PRIVACY AND ANTITRUST AT THE CROSSROADS OF BIG TECH

LAURA ALEXANDER

DECEMBER 16, 2021

AAI AMERICAN ANTITRUST INSTITUTE

TABLE OF CONTENTS

Summary of Major Conclusions 1

I. Introduction 3

II. The Complex Relationship Between Antitrust and Privacy Law 4

III. Antitrust Cannot Be a Complete Privacy Solution 7

IV. Antitrust and Competition as Part of a Broader Privacy Solution 16

V. Policy Can Fill the Gaps 18

VI. Policy Recommendations 21

AUTHOR

Laura Alexander is the American Antitrust Institute's Vice President of Policy. Her work draws on her decade of experience litigating antitrust and competition cases in private practice, and her industry expertise in finance, health care, pharmaceuticals, real estate, and digital technology.

SUMMARY OF MAJOR CONCLUSIONS

- **Data privacy law and antitrust law are distinct legal doctrines.** Data privacy is rapidly evolving into a distinct area of law that does not fit neatly within antitrust or any other existing doctrinal area. The overarching goal of antitrust is competition. The North Star of privacy law is the preservation of personal integrity. While there are privacy benefits to competitive markets, competition alone is insufficient to provide optimal levels of data privacy, and there are some areas where antitrust interests and privacy interests are in some tension.

- **Antitrust cannot completely protect privacy because markets cannot completely protect privacy.** Antitrust is fundamentally market-based; competition, the touchstone of antitrust, is a process that operates in a market-based system. Private markets, even perfectly competitive ones, cannot be expected to optimize data privacy. To the extent that data privacy has features of a fundamental property right or a public good it is not something that we should expect to be optimized by competition in a private market. Attempts to adapt antitrust law to bridge this gap risk undermining and diluting the primary goal of antitrust policy: competition.

- **Privacy markets are "missing" and subject to market failure.** To the extent that markets for privacy, as a good or as a quality of other goods and services, do exist, those markets are deeply flawed. Unclear allocations of data rights, the lack of effective legal frameworks, information asymmetries, and behavioral distortions all inhibit efficient markets for privacy features and the collection and use of personal data. As a result, the ability of antitrust to facilitate optimal levels of privacy is limited. Strong allocations of privacy rights and robust legal frameworks to protect and facilitate privacy choices are needed to set the stage for privacy markets, which is a necessary precursor to effective antitrust rules.

- **Antitrust can help consumers choose privacy.** Antitrust still has a role to play in promoting data privacy. Even though privacy itself may not be easily reduced to a commodity tradeable on markets, at least under the current legal and policy framework, privacy remains a quality by which some products and companies are differentiated. To the extent that individuals value privacy, protecting competition via antitrust can enable consumers to choose more privacy. By promoting and protecting the contestability of markets, antitrust can ensure consumers have real choices among products and services, including choices with better privacy protections that the market makes available.

- **Antitrust can change the incentives for companies to exploit sensitive data.** Companies invade data privacy and exploit sensitive data because it pays. One of the reasons invading users' data privacy is so lucrative is that it can be a means to acquire and exercise market power. By taking account of data exploitation in merger analysis, antitrust can directly address and prevent some privacy harms. And, by aggressively going after the anticompetitive uses of private data, antitrust can help change the incentives companies face to exploit private data.

- **The way forward: technology and tough choices.** The goal going forward should be to optimize both competition and data privacy where possible, but to make considered choices between them where necessary. Antitrust is one among may policy tools to achieve good public policy outcomes, and functions best when coordinated with other regulatory and enforcement tools. Technological and legal innovation may also be able to reduce the potential conflicts between privacy concerns and competition demands by enabling new ways for consumers to interact with the Internet while controlling their personal data. Inevitably, there will be some conflicts that will be unavoidable and where lawmakers will have to choose which goal to sacrifice.

I. INTRODUCTION

Antitrust law and policy and privacy law and policy have a complicated relationship. As the rise of the digital age has brought new threats to personal privacy, many have suggested that antitrust can or should be used to combat these threats. Likewise, those alarmed at attacks on personal privacy have sometimes blamed a lack of effective antitrust enforcement or competition policy for lax privacy policies and practices. But at the same time, frustrated competitors, consumers, and suppliers have accused big tech companies of using privacy policies (pre-textually or otherwise) to thwart competition and exclude them from markets.[1] And the leading proposed solutions to a lack of competition in tech markets involve forcing tech companies to share more, not less, of their users' private data.

What explains this complicated relationship and what are the implications for antitrust law and competition policy? Some of the explanation lies with certain quirks of modern antitrust law that make it an imperfect tool, at best, for checking and combatting privacy harms. Privacy challenges often arise in the context of zero-price products, non-price harms, and threatened market failures, each of which implicates limitations and challenges in using antitrust as a salutary tool. For example, many of the products at the center of debates about privacy are nominally free to consumers. Antitrust enforcement actions, rightly or wrongly, primarily use changes in price as a measure of harm. As a result, potential antitrust plaintiffs often struggle, as a practical matter, with how to account for all harms to competition involving zero-priced products, including privacy harms.

Even in priced goods, antitrust enforcers struggle to address harms to non-price dimensions of those goods effectively. This presents another impediment to using antitrust as a tool to address privacy. Although we know that market power and anticompetitive conduct often result in diminished privacy and degradation of other non-price quality attributes of goods and services,[2] few if any antitrust cases have rested their theory of harm or damages exclusively on these non-price attributes. The recently filed state case against Facebook stands out as a notable exception. It remains to be seen whether that case will prove a harbinger of change. Historically, if degradation of non-price attributes has been mentioned in antitrust litigation, it has been almost always in addition to, not in lieu of, pricing harms. This is a widely recognized issue in antitrust enforcement, but one that does not have an easy solution.

[1] For example, Google touts its "privacy sandbox" idea as a privacy measure, but critics argue it is only "privacy theater" that preserves Google's invasion of users' privacy while simultaneously excluding rivals from doing the same. *See* Cristina Caffarra, Gregory Crawford, Johnny Ryan, "The Antitrust Orthodoxy is Blind to Real Data Harms" (April 22, 2021).

[2] *See* Diana L. Moss, Gregory T. Gundlach, and Riley T. Krotz, *Market Power and Digital Business Ecosystems: Assessing the Impact of Economic and Business Complexity on Competition Analysis and Remedies*, American Antitrust Institute (June 1, 2021) at 19. *See also* Daniel P. O'Brien & Doug Smith, *Privacy in Online Markets: A Welfare Analysis of Demand Rotations*, Federal Trade Commission, Bureau of Economics, Working Paper No. 323, Jul 2014, at 26; Wolfgang Kerber, *Digital Markets, Data, and Privacy: Competition Law, Consumer Law, and Data Protection*, Gewerblicher Rechtsschutz und Urheberrect. Internationaler Teil (2016), at 7.

There is a deeper reason, though, why antitrust cannot provide a complete solution to modern privacy harms. There are numerous market failures that prevent privacy decisions from being effectively governed by market forces. Because antitrust is a market-based tool, these failures, unless corrected, necessarily limit the use of antitrust as a practical means for addressing sub-optimal levels of privacy protection. These market failures range from the existential (e.g., privacy has characteristics of a fundamental right or a public good that are incompatible with market allocation) to the psychological (e.g., the privacy paradox), to the circumstantial (e.g., information asymmetries). Without addressing these market failures through substantive regulation, promoting and protecting competition in the highly imperfect market for privacy can only accomplish so much, and may even undermine privacy goals.

