

April 2024

## Privacy's Commodification and the Limits of Antitrust

Jeffrey L. Vagle

*Georgia State University College of Law*

Follow this and additional works at: <https://scholarworks.uark.edu/alr>



Part of the [Antitrust and Trade Regulation Commons](#), and the [Privacy Law Commons](#)

---

### Recommended Citation

Jeffrey L. Vagle, *Privacy's Commodification and the Limits of Antitrust*, 77 Ark. L. Rev. (2024).

Available at: <https://scholarworks.uark.edu/alr/vol77/iss1/4>

This Article is brought to you for free and open access by the School of Law at ScholarWorks@UARK. It has been accepted for inclusion in Arkansas Law Review by an authorized editor of ScholarWorks@UARK. For more information, please contact [scholar@uark.edu](mailto:scholar@uark.edu), [uarepos@uark.edu](mailto:uarepos@uark.edu).

# PRIVACY'S COMMODIFICATION AND THE LIMITS OF ANTITRUST

Jeffrey L. Vagle\*

## INTRODUCTION

While markets and their mechanisms have long been the basis of mainstream U.S. economic thought, the version of market fundamentalism that found solid footing in the postwar years has expanded to permeate nearly every aspect of public and private life.<sup>1</sup> At the same time, a Cambrian explosion of technological growth made the gathering, processing, and distribution of information possible in ways unimaginable to those living only a few generations ago. The alignment of these phenomena is not entirely, and perhaps not very, coincidental. The control of enormous organizations like corporations and governments was highly dependent on the sort of information flow made available through the digital computer, and, with that control, all manner of new marketplace possibilities emerged.

Information was not only an instrumental mechanism to facilitate expanded market capabilities but was also identified as a resource upon which new markets could be built. That is, the increasingly large volumes of data being collected had value not only in their usefulness in running businesses or managing bureaucracies but could also be further processed to create highly detailed pictures of the people who had generated these data. Entire industries—and associated legal frameworks—were built

---

\* Assistant Professor of Law, Georgia State University College of Law. I wish to thank Steve Bellovin, Erika Douglas, Shreyas Gandlur, Kyle Hogan, Siona Listokin, Peter Ormerod, Neil Richards, Jeremy Seeman, Christelle Tessonno, Rory Van Loo, Mark Verstraete, Anne Washington, the organizers and attendees of the 2022 Privacy Law Scholars Conference; Sebastian Benthall, Gaia Bernstein, Elettra Bietti, Sherman Clark, David Gray, Amanda Levendowski, Kathy Strandburg, Benjamin Sundholm, Joe Turow, Salome Viljoen, Ari Waldman, and the organizers and attendees of the 2022 Joel R. Reidenberg Northeast Privacy Scholars Workshop; and the participants in the 2022 Georgia State University College of Law Faculty Retreat.

1. See JAMIE PECK, CONSTRUCTIONS OF NEOLIBERAL REASON 116 (2010).

around marketplaces established to support the collection, processing, and sale of this valuable resource. As technological advancement and growth outpaced existing legal and social rules and norms (as is often the case with new technologies), the resulting business models for these new industries relied heavily on the monetization of user-generated data, resulting in the commodification of personal information. We generate this information about ourselves both explicitly and implicitly, knowingly and unknowingly, sometimes with our consent but frequently without it, and its commodification is corrosive to privacy and, as I argue in this Article, forms the basis of an undesirable—or noxious—market.<sup>2</sup>

A recent resurgence of antitrust scholarship has advocated a return to the original purpose and intent of antitrust law in the United States prior to its recalibration in the 1970s and 1980s. Within this work, there is a related interest in applying this “neo-Brandeisian” antitrust law as a tool to regulate a technology industry that has grown far beyond the scale of the monopolistic trusts that inspired the creation of U.S. antitrust law in the first place. While antitrust regulation does have an important role in the regulation of Big Tech, its use to protect information privacy is flawed by its framing. Because antitrust law is meant to preserve competition within and between markets, its application validates, either explicitly or implicitly, the buying and selling of the commodities within those markets. Thus, to regulate information privacy primarily through antitrust law would accept personal data commodification and its corrosive effects on privacy.

