma.cc/UA3T-DUB5] (“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.”).
193. 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 [https://perma.cc/BHY8-PHVY] (“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 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.”).
194. Id.; see also 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”).
not be dependent on the whim or caprice, the political prejudices, [or] the emotional stability of a few self-appointed men."195

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.196 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.197 So while debate exists about the proper framework for U.S. enforcement, merger policy should take the approaches used in other countries into account.198

Traditionally, the United States’ and Europe’s views on antitrust and privacy were in concert.199 Europe, which too was influenced by the Chicago School, believed that monopolies were not intrinsically bad.200 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:201

[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

198. STUCKE & GRUNES, supra note 164, at 337–38.
could justify the consideration of privacy policies and regulations in competition proceedings.\footnote{202}

In particular, the report argued that data can entail a source of market power when it creates barriers to entry.\footnote{203} 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.\footnote{204} 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. Former FTC Commissioner Pamela Jones Harbour raised privacy concerns during the Google and DoubleClick merger debates.\footnote{205} 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.”\footnote{206} Harbour also raised the issue of network effects which could destroy consumer choice among platforms since “achieving a dominant market position might change the firm’s incentives to compete on privacy dimensions.”\footnote{207} The FTC echoed this sentiment when it reminded Facebook and WhatsApp about their duties.

\footnote{202. Id. at 25–24.}
\footnote{203. Id. at 11. 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-howcompanies-use-big-data-1514889000 [https://perma.cc/DA77-2SUU]. 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. (Sept. 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 [https://perma.cc/AVA5-G2JC].}
\footnote{204. Howard A. Shelanski, Information, Innovation, and Competition Policy for the Internet, 161 U. PA. L. REV. 1663, 1679 (2013).}
\footnote{206. Id. (citations omitted); Buttarelli, supra note 200, at 1.}
\footnote{207. Harbour & Koslov, supra note 166, at 794. 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).}
to uphold privacy commitments and forebear from consolidating data after their merger.208

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,209 which we examined earlier, government enforcers should, in balancing whether to bless a merger, consider infracompetitive 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


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.


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
While reports suggest that people care about privacy, 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 neoclassical ideas of rationality 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.” 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.

Perhaps consumers underestimate or ignore the costs of privacy, causing individuals to adopt behaviors that a rational actor would not. 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.

irresponsible rumors. As such, when given the requisite information, reasonable investors are able to properly price the risks and rewards of an investment.


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).


Actors could also be laboring under bounded rationality, limited by incomplete information.\textsuperscript{217} An essential quality of market efficiency is adequate information to make a decision.\textsuperscript{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.\textsuperscript{219} 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.

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.\textsuperscript{220} We hope that future projects will build off this Article’s research to study consumer rationality within platform markets.

\textbf{D. Future Research}

We invite future research on this topic. The lack of quantitative data about the causes of privacy injuries is likely due to the difficulty of designing such a study. Our hope is that others will measure privacy costs relative to market concentration using better data than we could find. Beyond

\begin{itemize}
\item \textsuperscript{219} Korobkin, supra note 217, at 1203.
\item \textsuperscript{220} Stucke & Grunes, supra note 164, at 9–10. The European Competition Commissioner, Margrethe Vestager, stated that \textit{“[v]ery few people realize that, if you tick the box, your information can be exchanged with others . . . . [A]ctually, 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 Mkt. INTERVIEW, Jan. 2015, at 5, available at https://mlexmarketinsight.com/insights-center/reports/interview-with-margrethe-vestager [https://perma.cc/T6X4-99DU].
\end{itemize}
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.

VI. 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.