Nevertheless, antitrust law and competition policy can contribute to more effective privacy protection. To the extent consumers are informed and would like to choose products and services with more robust privacy protections, antitrust law is integral to protecting consumers' opportunity to make that choice. By recognizing stores of personal data as a distinct market and potential source of market power, merger policy can better guard against the aggregation of personal data. And, by continuing to develop tools to better address broader issues with free products and non-price harms, antitrust enforcement can provide recourse where companies use market power to inflict harm that degrades privacy. Ultimately, however, socially desirable levels of privacy will only be achieved through law and policy decisions focused on recognizing the aspects of privacy as a fundamental right and a public good. And, antitrust law can only be effective as a practical tool for protecting privacy by either curing the market failures that surround privacy or by regulating failures that cannot be cured, not by the use of antitrust in a vacuum of privacy regulation.

II. THE COMPLEX RELATIONSHIP BETWEEN ANTITRUST AND PRIVACY LAW

Antitrust law and privacy law stand in a complex relationship to one another. The emergence of incredibly successful business models based on "surveillance capitalism"[3] poses new threats to both competition and privacy. These developments have also exposed long-simmering tensions between antitrust law and privacy law.[4] While often mutually reinforcing, the doctrines of privacy law and antitrust law are also regularly in tension and sometimes outright conflict.[5]

[3] SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM (2019).

[4] Laws and legal concerns regarding privacy are rapidly evolving and poorly defined. For purposes of this paper, I will use the term "privacy law" to refer to laws and legal norms concerned with rights of individuals to control access to and use of data and information about them.

[5] Erika M. Douglas, *The New Antitrust/Data Privacy Law Interface*, 130 YALE L.J. 647, 649 (2021) ("[T]he interests of data privacy and antitrust law are not always complementary—they can be in tension.").

The FTC is charged with enforcing both antitrust and privacy.[6] Likewise, there is considerable overlap between supporters of aggressive antitrust enforcement and strong competition policy and advocates for robust data privacy protections. And, the technology companies in the crosshairs of antitrust enforcers and legislators seeking to reform competition law are also the primary targets of criticism over lax privacy policies and exploitative data policies.

Yet, we also see multiple antitrust complaints alleging that big tech companies are using stricter privacy controls to disadvantage rivals. Google's plan to eliminate third-party cookies, digital tokens long criticized as a form of surveillance violating privacy norms,[7] was met with such strong allegations of anticompetitive intent and effect that it has since been shelved. The leading solutions being touted to solve the competition problems arising from network effects and other unique economic features in the tech industry would require forced sharing of consumers' data.[8] And, it is argued that imposing strong privacy rules in tech would further cement the market power and barriers to entry of tech's biggest players.

On the surface, this relationship between antitrust and privacy law sometimes appears a bit schizophrenic. While it was once assumed that antitrust law and privacy law are are aligned and mutually reenforcing, watching the interplay of these doctrines in tech markets in recent years has made clear that the relationship is much more complex. In fact, it appears that antitrust law, for theoretical and practical reasons, is often indifferent to or inept at addressing privacy concerns. Indeed, it is now clear that competition, and antitrust law's protection and promotion of competition, can sometimes exacerbate some privacy concerns, particularly in the face of market failures and missing regulatory frameworks. Far from uniformly mutually reinforcing, antitrust law and privacy law are often at cross-purposes. Laying bare this complexity has been the rise of the surveillance capitalism business model.

Surveillance capitalism is the business of harnessing personal data to predict and shape how people will behave for profit.[9] "Personalized facts about human beings," from mundane facts about retail preferences to deeply personal facts about legal and medical needs and deep-seated fears and vulnerabilities, are the "essential inputs" to surveillance capitalism.[10] The drive by those pioneering these new business models to develop and secure these inputs has led to unprecedented privacy incursions on a vast scale.

---

[6] Douglas, *supra* n.5, at 651-52 (detailing the emergence over the last 25 years of the FTC as the "*de facto* federal data privacy regulator"); *see also* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 598-600 (2014) (articulating the "new common law of privacy" developed by the FTC).

[7] *See, e.g.*, ZUBOFF, *supra* n.3, at 86 (2019) (detailing controversy over cookies and FTC efforts to regulate them in the 1990s and 2000s).

[8] *See, e.g.*, Fiona M. Scott Morton & David C. Dinielli, *Roadmap for an Antitrust Case Against Facebook*, at 2 (June 2020) (suggesting that mandating interoperability with other social media platforms may be the appropriate remedy to Facebook's alleged antitrust violations).

[9] ZUBOFF, *supra* n.3, at 8 ("Surveillance capitalism unilaterally claims human experience as free raw material for translation into behavioral data. Although some of these data are applied to product or service improvement, the rest are declared as proprietary *behavioral surplus*, fed into advanced manufacturing processes known as 'machine intelligence,' and fabricated into *prediction products* that anticipate what you will do now, soon, and later.").

[10] Randy M. Stutz, *Antitrust Law's Utility in the Digital Technology Sector: Toward an Actionable Agenda for Policymakers*, at 18, AM. ANTITRUST INST. (June 28, 2021).

At the same time, surveillance capitalism turns the typical relationship between consumers and markets on its head. In the classical antitrust paradigm, consumers are the buyers of goods and services. In surveillance capitalism, consumers are not the buyers, but the suppliers of personal data.[11] At the same time that consumers are using and consuming (and sometimes paying money for) online services and goods, they are simultaneously generating and handing over a critical input for surveillance capitalism—their personal data—to another supply chain in which they are the (often unwitting) supplier or raw material. In this supply chain, the ability to harvest and analyze personal data to make predictions about consumer behavior is the primary means of downstream competition.[12] As a result, the drive to compete incentivizes companies to attempt to extract as much information as possible, placing competition in direct opposition to privacy concerns.

Countervailing this incentive to compete by extracting as much information as possible from consumers is the fact that consumers are not passive. For the most part, tech companies rely on the willingness of consumers to engage with their products in order to extract data from them. Google, for example, relies on consumers using Gmail, Google Maps, Google Search, and other consumer-facing Google products for its access to consumer data. Likewise, Facebook has access to vast consumer data troves thanks to consumers' voluntary engagement with its social networking products. If companies go too far in extracting and exploiting personal data, they theoretically face the threat that consumers will shift to alternative products and services, taking their rich source of data with them.

On this dimension of surveillance capitalism, privacy law and antitrust law are much more closely aligned. The strength of this countervailing incentive, this check on surveillance capitalists' otherwise unbridled drive to extract and exploit personal data, depends on the existence of effective competition. The threat that consumers will abandon a given company's products and cut off its access to their data, is only as strong as the alternatives available to the consumers.

A lack of competition, and of viable alternatives to a given company's products and services, neutralizes this force that might otherwise curtail, to an extent, surveillance capitalists' extraction and exploitation of personal data. This dynamic is why the fact that tech markets are often subject to network effects and tipping, where dominant players have no meaningful rivals and consumers are locked in by high collective switching costs,[13] is a critical concern of both antitrust enforcers and privacy advocates; network effects and tipping in tech markets are a threat to privacy because they act to undermine the competition that serves as a check on what is an otherwise unlimited incentive faced by surveillance capitalists to extract and exploit consumer data.

---

[11] Erika Douglas, *Monopolization Remedies and Data Privacy*, 24 VA. J.L. & TECH. 2, at 44 (2020) ("Consumer data is the raw material driving the businesses of the largest digital platforms."); *see also* Maurice E. Stucke & Allen P. Grunes, *No Mistake About It: The Important Role of Antitrust in the Era of Big Data*, University of Tennessee—Knoxville, College of Law, Research Paper #269, at 3 (May 2015).