---

2. See *infra* Section I.B. The careful reader may note a potential lexical mismatch when I refer to the commodification of privacy in this Article’s title, when what is actually being bought and sold as a commodity in this context is not privacy, *per se*, but the underlying data that forms the basis of privacy concerns. Despite this distinction, I beg the reader’s indulgence as I argue that the value we find in information privacy and the protection of data is, in fact, tightly coupled with the value the market assigns to those same data. That is to say, the commodification of data is essentially the commodification of privacy itself. So, while it may not technically be the case that “privacy” is itself a market good—and throughout this Article I will concentrate on the information that is being bought and sold—please note that it is privacy that is effectively commodified just the same. I will also note that this usage follows the same spirit as Paul Schwartz’s “commodification illusion.” Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 830-32 (2000).

This Article argues that the buying and selling of personal data forms what Debra Satz calls a “noxious market,” and, thus, any regulation of information privacy should not accept or depend upon its commodification but should stand on its own.<sup>3</sup> These noxious markets are not simply examples of market failures to be corrected through carefully limited economic interventions and thus restored to market optimality. The true roots of the problems relating to information privacy do not stem from inefficient externalities or a lack of competition, but from an inherent contradiction between privacy’s fundamental importance, both individually and societally, and a market-focused ideology. Subjecting privacy to market values is corrosive to individual and societal norms and tends to force much of this social cost onto those without the ability or means to engage in these markets. Further, because privacy power imbalances can originate not just between firms but within them, regulating privacy through an antitrust lens can actually exacerbate these inequities.

This Article proceeds in three parts. Part I first lays out the history and effects of data commodification, arguing that the market created by this commodification is noxious and undesirable. Part II examines the renewal of antitrust’s purpose as a regulatory tool, especially in the context of its use in the regulation of large technology firms. Finally, Part III argues that antitrust law, while useful to some aspects of technology regulation, is not an appropriate tool for the protection of information privacy, as it tacitly accepts the noxious market formed through data commodification.

## I. DATA COMMODIFICATION’S CORROSIVE EFFECT ON PRIVACY

Imagine a perfect market. In the most abstract economic terms, this would be some kind of framework or site for exchange where prices are set solely by the intersection of supply and demand.<sup>4</sup> As we layer on additional sociological detail, we see the market as a social interaction where goods, services,

---

3. DEBRA SATZ, *WHY SOME THINGS SHOULD NOT BE FOR SALE: THE MORAL LIMITS OF MARKETS* 9-10 (2010); *see also infra* Section I.B.

4. *See, e.g.*, PAUL KRUGMAN & ROBIN WELLS, *ECONOMICS* 13-15 (4th ed. 2015).

investments, and labor power are exchanged under a process governed by the market forces themselves.<sup>5</sup> Any intervention or interruption of this process disrupts the market and will alter the perfect market's natural equilibrium, producing allocative and productive inefficiencies.<sup>6</sup> If, however, utilitarian principles are followed, whereby individual self-interest will guide every market actor's actions like an "invisible hand," the market will settle into a natural equilibrium on its own and will promote the greatest amount of good for all involved.<sup>7</sup>

In practice, however, markets are not perfect. Even acknowledging as much, markets both real and metaphorical are prevalent in American social, political, and legal thinking.<sup>8</sup> A

---

5. See, e.g., RICHARD G. LIPSEY, AN INTRODUCTION TO POSITIVE ECONOMICS 61-62 (5th ed. 1979) ("In a market economy, the allocation of resources is the outcome of millions of independent decisions made by consumers and producers, all acting through the medium of markets.")