[12] Stucke & Grunes, *supra* n.11, at 3 (May 2015) ("[C]ompanies undertake data-driven strategies to obtain and sustain competitive advantages.").

[13] Stutz, *supra* n.10, at 23-24.

Strong antitrust laws and competition policy that protects and promotes competitive markets also promotes consumer choice and enhances this market-based limit on privacy violations. Nevertheless, it would be a mistake to look to antitrust law as a complete privacy solution. The reasons for this are the subject of the following section. Markets, and therefore antitrust, cannot address the failure of policymakers to provide legal protections for privacy rights or address the public interest in personal privacy. But, even within markets, market failures and underdeveloped tools for reaching certain kinds of antitrust harms limit the effectiveness of antitrust solutions to privacy.

III. ANTITRUST CANNOT BE A COMPLETE PRIVACY SOLUTION

There are significant limitations on the ability of antitrust, as a policy tool, to address privacy. The most impactful and intractable limitations are discussed below. Some of these limitations arise from the nature of privacy and privacy rights, some from market failures, and others from limitations inherent to antitrust as a tool. Accordingly, while revising, expanding, or strengthening antitrust laws may help mitigate some of these barriers, others will be unaffected. To provide a complete solution to current privacy concerns, other legal and policy tools beyond antitrust are also needed.

A. Privacy Outside of Markets

Antitrust is, fundamentally, a tool for policing and managing private markets. That is, the exchange of goods and services for value between individual market participants. The benefits of competition and competitive markets extend well beyond those markets. Indeed, the indirect benefits of competitive markets for social stability, upward mobility, and democracy all motivate the strong commitment in the United States to the antitrust laws. But, despite its broad implications and motivations, antitrust is a narrow tool. The arena in which antitrust plays is market-based competition. To the extent that privacy and data issues either precede markets or are not captured by markets, antitrust is not a very useful tool for addressing those issues. There are at least two such dimensions of data privacy and security for which this limitation applies, as discussed below.

Privacy as a Fundamental Right. Privacy scholars and policymakers disagree about whether privacy is a fundamental right of all individuals or whether privacy is merely another quality dimension of products to which consumers are entitled only if they are willing to pay the associated cost. At its core, this is a debate about how to allocate property rights to data and privacy in the first instance.

If privacy is a fundamental right, then the individual owns his or her data and has the right to dictate how it is used, without needing to buy or acquire that right from a company. [14] At the extreme, some argue the right is inalienable—that much as one cannot sell his or herself into slavery, one cannot fully surrender the right to control one's own data.

On the other hand, if privacy and control of one's data is only a quality attribute of products and services, then individuals are only entitled to the amount of privacy they are willing to buy from a company. Those who choose to use products that harvest and exploit their data do so at their peril and have no right to expect baseline privacy protections, just as customers who buy cheap toasters have no right to expect the toasters will make good toast.

The dichotomy between these two approaches is not complete. Just because something is a quality of a product does not mean that society cannot decide to set a baseline level for that quality. For example, no matter how cheap, the law still protects consumers from exploding toasters; society has set a floor for product quality, but there is plenty of room above that floor for consumers to elect (and pay for) different levels of quality that suit their needs and budgets.

The important point about this debate for antitrust policy is that it concerns the initial allocation of privacy rights. How and to whom privacy and data rights are allocated in the first instance is not a problem antitrust policy and enforcement can solve. Antitrust is a market-based doctrine, concerned with preserving competition in markets for the exchange of goods and services. But, economists have long recognized that markets do not allocate property rights in the first instance; indeed, in order for markets to function, something outside the market (property law, brute strength, etc.) must first allocate the goods and services to be exchanged.

Once rights are allocated, antitrust has an incredibly important role in ensuring that the markets for the exchange of those rights are competitive. [15] But those who look to antitrust to answer questions about whether consumers have rights to privacy and, if so, what those rights consist in, will be perpetually disappointed.

Privacy as a Public Good. To the extent there is a value to society from privacy and data protection, markets, and thus antitrust, are unlikely to recognize and account for that value. The self-interested decisions of individuals and businesses that guide the invisible hand of the market do not, by definition, account for the interests of the public writ large. Acknowledgment of this reality is why we have long carved public goods out of the market sphere and relied on governments to protect and allocate them. To the extent there are significant public costs from

[14] *See, e.g.*, Nicholas Economides & Ioannis Lianos, *Restrictions on Privacy and Exploitation in the Digital Economy: A Market Failure Perspective*, J. OF COMPETITION L. & ECON. 1, 4-5 (2021) ("Indeed, data protection and privacy regulations often take a fundamental rights perspective, with privacy perceived as a rights issue."). Somewhat ironically, Apple has taken a firm stance that privacy is a fundamental human right. https://www.apple.com/privacy/

[15] Note, though, that some argue privacy rights are inalienable and, thus, beyond the reach of markets. The California Constitution, for example, lists privacy as an inalienable right. Cal. Const. art. I, § 1 ("All people are by their nature free and independent and have inalienable rights. Among these are…pursuing and obtaining …privacy.); *see also* Daniel J. Solove & Paul M. Schwartz, *An Overview of Privacy Law*, GW Law School Public Law and Legal Theory Paper No. 2015-45 (2015), at 41. Under this conception of privacy, as outside of markets, the role for antitrust is exceedingly limited.

under-protecting privacy, market-based privacy protections, including antitrust, will not account for them.[16]

Current debates over microtargeting of misinformation and political advertising highlight the societal interest in guarding privacy and data. The storage, control, and manipulation of huge volumes of personal data by private companies has enormous implications for political process and the ability to guard against conspiracy theories and other lies that can undermine everything from public health measures (in the case of COVID-19 and vaccinations, for example), to public safety (in the case of Pizzagate and other misinformation-fueled violence, for example), to democracy itself (in the case of the January 6 uprising, for example).

Data and privacy issues also have enormous implications for national security. Private companies that gather and store huge volumes of detailed personal data are targets for espionage by foreign governments, hacks and ransomware attacks that can shut down critical infrastructure like hospitals, and inadvertent leaks that can lead to identity theft, bank fraud, and blackmail. And, of course, there is the threat that companies might voluntarily share information with foreign governments or other bad actors for profit.

Looking to market-based tools, like antitrust, to optimize these public goods associated with privacy and data rights would be a grave mistake. Markets, the interface of self-interested private actors, do not and cannot account for or optimize such societal interests. Even with perfect competition, markets will fail on this front.

While one could incorporate such public interests into, say, merger clearance procedures before the antitrust agencies, doing so would not make them antitrust issues; trying to twist antitrust analysis to directly account for broad public interests would only confuse and dilute the antitrust inquiry, which should be focused on competition. There are other tools that are and can be better designed and better deployed to account for public interests in mergers beyond competition. For example, the Committee on Foreign Investment in the United States ("CFIUS") reviews certain foreign investment transactions for national security concerns.[17] National security interests would not be better protected by being incorporated directly into the FTC and DOJ antitrust analysis, and doing so would substantially muddle the antitrust inquiry. So, too, with non-competition-based privacy concerns.

[16] Economides & Lianos, *supra* n.14 at 26 ("If these social costs were significant, there is also an argument for banning such transactions [exchanges of personal data for money] and, thereby, making personal data inalienable."). The authors go on to assert that banning such transactions is "non-pragmatic" given "the level to which the dignital economy has developed." *Id.*

[17] https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius. This review is authorized under the Defense Production Act of 1950, 50 U.S.C. § 4565, as modified by the Foreign Investment Risk Review Modernization Act of 2018, P.L. 115-232.

B. Privacy as a Product Attribute

As the above discussion makes clear, government intervention is necessary to allocate privacy rights and to regulate to protect the public interest in data security and data privacy. But unless privacy rights are inalienable or the public interest in data privacy is so complete as to leave no room for individual preferences, it is worth delving deeper into the interplay between markets, competition, and individual data privacy. Is "the relationship between Internet privacy and competition direct and positive"?[18] Do consumer preferences about privacy fit the rational choice theory that underpins the case for competition? Are there other market failures that prevent competition from optimizing privacy preferences? Is antitrust law underenforced against privacy harms? Are there market-based aspects of privacy competition that the current antitrust laws fail to capture? How can antitrust law be adapted or reconceptualized to better address anticompetitive conduct or agreements related to privacy.

A cursory examination of some of these questions makes obvious that, even within the market sphere, to the extent that data privacy is a fungible attribute of goods and services we buy and sell, there are multiple limitations on antitrust as a complete privacy solution[19] and numerous reasons to believe that the relationship between privacy and competition is far from direct or straightforward. These limitations perhaps explain why, despite the FTC, DOJ, and European competition authorities all agreeing that privacy is, in theory, an antitrust concern, privacy-based competition is rarely, if ever, outcome determinative in cases.[20]

Antitrust absolutely can and should be used to promote transparency, choice, and competition on privacy. But, for various reasons explained below, robust technology and policy solutions outside of antitrust are needed to provide optimal levels of privacy that are not realistically attainable through competition alone.

Quality Attributes. Antitrust law encompasses both price and non-price aspects of competition, including quality attributes. The primary mechanisms for antitrust enforcement—civil damages, injunctions, disgorgement, and merger control[21]—however, all use price and changes in price to measure both antitrust harm and, where relevant, damages.[22] Unlike prices, non-price quality attributes, including privacy, are neither readily quantifiable nor linear. This presents a two-fold challenge for courts and antitrust enforcers, whose primary yardstick for anticompetitive effects is prices.

---

[18] Frank Pasquale, *Privacy, Antitrust, and Power*, 20 GEO. MASON L. REV. 1009, 1009 (2013).

[19] Stucke & Grunes, *supra* n.11, at 5 (noting that theories for addressing privacy via antitrust regard loss of privacy as a reduction in quality).

[20] Douglas, *supra* n.11, at 26-27.

[21] In *AMG Capital Management, LLC v. FTC,* the Supreme Court held the FTC lacks the authority to seek equitable remedies, including restitution and disgorgment. The fact that the FTC can no longer recover these monetary remedies is not expected to change the fact that effects on competition are largely determined by reference to impacts on prices. It is, however "significantly likely to change the way the commission approaches privacy and data security enforcement." Allison Grande, *FTC to Shake Up Privacy Enforcement in Wake of AMG Ruling*, LAW360 (May 28, 2021). Criminal antitrust enforcement is also an important tool, but one largely limited to cartel conduct.

[22] John M. Newman, *Antitrust in Zero-Price Markets: Foundations*, 164 U. PENN. L. REV. 149 (2015).

Without a way to convert privacy and other quality harms to dollars, courts and agencies are left without a ready mechanism to impose monetary damages and disgorgement.[23] Policymakers and academics recognize the need for better antitrust tools in this regard, and have made considerable progress in recent years to develop them.[24] Perhaps more vexing, there is no ready way to balance privacy harms against other benefits from a practice or a transaction.[25] Thus, even where it can be established that a merger or anticompetitive conduct reduces privacy, if the merger or conduct also leads to efficiencies, enforcers lack the means to reconcile those conflicting effects.

Even beyond the lack of a ready means to convert privacy to dollars, the multi-dimensional nature of privacy makes it hard to assess privacy harms. The ways in which companies invade our privacy are multifaceted. The collection of information without user awareness or consent harms privacy, but so does the unauthorized sharing of information a user willingly shared. Sometimes, it is not the collection of the information that presents a privacy harm, but the aggregation and analysis of information innocuously collected. Or, the use of that information for a new purpose. And, some of the companies that collect the most information about people are also among the best at guarding that information from cybercriminals, data leaks, and, even, appropriation by the government.

Antitrust enforcers lack the ability to weigh these competing privacy concerns or to say with any rigor whether a merger will, overall, enhance or impair user privacy.[26]

"Free" Products. The products and services that surveillance capitalists use to extract data from individuals are, generally, non-price goods. Surveillance capitalists make money by selling data and predictions based on data. To generate and collect this personal data, companies offer nominally "free" products and services to consumers and businesses. Although consumers do not pay for zero-price goods with money, they do sacrifice their attention and their data to obtain them.[27] Such zero-price goods pose a dilemma for antitrust and, until very recently, the dominant view among antitrust courts, enforcers, and theorists regarding such zero-price products has been that "without prices, there can be no welfare harms of the type that antitrust law seeks to prevent."[28]

The perspectives of antitrust scholars and enforcers on zero-price markets are beginning to shift, and most now recognize that consumers can, in fact, incur antitrust harms in zero-price goods. Important work by John Newman and others has made the case that customers in zero-price markets do in fact incur costs from these transactions (namely, the sacrifice of their time

[23] Some have suggested that enforces should regard "privacy features, and the loss or lack of data protection that comes with their relaxation, as a price," *see* Caffarra, et al., *supra* n.1, but this does not ultimately resolve the issue. Whether viewed as a price or a quality, we still lack a rigorous way to weigh privacy harms against dollars.

[24] ALEX MARTHEWS & CATHERINE TUCKER, PRIVACY POLICY AND COMPETITION, at 25, BROOKINS INST. (2019); *see also* Newman, *supra* n.22.

[25] *See* Douglas, *supra* n.11, at 72 ("Weighing such harms against each other with precision may well prove difficult.").

[26] Stucke & Grunes, *supra* n.11, at 8-9 (noting that "enforcement agencies are more comfortable assessing a merger's effects on prices and less comfortable assessing its non-price effects).

[27] ZUBOFF, *supra* n.3, at 18.

[28] Newman, *supra* n.22 (collecting examples of expressions of this idea).

and attention) and, importantly, "that some of the costs incurred *are* exchanged and play the same role that money plays in positive-prices markets."[29] Because these costs "function as [a] media of exchange" they signify market transactions that are theoretically subject to competitive processes where antitrust can play a role. Yet, despite recognizing the theoretical potential for harm in zero-price markets, enforcers still struggle because "some of the tools of market definition and market power break down when the price to consumers is zero."[30] This is an area where more work is needed to develop effective antitrust tools.

Behavioral limitations and the So-Called Privacy Paradox. The problems with measuring privacy harms go deeper than finding the appropriate metric; some scholars have argued that people's privacy choices appear both irrational and contrary to their own stated interest.[31] This purported disconnect, where people claim to value their privacy but fail to take steps to protect it, is often referred to as the "privacy paradox."[32]

Some cite the privacy paradox as evidence that consumers do not actually value privacy. Others characterize the privacy paradox as a behavioral issue, meaning an instance where humans do not behave rationally because of various limitations in perceiving risks. Under either of these explanations, the failure of individual choices to demonstrate that consumers consistently value privacy presents a major hurdle to antitrust enforcement premised on privacy harms. The entire model of antitrust harm is built on the notion of consumer sovereignty. If consumers do not, in fact, value privacy, then invasion of privacy cannot be rightly viewed as an infringement on their sovereignty. If consumers do actually value privacy, but for some reason that is not revealed by the choices they make, then that presents an even deeper problem, as it calls into question the notion that antitrust can rely on revealed preferences generally.