6. See, e.g., KRUGMAN & WELLS, *supra* note 4, at 132-34, 141-45.

7. See 2 ADAM SMITH, AN INQUIRY INTO THE NATURE AND CAUSES OF THE WEALTH OF NATIONS 181 (9th ed. 1799) [hereinafter 2 WEALTH OF NATIONS]; PAUL A. SAMUELSON, ECONOMICS 57 (11th ed. 1980) ("Without a central intelligence, it solves one of the most complex problems imaginable, involving thousands of unknown variables and relations. Nobody designed it. It just evolved, and like human nature, it is changing. But it does meet the first test of any social organization—it can survive."). Over the past fifty years or so, a version of this principle has found its way into legal theory. See, e.g., RICHARD A. POSNER, THE ECONOMICS OF JUSTICE 103-07 (1981) [hereinafter POSNER, ECONOMICS OF JUSTICE]. The focus for this theory is on finding the most efficient use of the law, such as the analysis of decisions that reflect the economic objective of wealth maximization, where "social wealth" is the variable in question. See Ronald M. Dworkin, *Is Wealth a Value?*, 9 J. LEGAL STUD. 191, 191 (1980); Richard A. Posner, *A Reply to Some Recent Criticisms of the Efficiency Theory of the Common Law*, 9 HOFSTRA L. REV. 775, 776 (1981) (outlining positive and normative schools of law and economics thinking). It is also worth noting that part of the work of Posner and others was meant to distinguish his use of wealth maximization theory from utilitarianism. See POSNER, ECONOMICS OF JUSTICE, *supra* note 7, at 48. There is some confusion, however, regarding which form of utilitarianism is objectionable to this legal theory, since utilitarianism is not in general a coherent theory, and differing utilitarian analyses will result depending upon which foundation one chooses. See J.J.C. Smart, *An Outline of a System of Utilitarian Ethics*, in UTILITARIANISM: FOR AND AGAINST 3, 7 (J.J.C. Smart & Bernard Williams eds., 1973).

8. See, e.g., John T. Jost, Sally Blount & György Hunyady, *Fair Market Ideology: Its Cognitive-Motivational Underpinnings*, 25 RSCH. IN ORGANIZATIONAL BEHAV. 53, 54 (2003) (studying social-psychological theories explaining the adoption of market ideologies in what were generally considered non-market spheres); ROBERT J. SHILLER, IRRATIONAL EXUBERANCE 170-72, 195-96 (3d ed. 2015) (examining history of increasing faith in market mechanisms in United States); MICHAEL ENGEL, THE STRUGGLE FOR CONTROL OF PUBLIC EDUCATION: MARKET IDEOLOGY VS. DEMOCRATIC VALUES 2-5 (2000) (discussing the expansion of market-based thought into the sphere of public education); David Singh Grewal & Jedediah Purdy, *Introduction: Law and Neoliberalism*, 77 L. & CONTEMP. PROBS., no. 4,

significant part of these market-oriented models is the concept of commodification, which, in its simplest form, stands for the proposition that anything that someone is willing to sell and others are willing to buy can and should be made available through the marketplace, at least in principle.<sup>9</sup> From a market absolutist point of view, anything and everything that meets the above definition is subject to commodification, which could include the valuation of personal relationships, religious ideals and commitments, one's physical environment, and the right to children and family.<sup>10</sup> Yes, an adherent of this viewpoint would acknowledge some of these items may be subjectively more valuable to some individuals, but it would be the market that would decide that item's objective value.<sup>11</sup> Under these criteria, anything people value should be commodifiable, and through the marketplace, its (objective) value would be maximized.<sup>12</sup>

---

2014, at 1, 1 (“[T]he assertion and defense of particular market imperatives . . . has reshaped most important domains of public and private life, and the law has been no exception.”); Hilde Eileen Nafstad, Rolv Mikkel Blakar, Erik Carlquist, Joshua Marvle Phelps & Kim Rand-Hendriksen, *Ideology and Power: The Influence of Current Neo-liberalism in Society*, 17 J. CMTY. APPLIED SOC. PSYCH. 313, 316 (2007) (“The market increasingly replaces the state as the principal regulatory force in society. Thus, the modern individual finds itself in a world characterised by an increasingly pervasive globalised ideology of competition, freedom from others, self-fulfilment and consumerism, taking place with a so-called free market.” (citations omitted)).

9. See Margaret Jane Radin & Madhavi Sunder, *Introduction: The Subject and Object of Commodification*, in *RETHINKING COMMODIFICATION: CASES AND READINGS IN LAW AND CULTURE* 8, 8 (Martha M. Ertman & Joan C. Williams eds., 2005).