In a recent article, Daniel Solove argues persuasively that the privacy paradox is not, in fact, a paradox at all.[33] Rather, the apparent disconnect between people's stated support for privacy and their willingness to reveal personal information "emerges from conflated issues, unwarranted generalizations, and leaps of logic."[34]

---

[29] Newman, *supra* n.22, at 163. *See also*, Tim Wu, *Blind Spot: The Attention Economy and the Law*, 82 ANTITRUST L.J. 771, 771 (2019). In contrast, some economists argue that, while consumers are being harmed by the harvesting of data, the harm is not market-based because "there are no markets in which data and/or attention are demanded by companies and supplied by users, and this being traded at publicly known prices." Economides & Lianos, *supra* n.14 at 25. The primary difference being that the latter view would require an exchange for money, whereas the former would be willing to treat attention "as a media of exchange."

[30] Stucke & Grunes, *supra* n.11, at 8.

[31] *See, e.g.*, Sarah Spiekermann, Jens Grossklags & Bettina Berendt, *E-Privacy in 2nd Generation E-Commerce: Privacy Preferences Versus Action Behavior*, in EC '01: PROCEEDINGS OF THE 3RD ACM CONFERENCE ON ELECTRONIC COMMERCE 38, 38-39, 45 (2001) (shoppers divulge large amounts of personal data to bot, despite indicating that they highly value privacy); Bettine Berendt, Oliver Gunther & Sarah Spiekermann, *Privacy in E-Commerce: Stated Preferences vs. Actual Behavior*, COMMC'NS ACM, Apr. 2005, at 101, 104 (finding that people "do not always act in line with their stated privacy preferences, giving away information about themselves without any compelling reason to do so"); Alessandro Acquisti & Jens Grossklags, *Privacy and Rationality in Individual Decision Making*, IEEE SEC. & PRIV., Jan.-Feb. 2005, at 26, 28.

[32] *See* Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEO. W.L. REV. 1, 2 (2021) (noting that a search for "privacy paradox" on Google Scholar returns more than 8,000 results).

[33] *Id.* at 4 ("The privacy paradox is essentially an illusion created by faulty logic, unwarranted generalizations, and conflated issues.").

[34] *Id.* at 23.

Far from irrational, the choices that modern consumers make about information sharing and privacy reflect that "[p]rivacy regulation too often relies on privacy self-management as its major tool for privacy protection."[35] We take individual information sharing choices as evidence of consumer attitudes about privacy, but individuals in the modern age do not actually have the ability to control their privacy in any meaningful way. "[E]ven totally rational people cannot succeed at privacy self-management."[36]

The pragmatic choices that people make about, e.g., whether to use Gmail or pay for an email service that does not scan their data, whether to agree to Facebook's onerous terms or forego social media—which the privacy paradox takes as evidence that people do not value their privacy—actually reflect the lack of effective privacy choices available to consumers and consumers' recognition of the futility of trying to guard interests in data privacy through a series of individual choices against a backdrop of a complete absence of a legal framework for privacy rights and data usage.

What is the point of a consumer going through the steps to opt out of some particular website's data gathering process if their ISP is going to track their every move anyway?[37] Why bother doing a cumbersome custom install of Microsoft's products if Microsoft is going to install its tracking software even if the user declines it?[38] How does one even opt out of ubiquitous trackers that follow users and non-users alike across the web?[39]

Whether the privacy paradox is explained by behavioral factors, overstated privacy ideas, or despair, the fact that individual choices do not seem capable of achieving any given user's desired level of privacy suggests that no amount of competition, alone, will provide sufficient levels of privacy. Moreover, increased competition may further degrade some aspects of privacy, because efforts to obtain person data may intensify.[40] Whether paternalistic measures to countermand behavioral issues are needed or whether a framework of substantive and procedural privacy measures can empower consumers to make effective privacy choices, the fact that consumer privacy preferences cannot be accurately discerned from their choices against the current legal backdrop presents a major impediment to using antitrust law, which depends on revealed preferences, to protect privacy.

Information asymmetries. A final issue that no doubt contributes to the disconnect embodied in the privacy paradox is the enormous information asymmetries that plague data privacy issues. Implicit in the rational choice theory underlying antitrust economics is the assumption that the parties in the market have comparable levels of information and the ability to discover

[35] *Id.* at 33.

[36] *Id.*

[37] ZUBHOFF, *supra* n.3, at 166 (discussing Verizon's and AT&T's ongoing programs to track their ISP customers across the web, despite those customers opting out of such tracking).

[38] ZUBHOFF, *supra* n.3, at 164 (describing how Microsoft's Cortana assistant would continue to collect and transmit data, even when the user disabled it during installation of the Windows operating system).

[39] ZUBHOFF, *supra* n.3, at 158.

[40] *See, e.g.*, Moss, et al., *supra* n.2; Eugene Kimmelman, Harold Feld, and Agustín Rossi, *The Limits of Antitrust in Privacy Protection*, 8 INT'L DATA PRIVACY L. 270 (2108).

the knowledge relevant to the decisions they make.[41] When it comes to privacy, at least under the current U.S. notice-and-consent based privacy regime, this assumption fails on a massive scale.[42]

American privacy law currently requires companies to disclose what data they are collecting and with whom they plan to share it. By using the goods and services offered, consumers are considered to have consented to the data policies. There is no requirement that consumers affirmatively opt in to data collection or are offered an option to access the goods or services without consent to the data collection and privacy policies. The idea is that the required disclosures will give consumers sufficient information to make effective privacy choices and that consumer choices to use the goods and services after disclosure amount to consent. But this method for protecting privacy fails on both prongs.[43]

Legally mandated disclosures do not, and cannot, give consumers the information they need to make rational choices about data privacy. Rather, "[n]otice and consent has become a way to exploit the rational ignorance of consumers."[44] And, even if the disclosures were effective to resolve information asymmetries, consent is only effective where consumers have real choices. When faced with a monopoly, or uniform industry policies, consent may not reflect real choice.[45] Antitrust can and should be used to combat the lack of real choice surrounding consent, as is discussed in Section IV below. But antitrust can do little to solve the information asymmetry issue.

Absent broadly applicable and detailed privacy laws that provide a baseline, consumers will always have much less information about which of their data is being collected, with whom it is shared, and what is being done with it, than the companies that are doing the collecting.[46] First, it is not feasible for consumers to read all the privacy policies they encounter. Second, even if one did spend the estimated 76 full workdays it would take to read all the policies the average consumer encounter in a single year,[47] and could understand them,[48] the privacy policies generally do not provide enough detail for a consumer to get an accurate picture of how their

[41] Note, though, that many of the issues discussed also apply if one regards privacy as a right. Economides & Lianos's maket failure solution, for example, depends on consumers' ability to rationally determine whether and under what terms to agree to share their data. *See* Economides & Lianos, *supra* n.14, at 20 ("Assuming that people can rationally determine whether it makes sense for them to provide their data, a competitive market concerning the collection of data from users would lead to users being paid by digital platforms for the harvesting of their data.").

[42] *See, e.g.*, Stucke & Grunes, *supra* n.11, at 12 (describing "take-it-or-leave-it" privacy policy structure as a market failure).

[43] The FTC has recognized this point, as evidenced by its movement into enforcement efforts focused on protecting consumers' reasonable expectations of privacy. *See* Douglas, *supra* n.11 at 56. FTC Commissioners have also directly criticized notice-and-consent as ineffective. *Id.* at 80-81. Courts have likewise flirted with "reasonable expectations of privacy" as a standard. *Id.* at 60.

[44] Douglas, *supra* n.11, at 81.

[45] *See* Economides & Lianos, *supra* n.14, at 24 (noting that such a lack of competition also "results in a lack of informational transparency regarding the value of the user to the relevant digital platform").