10. See, e.g., David B. Resnik, *The Commodification of Human Reproductive Materials*, 24 J. MED. ETHICS 388, 388 (1998) (examining the moral basis for the commodification of human reproductive materials, including gametes, genes, zygotes, embryos, and genomes); Rutger Claassen, *The Commodification of Care*, 26 HYPATIA 43, 45, 60 (2011) (opining on the commodification of labor, especially in the care of others); Nancy Beadie, *Toward a History of Education Markets in the United States*, 32 SOC. SCI. HIST. 47, 47-48 (2008) (establishing a history of applying market thought to education in the United States); Michael Pappas & Victor B. Flatt, *The Costs of Creating Environmental Markets: A Commodification Primer*, 9 U.C. IRVINE L. REV. 731, 731-32 (2019) (exploring the emergence of markets for environmental goods).

11. While related to the complex theories of value coming from, for example, Marx, Smith, Ricardo, and others, my use of subjective and objective value here is more prosaic, indicating only an item's worth to the individual versus the price she could fetch for that item through a market. See, e.g., 2 WEALTH OF NATIONS, *supra* note 7, at 42.

12. See, e.g., RICHARD A. POSNER, *ECONOMIC ANALYSIS OF LAW* 33 (7th ed. 2007). Posner discusses an economic theory of property where everything having some kind of value should be commoditized, which

Nor are markets limited to merely “capitalist acts between consenting adults,” but through the laws, regulations, and institutions we establish to support said markets, they become a matter of public concern to everyone within the society that creates those laws, regulations, and institutions.<sup>13</sup> Pre-marginal revolution economists recognized this fact, that markets required some limits that arose as the product of social organization, and were thus embedded in society as institutions.<sup>14</sup> My focus in this Article is not on the market system per se, however, but on markets based on the commodification of particularly sensitive items that strain the core values of the society in which those markets act so much that they become anathema, and thus fall outside of the usual liberal economic ideals. I argue that this is the case in markets that commodify privacy.

A controversial proposal by Richard Posner makes it clear that concerns about the commodification of certain things are not some kind of abstract theory. In an article written with Elisabeth Landes, Posner proposed a market for the commodification of babies, taking into account the potential social costs and benefits of such a market, and claimed that there was a potential benefit, relative to the status quo, for families wishing to adopt a child, as a “free baby market” would reduce the negative effects of black market adoptions, including inflated prices, fraud, and abuse.<sup>15</sup> In fact, Posner argued that concerns about child abuse in a free baby

---

impl[ies] that if every valuable (meaning scarce as well as desired) resource were owned by someone (call this the criterion of universality), if ownership connoted the unqualified power to exclude everybody else from using the resource (exclusivity) as well as to use it oneself, and if ownership rights were freely transferable or, as lawyers say, alienable (transferability), value would be maximized.

*Id.*

13. See ROBERT NOZICK, ANARCHY, STATE, AND UTOPIA 163 (1974).

14. See 2 WEALTH OF NATIONS, *supra* note 7, at 412; KARL POLANYI, THE GREAT TRANSFORMATION 81 (Beacon Press 2001) (1944); 1 KARL MARX, CAPITAL: A CRITICAL ANALYSIS OF CAPITALIST PRODUCTION 280-81 (Frederick Engels ed., Samuel Moore & Edward Aveling trans., Appleton & Co. 1889) (1867).

15. Elisabeth M. Landes & Richard A. Posner, *The Economics of the Baby Shortage*, 7 J. LEGAL STUD. 323, 339-41, 347 (1978); POSNER, *supra* note 12, at 154 (“Since many people who are capable of bearing children do not want to raise them, many other people who cannot produce their own children want to raise children, and the costs of production to natural parents are lower than the value that many childless people attach to children, a market in babies for adoption would be feasible.”).

market should be lessened since “abuse is not the normal motive for adopting a child” and “[f]ew people buy a car or a television set in order to smash it,” adoptive parents who pay free market prices for their baby will be more likely to care for her, since “[i]n general, the more costly a purchase, the more care the purchaser will lavish on it.”<sup>16</sup> After publishing these articles, however, Posner later said that he “did not advocate a free market in babies” but rather was proposing that the commodification of babies should be allowed only where it is economically efficient and accompanied by consent by all relevant parties.<sup>17</sup> But why would Posner offer such a clarification if his original economic analysis of the factors was sound? We can find answers to this question in the levels of discomfort that many experience when faced with a market-oriented worldview that can extend to every facet of human life.