[46] Economides & Lianos, *supra* n.14 at 6 (detailing the various information asymmetries that persist regarding the collection of personal data).

[47] ZUBHOFF, *supra* n.3, at 50 (citing Aleecia M. McDonald and Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, JOURNAL OF POLICY FOR THE INFORMATION SOCIETY, 4, no.3 (2008), http://hdl.handle.net/1811/72839).

[48] *See* Moss, et al., *supra* n.2, at 14 (discussing informational barriers to notice-and-consent-based consumer privacy).

data is being collected, stored, shared and used.[49] Moreover, privacy policies often include language allowing the company to change the policy at will in the future. And, when companies are sold or merged, the data they have collected can be put to uses not foreseeable when users agreed to disclose it. "[B]ecause data protection characteristics are unobserved and consumers cannot act on them, competition won't work to … provide more data protection."[50]

In this environment, some competition based on privacy may still occur, but only at the most basic level.[51] Companies that can make bold and categorical privacy claims, such as "We don't store your personal information. Ever."[52] can differentiate themselves to an extent, notwithstanding the opacity of privacy policies generally. And, when particularly egregious privacy invasions are publicized, it does sometimes cause some users to move away from a company's products.[53] But even in these extreme cases, which are few and far between, the user response is modest and often temporary.[54] And we see almost no competition on more subtle differences between privacy policies and practices, such as collecting only data needed for client-directed requests or time-limiting data storage.

If markets, even perfectly competitive ones, will never provide an optimal level of privacy, then the scope of antitrust as a privacy solution is necessarily limited. It is important to recognize this both to avoid false hope that privacy problems can be addressed using only antitrust tools and to avoid pulling antitrust law away from its competition goals in a misguided attempt to use antitrust to fill gaps in privacy policy.[55] Adequate privacy protection will require empowering individuals with the legal tools to directly address infringements of their rights and regulation to protect society's interest in privacy as a public good.

[49] *See, e.g.*, Dorothy Atkins, "Android Users Slam Google's 'All or Nothing' Privacy Stance," Law360 (Jan. 19, 2021) (summarizing allegations in consumer lawsuit against Google alleging data disclosures were too broad and too disconnected to put Android users on notice of the type of data being collected and the uses to which it was being put).

[50] Caffarra, et al., *supra* n.1.

[51] *See* Stucke & Grunes, *supra* n.11, at 9 (characterizes existing competition on privacy as at a "dysfunctional equilibrium") (quoting Joseph Farrell, *Can Privacy Be Just Another Good?*, 10 J. ON TELECOMM. & HIGH TECH. L. 251, 256-59 (2012)).

[52] https://duckduckgo.com.

[53] After the Cambridge Analytica scandal received widespread press attention, for example, many of Facebook's U.S. users de-activated their Facebook accounts, at least temporarily. Stutz, *supra* n.13 at 25. *See also* Maria LaMagna & Jacob Passy, *Want to Delete Facebook? Read What Happened to These People First*, MARKETWATCH (Oct. 31, 2019, 8:50 AM) (noting that 44% of users ages 29-44 reported deleting the app but that the company reported a 1.6% increase in active users year-over-year).

[54] *Id. See also* MARTHEWS & TUCKER, *supra* n.24 (discussing lack of increase in DuckDuckGo search traffic in response to Edward Snowden's revelation that an NSA surveillance program relied on data from Google and Bing but not DuckDuckGo).

[55] While some so-called "separatists" argue data privacy should play no role in antitrust and competition policy, in order to avoid blurring the focus of antitrust on consumer welfare and the promotion of market competition, *see e.g.* James C. Cooper, *Privacy and Antitrust: Underpants Gnomes, the First Amendment, and Subjectivity*, 20 GEO. MASON L. REV. 1129, 1146 (2013), this goes too far. Rather, to the extent market power or harms from anticompetitive conduct take the form of data exploitation and privacy degradation, antitrust law and competition policy should recognize them.

IV. ANTITRUST AND COMPETITION AS PART OF A BROADER PRIVACY SOLUTION

Even if antitrust and competition policy cannot, alone, adequately protect privacy, competition is nonetheless integral to effective privacy protection. Antitrust is only one tool in the toolbox, but it is an important one.

Competitive markets are integral to robust data privacy. The absence of competition breeds all manner of ills. High prices, to be sure, but also diminished quality, including, in some instances, diminished privacy. The case filed against Facebook in December 2020 by 48 state attorneys' general alleges, for example, that Facebook's diminished consumer privacy is a form of monopoly rent.[56] Privacy policies and practices can also be the subject of anticompetitive conduct cases, such as "privacy fixing,"[57] as nine state attorneys general alleged in their recent case against Google.[58]

Even if current antitrust laws struggle to directly target privacy harms, by guarding against the accumulation of market power and prosecuting abuses of market power, the antitrust laws contribute to more competitive markets which, generally, have privacy benefits.[59] Moreover, the privacy benefits from competition can be greatly enhanced, and the increase in privacy threats driven by competition largely mitigated, by robust privacy regulation and the clear allocation of privacy and data rights through mechanisms outside of antitrust but reinforced by strong antitrust and competition enforcement and policy.

Competitive markets also provide consumers with market-based tools to punish companies that commit egregious privacy violations. "The exploitation of personal data may result from economic coercion on the basis of the user's resource-dependence or lock-in with the user having no other choice than to consent to the harvesting and use of their data, to enjoy the consumption of a specific service provided by the data controller or its ecosystem."[60] The lack of effective competition in social networking markets no doubt hampered the consumer response to the Cambridge Analytica scandal; without any alternatives to Facebook, consumers only choices were to tolerate the violation or quit social media all together.

A corollary of the idea that the privacy paradox actually reflects rational behavior in the face of a lack of effective privacy choices is the idea that if people had real choices on privacy they would make them. Against a backdrop of effective privacy regulation, there would still be room

[56] Caffarra, et al., *supra* n.1; Complaint, *State of New York, et al. v. Facebook Inc.*, Case No. 1:20-cv-03590 (D.D.C. Dec. 9, 2020).

[57] Robert H. Lande & Howard P. Marvel, *Collusion Over Rules*, 16 Antitrust 36 (2002).

[58] *Id.*; Facebook Complaint, *supra* n.56 (alleging agreement to fix privacy policies between Google and Facebook). *See also* Economides & Lianos, *supra* n.14 (for an EU perspective detailing other ways of directly attacking privacy invasions as anticompetitive harms under an abuse of dominance theory).

[59] *See* Economides & Lianos, *supra* n.14, at 74 (noting indirect benefits to privacy from increased competition).

[60] Economides & Lianos, *supra* n.14, at 6. *See also*, Moss, et al., *supra* n.2, at 12.

for consumer choice about details and levels of privacy protection, provided competition in these markets exists.

Merger policy also has an important role to play in preventing the accumulation of data-based market power.[61] By preventing mergers between companies controlling separate troves of data, antitrust authorities can prevent the concentration of large amounts of data in the hands of a single company, and thus limit the exploitation of that data.[62] For example, the DOJ successfully blocked the merger of Bazaarvoice and its rival PowerReviews, relying in part on a theory that the ability to leverage consumer data from their combined database would serve as a barrier to entry.[63] Caffarra, et al., have persuasively argued that agencies need to expand merger review to systematically account for this type of market power and threat of harm.[64] This both guards against exploitation in the mergers that are denied, and also changes the incentives for accumulating this data in the first place.[65]

EU antitrust authorities have acknowledged that privacy concerns should be considered in merger analysis, but have yet to actually base any merger decisions on this potential source of market power.[66] In the U.S., privacy has historically been regarded as a consumer protection issue with little to no role in antitrust merger analysis.[67] The FTC has recently signaled an intent to incorporate privacy issues into merger analysis, but has not articulated how that will be accomplished.[68] The DOJ, which shares responsibilities for merger clearance has been more circumspect,[69] raising the prospect that the agencies may disagree on the role of privacy in merger analysis.

[61] Economides & Lianos, *supra* n.14, at 27 ("It is generally accepted that merger control should take into account the fact that access to personal data may constitute on important source of market power.")

[62] Caffarra, et al. articulate three ways in which data accumulation can threaten competition: creating positive feedback loops; empowering discrimination; and extending market power into new markets. Caffarra, et al., *supra* n.1. *See also* Z. Chen, C. Choe, J. Cong, and N. Matsushima, *Data Driven Mergers and Personalization*, ISER Discussion Paper 1108, Institute for Social and Economic Research, Osaka University (2020); Economides & Lianos, *supra* n.14, at 9 ("Because the data are used to sell advertisements, Facebook's requirement [that users hand over their personal data] directly increases its own market power, while simultaneously stifling competition, in the advertisement market.").

[63] Stucke & Grunes, *supra* n.11, at 8 (discussing case); *see also* United States v. Bazaarvoice, Inc., Case No. 13-cv-00133-WHO, 2014 WL 203966, at *50 (N.D. Cal. Jan. 8, 2014).

[64] *See* Caffarra, et al., *supra* n.1.

[65] Stucke & Grunes, *supra* n.11, at 8 (noting that currently "the economic incentives run almost entirely in one direction—towards accumulating more personal data").

[66] Economides & Lianos, *supra* n.14 at 27-36 (discusses a series of European mergers where privacy theories of market power and harm were articulated, but largely disregarded in the the EC decisions).

[67] Economides & Lianos, *surpa* n.14, at 36 ("This issue takes a different dimension in the United States where harm to privacy does not come up when assessing merger activity and any privacy issues are to be dealt with through Section 5 of the [FTC] Act of 1914….").

[68] Memorandum, *Chair Lina M. Khan to Commision Staff and Commissioners re Vision and Priorities for the FTC*, Federal Trade Commission (Sept. 22, 2021) (outlining a broader frame for evaluating mergers and noting that such broadening "can also help suface the macro effects of our policy decisions, such as…data consolidation and security vulnerabilities.")

[69] Bryan Koenig, *DOJ Nominee Hedges on Expansion of Competition Reviews*, LAW360 (Oct. 6, 2021).

V. POLICY CAN FILL THE GAPS

Many apparent conflicts between antitrust and privacy would abate in the face of effective privacy legislation. Privacy is a broad concept, and there are many privacy harms that are not competition harms.[70]

Currently, data privacy, and protecting that privacy, is effectively left in the hands of the technology gatekeepers. This means that privacy is protected only when and how it serves the interests of those gatekeepers. As a result, privacy is not only under protected, but what efforts exist to protect privacy are often exclusionary and anticompetitive. Taking privacy protection out of the hands of big tech gatekeepers and putting it into the hands of the government would be expected to significantly reduce the use of privacy policy as an excuse for exclusionary and anticompetitive conduct. [71]

Effective privacy policy, and particularly the allocation or recognition of privacy rights, is necessary to establish a market for privacy.[72] Tools to facilitate baseline privacy protections and transparency are likely also required, given the information asymmetry issues discussed above. Once such a market is in place, antitrust tools can be used to protect competition in that market and to remedy anticompetitive conduct. Even with markets in place, some market failures will likely persist, making concurrent regulation almost certainly necessary. Without an effective market for privacy, however, antitrust is severely limited as a privacy tool.

As much as robust privacy policies will resolve some tensions between privacy law and antitrust, it will only increase tensions in other respects. In particular, considerable tension will remain between competition and privacy concerns with respect to certain types of antitrust remedies. Recognizing that accumulated data can be a a source of market power, and that "switching costs and lock-in are ubiquitous in information systems,"[73] invites the question of how these systemic forces favoring "market concentration and dominance"[74] and its associated leveraging should be remedied. Both legislators and litigants have, in answering this question, suggested that forcing big tech companies to share their data ("data portability") and enable competitors to access their networks ("interoperability") as remedies to this type of monopolization.[75]

---

[70] Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, George Washington Law School Public Law and Legal Theory Paper No. 2021-11 (2021) (cataloging the various ways that infringement of privacy can inflict personal and social harm).

[71] Stucke & Grunes, *supra* n.11, at 7 (noting the flow of information from consumers to online firms in exchange for products is critical to the business model of big tech).

[72] *See* Economides & Lianos, *supra* n.14.

[73] CARL SHAPIRO & HAL R. VARIAN, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY 104 (1999); *see also* Stucke & Grunes, *supra* n.11, at 8 (citing same).

[74] SHAPIRO & VARIAN, *supra* n.73, at 168.

[75] Douglas, *supra* n.11, at 20 ("Data access remedies have entered the conversation on digital platforms in no small part because of new theories of monopolization focused on data accumulation."); *see also* Stucke & Grunes, *supra* n.11, at 13 (suggesting data portability as a remedy to network effects and other competition issues in tech).

Such "data access" remedies have precedent in antitrust. As Erika Douglas has pointed out, telephone monopolies were forced to share their customer data with competing providers of yellow pages.[76] The remedy in the Microsoft case, often cited as lighting the path forward in challenging the market power of today's big tech companies, also involved forcing Microsoft to grant interoperability and other data access to its rivals.[77]

While promising as competition remedies, data access remedies in modern big tech present significant privacy concerns.[78] The data that data-access remedies would force the holders of market power to share are the very data over which privacy advocates would assert consumers should have the right to control.[79] Whereas privacy concerns would dictate that consumers should be able to choose what data they share with which companies and what those companies can subsequently do with the data, data portability remedies would force sharing of data to protect and enable competition.

Not all data access remedies present this concern. Some data portability remedies, for example, would empower the consumer to take control of his or her data held by one company, and transfer it to another.[80] This form of data portability, because it involves an individual's own data and sharing at the individual's direction, raises few privacy concerns.[81] But, what it saves on privacy, this type of solution loses on effectiveness; many are rightly skeptical that enabling this sort of data portability in tech markets will have a meaningful effect on competition. Indeed, several tech companies claim they already allow customers to port their data, but competition concerns grown unabated.

But even these types of remedies can raise novel privacy concerns. In some of the industries where data portability remedies are contemplated, such a social networking, one individual's personal data is inseparable from that of his or her friends'. Even if the individual porting the data consents, and indeed instigates, the movement of data from, say, Facebook to another social network, if it is to be effective, that data must also include information about his or her friends—their connections, their "likes," their sharing history, etc.[82] Sharing of exactly this type

[76] Douglas, *supra* n.11.

[77] *Id.*, at 19-20.

[78] *See Id.*; *see also* Caffarra, et al., *supra* n.1 (noting same). Douglas defines data access remedies as remedies that provide rivals with access to user data through interoperability, neutrality obligations, or disclosure. *Id.* at 17.

[79] *See* Douglas, *supra* n.11, at 23-24 ("While FTC data privacy enforcement works to limit the collection, use and sale of consumer information online, a data access remedy could do the opposite, requiring that rivals be permitted to access and use consumers' private information."); *id.* at 67 (noting that the effect on consumers is the same whether their privacy preferences are ignored for profit or overridden by a remedial order mandating data access).

[80] Such remedies are often analogized to the Telephone Number Portability Act, which gave consumers the right to keep their phone number when transferring service to a new telephone provider. *Id*.

[81] The primary privacy concern being data security and a worry that consumers will fail to safeguard their own data, leading to its misappropriation, or will overshare it with unscrupulous or incompetent companies.