The tensions that universal commodification bring can manifest in a number of ways and are justified (or opposed) through political, moral, and economic argument that can sometimes muddy the waters through disagreement over the validity of these bases. For example, an economist might argue that some things should not be open to commodification if the externalities that emerge from their sale result in greater third-party costs than the benefits of the transaction can justify.<sup>18</sup> A sociologist might say that some things cannot be commodified because they are subject to moral or political duties that are owed by the individual to broader society and, therefore, are not the individual's to buy or sell.<sup>19</sup> Or an ethicist might counter that certain items cannot be commodified because they lie outside the normative sphere of the market.<sup>20</sup> These arguments, and many

---

16. Landes & Posner, *supra* note 15, at 343.

17. Richard A. Posner, *Mischaracterized Views*, 69 JUDICATURE 321, 321 (1986).

18. See, e.g., Norman W. Spaulding III, *Commodification and Its Discontents: Environmentalism and the Promise of Market Incentives*, 16 STAN. ENV'T L.J. 293, 298 (1997).

19. See, e.g., Resnik, *supra* note 10, at 388 (“Since commodities are alienable—they can be sold—it is possible to regard something as a form of property but not as a commodity. For example, we might view voting rights as a type of property but not as a type of commodity, since voting rights may be acquired, lost, or owned, but not sold.”).

20. See, e.g., Edmund D. Pellegrino, *The Commodification of Medical and Health Care: The Moral Consequences of a Paradigm Shift from a Professional to a Market Ethic*, 24 J. MED. & PHIL. 243, 244 (1999).



others, are not mutually exclusive and can take shape across multiple disciplines. But it is evident that for some subset of “things” within the scope of human existence (and for a generous definition of the term “things”), their commodification is challenged by a significant segment of society, even if we generally acknowledge that those things have some kind of value to us.<sup>21</sup>

Information clearly has value in many ways and in many forms.<sup>22</sup> If a manufacturer has more and better information about their customers, both actual and potential, those data can be used to create better products, improve product distribution, and respond to customer service requests. But that same information can also be used to manipulate that same group of customers through unscrupulous advertising techniques or to unfairly set prices or market shoddy products.<sup>23</sup> Irrespective of its use, however, the value of information has made the transition to monetary terms, a fact that has become the primary basis for most technology business models today.<sup>24</sup> I argue that the commodification of information—and with it, data privacy—has brought with it many of the negative aspects that are found in multiple arguments against an item’s commodification. Indeed, the harmful effects of privacy’s commodification, while dismissed as minimal when compared to the benefits of the technological innovations it supported, have become increasingly evident the further we have extended this market-oriented model.

---

21. See generally SATZ, *supra* note 3, at 3-4; MARGARET JANE RADIN, *CONTESTED COMMODITIES* 20-21 (1996); Richard Giulianotti, *Sport Spectators and the Social Consequences of Commodification: Critical Perspectives from Scottish Football*, 29 J. SPORT & SOC. ISSUES 386 (2005) (examining how commodification of sport affects fans and culture generally); Katharine Silbaugh, *Commodification and Women’s Household Labor*, 9 YALE J.L. & FEMINISM 81, 82-83 (1997) (criticizing commodification of domestic labor); Katharine Silbaugh, *Testing as Commodification*, 35 WASH. U. J.L. & POL’Y 309, 310 (2011) (criticizing commodification of education and testing); Marcos Barbosa de Oliveira, *On the Commodification of Science: The Programmatic Dimension*, 22 SCI. & EDUC. 2463, 2463-64 (2013) (exploring criticisms of commodification of scientific research); Julian J. Koplin, *Commodification and Human Interests*, 15 J. BIOETHICAL INQUIRY 429, 430 (2018) (arguing for boundaries in application of market principles to areas of vital human interest).

22. See *infra* Section I.A.

23. See, e.g., Ariel Dobkin, *Information Fiduciaries in Practice: Data Privacy and User Expectations*, 33 BERKELEY TECH. L.J. 1, 3-5, 7 (2018).

24. See Shoshana Zuboff, *Surveillance Capitalism and the Challenge of Collective Action*, 28 NEW LAB. F., Winter 2019, at 10, 10.

### A. Privacy's Value

Describing the value of something is often more difficult than we might initially think. When we observe that something is of higher or lower value, what exactly are we saying? We could mean that the item in question is economically expensive and that it would cost a significant amount of money to acquire it. We could also mean that something has significant moral, emotional, aesthetic, or social importance, and its loss would have an impact in ways that cannot be completely described in terms of dollar value. But a thing's value can—and often does—resonate simultaneously in both worlds, and our descriptions of its worth often blur the boundaries between these meanings. Economists may be more technical in the term's use, but we are generally less exacting when we deploy the term in everyday conversation.<sup>25</sup>

The term's relevance to this Article comes in both its economic and non-economic contexts. We assign value to things because we want or need them, according to our interests. Those interests can have roots that range from basic survival needs (food, water, shelter, and the like) to seemingly less concrete desires, such as art or religion. Anything along this spectrum can have value in the broad, inexact sense of the term, but we sometimes decide that certain items should not be bought or sold, even if markets do, did, or could exist for those items. Conversations on this topic debate whether the commodification of something is acceptable and, if so, whether there should be limits placed on its inclusion in the marketplace. These conversations are really questions about the moral value of an item, as well as the moral limits of market values, and there is often disagreement about the answers to these questions.

---

25. Early theorists of political economy went to some lengths to standardize the meaning of "value." For example, John Stuart Mill remarked, "The word Value, when used without adjunct, always means, in political economy, value in exchange." JOHN STUART MILL, PRINCIPLES OF POLITICAL ECONOMY 249 (J. Laurence Laughlin ed., D. Appleton & Co. 1884) (1848). Similarly, Adam Smith used the terms "value in use" and "value in exchange" to establish the same conventional meaning. 2 WEALTH OF NATIONS, *supra* note 7, at 42. Contrast this with the less exact usage of terms like "priceless" and "cheap." These terms can, of course, have meaning in the technical economic sense, as with Mill's and Smith's "value in exchange," but common usage often imparts a moral component, as well.

Privacy is one of those items we have these conversations about. And, while it is not a tangible item, its loss or degradation has tangible consequences. Different people occupying differing contexts will have differing ideas about its role, both across cultures as well as within households. Debates over privacy's commodification are not terribly new, but these conversations have carried with them much more significance since the advent of the Information Age and ubiquitous networked computing.

A significant difficulty when examining questions of privacy's value comes from its multiple, and often subjective, meanings. People can—and do—disagree about the things they care about, as well as to what degree, and those differences are often represented in the way we treat those things. Further, concepts like privacy, especially in rapidly changing technological environments like ours, can be slippery to pin down. That is, what exactly is privacy? Is it something that has intrinsic value, like good health or, for that matter, human life itself, or is its value derived from its effect on other (valued) aspects of our lives?

Additionally, what do we mean when we say that something like privacy has *value*? The word *value* itself requires some unpacking, as it would be a mistake to adopt a reductionist definition that does not take into account all of the various ways we use the term to describe properties that may be related but take on different valences in different contexts.<sup>26</sup> For example, we do not generally mean the same thing when we describe something in terms of its market value (e.g., price) versus when we describe something as valued in the way we honor, admire, respect, or love it.<sup>27</sup> Of course, there is often overlap between these categories. We can cherish something that also has a market value associated with it, and there are many other nuances we can attach to the word's use.<sup>28</sup>

But there are also sufficient differences between these definitions that can make us think twice before conflating the categories. Certain things have value in a moral, political, or

---

26. See, e.g., Ralph Barton Perry, *Economic Value and Moral Value*, 30 Q.J. ECON. 443, 444-45 (1916).

27. See *id.* at 445.

28. *Id.*

emotional sense that precludes their having value in the market sense. Or, more precisely, while it is acknowledged that the thing in question could be subjected to market values because of its special significance, its commodification is discouraged or forbidden.<sup>29</sup> Depending on the subject, sometimes the overlap between the senses of its value is near enough that, while some, perhaps many, consider its being bought and sold on the market as distasteful or even immoral, our laws may allow for its inclusion in the marketplace, albeit with certain restrictions.<sup>30</sup>