[82] FTC Commissioner Noah Joshua Phillips, *Portability: An Event to Develop Rights and Uses*, Commission Nationale de l'Informatique et des Libertés (Nov. 23, 2020) (noting that mandating portability of information including social graphs or messages raises issues with consent, notice, and privacy).

of information, not about the users who consented but about their friends, was at the root of the Cambridge Analytica scandal.[83]

Moving away from the user-directed data portability proposals, other data-access remedies present privacy concerns of another magnitude. The creation of shared data banks or forcing dominant companies to allow rivals access to their networks and data would mean that users could not pick and choose the companies with whom they share their data. Instead, sharing data with one company would imply sharing it with all that company's rivals, as well. While this would level the competitive field on data, it would do so at the expense of user control and of privacy. And, far from countering the invasions of surveillance capitalism, it would enable more companies to compete in the effort to analyze consumers' data to try to discern their innermost motivations and desires and to influence and satiate them.

Much of the privacy legislation currently contemplated would make mandated interoperability and data sharing, at least as currently envisioned, harder if not impossible. Requiring user consent to such measures would gravely undermine their effectiveness as competition remedies, which depends on their deployment seamlessly and at scale.[84] Yet, the information likely to be at issue is, under privacy law, co-controlled by consumers.[85] Asking courts to weigh privacy concerns against competition concerns in such cases puts the courts in the role of deciding between public policy goals that properly belongs to the legislature.[86]

Competition law and policy has not yet grappled with this tension.[87] As Erika Douglas has observed, the past cases where enforcers have deployed data-access as a competition remedy all either occurred before the common law of privacy was developed or involved the forced sharing of company data and trade secrets, not user data.[88] And, as the telephone directory cases show, there is no inherent principle within antitrust law that precludes the disclosure of information as an antitrust remedy "simply because it is about individual consumers and potentially private."[89] But, the FTC's common law of privacy, and statutory privacy regimes like that in California, are "rooted in consumer control over personal information."[90]

Privacy regulation also risks introducing new competition concerns. Compliance with regulations can serve as a barrier to entry, particularly when complex or technologically

[83] Stutz, *supra* n.13, at 23.

[84] Douglas, *supra* n.11, at 79-80.

[85] Douglas, *supra* n.11, at 64.

[86] Although, as Douglas notes, the *Micosoft* court did wade tentatively into this territory in exempting Microsoft from the forced disclosure of APIs and other information that compromise the its security and anti-virus systems. *Id.* at 73 (citing *United States v. Microsoft*, No. 98-1232 (CKK), 2009 WL 1348218, at *6 (D.D.C. Apr. 22, 2009) (originally entered Nov. 12, 2002; modified Sept. 7, 2006; further modified Apr. 22, 2009)).

[87] Douglas, *supra* n.11, at 61 ("More than ever before, it is likely that competitively important data will also be subject to consumer data privacy interests. Antitrust theory has yet to consider the impact of this new reality on remedies.").

[88] Douglas, *supra* n.76. In contrast, "[c]onsumer information is fueling this generation of digital companies, and this means contemporary data access remedies are likely to involve that consumer data." *Id.* at 47, 53.

[89] *Id.* at 48.

[90] *Id.* at 62.

intensive.[91] Moreover, such barriers are often higher for smaller players and new entrants, because larger, more established companies can spread the costs of compliance across a broader user base. As a result, the scalability of compliance costs tends to favor large incumbents, and risks compounding and ossifying existing market concentration. This concern is particularly acute in tech, where the nature of network effects and winner-take-all markets means that competition most often comes from new entrants that are able to disrupt markets.

These risks and interactions make it imperative that competition and privacy policymakers work to understand the issues and concerns they each face. Policymakers must grapple with the tensions between antitrust and privacy law, weigh the competing interests, and choose how to reconcile them. This role cannot be left to courts.[92] The resulting policies will better serve both privacy and competition if those choices are made deliberately by policymakers with a full appreciation of the issues and the implications of various policy choices.

An additional area that merits more attention than it has gotten thus far, is the potential for technology to provide new solutions to privacy and competition concerns in tech markets and to resolve tensions between them. This area is too underdeveloped to know whether technological solutions are possible that could enhance competition in data-driven markets while simultaneously protecting privacy, but this area shows tremendous promise and should be fully explored.

VI. POLICY RECOMMENDATIONS

The primary goals of antitrust policy related to privacy should be to recognize and account for privacy-related market power and harms to competition and to protect and facilitate competition regarding privacy through resolving information asymmetries and other sources of market failure. In particular, we suggest the following:

- **Legislators and policymakers must move beyond notice-and-consent privacy regimes.** Notice-and-consent privacy regimes do not work, as markets or as a means for protecting privacy.[93] Instead, one of two paths (or a combination of both) should be explored: direct regulation of consumer data collection or strong property rights of consumers in their data. Which of these two approaches is favored depends in large part on the extent to which we believe there are large social costs from a lack of privacy or that privacy rights are so fundamental that they should be inalienable.

[91] *See, e.g.*, Phillips, *supra* n.82.

[92] While Douglas suggests that courts can incorporate privacy concerns into the remedies stage of their antitrust analysis because privacy violations cause "consumer harm," *see* Douglas, *supra* n.11, at 71, the consumer harm standard of antitrust law does not imply that antitrust analysis can and should account for all sources of harm to consumers. Such an interpretation would impose a "public interest" standard on antitrust that has never existed and was never intended. Rather, antitrust's consumer harm standard is limited to competition harms. Where, as may sometimes be the case with privacy and antitrust remedies, competition concerns are overridden by other policy interests, lawmakers must choose between competing policy considerations.

[93] There appears to be broad consensus on this point. *See, e.g.*, Stucke & Grunes, *supra* n.11, at 12 ("The consensus is that the current notice-and-consent framework is inadequate to safeguard privacy.").

- **In crafting privacy legislation, legislators and policymakers should account for potential impacts on competition.** To the extent substantive privacy regulations are imposed, we should be mindful to avoid regulatory regimes that will lock-in the currently dominant tech companies or otherwise be biased toward bigger companies with the means to spread compliance costs across a large user base. Such regulations should also, whenever possible, avoid compromising or imposing unnecessary burdens on data portability and interoperability.

- **Antitrust complaints about the deployment of privacy practices and tools must be evaluated on the basis of their competitive impact.** Courts and enforcers should not entertain or give weight to arguments that anticompetitive conduct is being undertaken "for privacy." Instead, antitrust enforcement should remain focused on the competitive impacts of the conduct at issue, and courts and enforcers should resist the temptation to attempt to balance privacy and antitrust concerns.

- **Antitrust enforcers, legislators, and policymakers should develop mechanisms to better account for privacy harms as anticompetitive effects.** To the extent that antitrust cannot account for privacy harms because it lacks effective tools for measuring those harms, there should be a concerted effort to develop those tools. Important theoretical work has already been done to develop the economics of zero-price markets and to unpack the so-called privacy paradox. More work is needed, however, to determine how and how much consumers truly value privacy and to expand our understanding of the economic and social impacts from degradation of privacy.

- **Antitrust enforcers, legislators, and policymakers should continue to develop merger policy that accounts for stores of personal data as a source of market power and degradations of privacy as an anticompetitive effect.** The collection and accumulation of data can be a source of market power and merger analysis should account for it. Likewise, degradations of consumer privacy can be a means for exercising market power. Merger policies should acknowledge and account for this. However, not all privacy harms and concerns are competition issues. Accordingly, it is critical that privacy issues are incorporated into merger analysis through the lens of competition and that guidance is developed for how to do so.