As the question of privacy's value is necessarily situated within societal structures, we might also look to anthropology for guidance. David Graeber observed that discussions of "value" generally fell into one of three categories: "value" in the sociological or philosophical sense, as in "family values"; "value" in the economic sense, such as an item's price; and "value" in a more specific linguistic sense, such as a method of differentiation between objects, which Graeber asserts are all versions of the same thing, despite marginal revolution economists' claim to the contrary.<sup>31</sup> Classical economists saw the necessary synthesis between value's seemingly different meanings, as shown in Smith's example of the seeming paradox that exists between an item's use value and its exchange value.<sup>32</sup> Smith recognized that "value" cannot have but one meaning for economic purposes, as it is part of a system of meaning that includes moral questions that cannot be simply discarded for market-related purposes. In this manner, privacy's value, and the data related to it, cannot simply be reduced to an economic calculation but must also incorporate moral, ethical, and symbolic evaluations that do not fit neatly within market definitions.<sup>33</sup>

---

29. See MICHAEL J. SANDEL, *WHAT MONEY CAN'T BUY: THE MORAL LIMITS OF MARKETS* 43, 56, 59 (2012); see generally ROBERT KUTTNER, *EVERYTHING FOR SALE: THE VIRTUES AND LIMITS OF MARKETS* (1997).

30. See SANDEL, *supra* note 29, at 43, 56, 59; see e.g., ELIZABETH ANDERSON, *VALUE IN ETHICS AND ECONOMICS* (1993).

31. David Graeber, *Value: Anthropological Theories of Value*, in *A HANDBOOK OF ECONOMIC ANTHROPOLOGY* 439, 439 (James G. Carrier ed., 2005).

32. "Nothing is more useful than water: but it will purchase scarce any thing; scarce any thing can be had in exchange for it. A diamond, on the contrary, has scarce any value in use; but a very great quantity of other goods may frequently be had in exchange for it." 2 *WEALTH OF NATIONS*, *supra* note 7, at 42.

33. As Graeber puts it,

Moral objections to the commodification of certain things rest mainly on a concern that the valued (in the extra-market sense) item in question will be somehow tainted or degraded by market values. A particularly vivid example of this can be found in the differing ways governments treat public health and healthcare, specifically in questions of access, efficacy, and affordability. In the United States, for example, healthcare is generally subject to market fundamentals, where private insurers act as both gatekeepers and private regulators, and market incentives have led to a number of perverse results.<sup>34</sup> Other nations have developed healthcare systems that rely very little or not at all on market dynamics, choosing instead to treat public health as a common good, often with better results when compared with the U.S. system, even when far less money is spent while doing so.<sup>35</sup> But in both examples, the populations of these countries would likely agree on certain broad healthcare and public health-related principles, such as the importance of basic sanitation, that no one in a medical emergency should be turned away from treatment, and that no one should be barred from a basic level of medical treatment because they cannot afford it.<sup>36</sup> And despite these commonly held values, healthcare's commodification has expanded in the postwar United States, sometimes with disastrous results.<sup>37</sup> How much a society is willing to tolerate this sort of overlap between extra-market and

---

The study of value, then, invariably takes us beyond what we normally refer to as "economics", for it leads us into moral, aesthetic and symbolic territory that is very hard to reduce to rational calculation and science. In the Western tradition, economics began as a series of questions about the morality of value; it could only claim the status of a science by trying to exorcise value completely.

Graeber, *supra* note 31, at 452-53.

34. See, e.g., Pellegrino, *supra* note 20, at 248, 256.

35. See, e.g., Jason Beckfield, Sigrun Olafsdottir & Benjamin Sosnaud, *Healthcare Systems in Comparative Perspective: Classification, Convergence, Institutions, Inequalities, and Five Missed Turns*, 39 ANN. REV. SOCIOLOGY 127, 131 (2013).

36. See, e.g., Norman Daniels, *Justice, Health, and Healthcare*, AM. J. BIOETHICS, Spring 2001, at 2, 4.

37. See, e.g., J. Michael McWilliams, *Health Consequences of Uninsurance Among Adults in the United States: Recent Evidence and Implications*, 87 MILBANK Q. 443, 444 (2009).

market values is dependent on a number of factors I will address later in this Article.<sup>38</sup>

When discussing something's value as it pertains to how laws and regulations should treat that thing, it is tempting to search for an objective standard of value that the oft-cited reasonable person would accept.<sup>39</sup> However, proper consideration for individual agency is important when examining the value of privacy. Paying attention to the subjective importance a person places on privacy, whether they explicitly articulate it or not, goes beyond the surface of individual well-being, but it can also provide a window into her more personal obligations, judgments, and beliefs. Because privacy has many definitions, often based on specific applications and contexts, establishing an objective value of privacy is a Sisyphean task. It is therefore helpful in this context to think of privacy not as an end in itself but as a means of protecting other things of value in society, including dignity, individual agency, psychological growth and health, and many other items core to a free society. This contextual framing of privacy's value is an important tool when evaluating market effects on privacy.

### **B. The Noxious Privacy Market**

When markets work, they work well. Market-based economies generally outperform command economies and create efficiencies and rewards across multiple metrics.<sup>40</sup> For all their general benefits, the core of market dynamics, the engine that makes it all work, can be found in its reliance upon individual selfishness.<sup>41</sup> By pursuing each's self-interest, market participants create an aggregate effect that simultaneously maximizes market output, efficiently allocates resources,

---

38. See *infra* Section I.B.

39. This is, of course, a famously difficult problem, one which philosophers have wrestled with since the days of Plato. See, e.g., L.P. Chambers, *Plato's Objective Standard of Value*, 33 J. PHIL. 596 (1936).

40. Problems begin to arise, however, when rules and assumptions of markets begin to fray. See CASS R. SUNSTEIN, *FREE MARKETS AND SOCIAL JUSTICE* 3-4 (1997).

41. See generally THOMAS HOBBS, *LEVIATHAN*, 439 (1651); Charles K. Wilber, *The 'New' Economic History Re-Examined: R.H. Tawney on the Origins of Capitalism*, 33 AM. J. ECON. & SOC. 249, 249 (1974).

decentralizes decision-making, and optimally satisfies demands.<sup>42</sup> The market signals its status through price, which is continually adjusted as market supply, demand, and individual preferences ebb and flow.<sup>43</sup> In the perfect market, this process will eventually settle to a point where the market's last buyer has obtained the market's last available product, and there is no waste, but even in the purest of marketplaces, this is an unobtainable ideal.<sup>44</sup>

These imperfect results attract market fundamentalist thinking that tend toward a circular argument if left to its own devices. This argument begins and ends with the concept that everything—or nearly everything—can be best understood as a market, and because of the naturally optimized outcomes of market dynamics, this lens will ultimately lead to the most efficient solution for everyone.<sup>45</sup> If, however, these optimal results do not come to fruition, that result can be blamed on a flawed marketplace, where these market failures can only be rectified through more market-friendly means.<sup>46</sup> These superficially simple solutions can be modeled, analyzed, simulated, and demonstrated through some rather complex mathematics to illustrate and prove this tautological point: markets produce optimal outcomes, but when they do not, they must not have been true markets in the first place.<sup>47</sup>

Among the key attractors to market fundamentalism lies in its theory of competition, where the conduct and performance of firms in a marketplace will be constantly driven toward innovation, quality, and optimal pricing through the pressures the market exerts through the need to compete for share.<sup>48</sup>

---

42. See Wilber, *supra* note 41, at 250.

43. See F.A. Hayek, *The Use of Knowledge in Society*, 35 AM. ECON. REV. 519, 526-27 (1945).

44. See, e.g., Sanford J. Grossman & Joseph E. Stiglitz, *On the Impossibility of Informationally Efficient Markets*, 70 AM. ECON. REV. 393 (1980).

45. See N. GREGORY MANKIW, PRINCIPLES OF ECONOMICS 147-50 (3d ed. 2004).

46. KUTTNER, *supra* note 29, at 6.

47. *Id.*

48. One of the ironic exceptions to this market axiom is found in Schumpeter's theory of innovation, where he posits that too much competition is actually bad in the long run:

What we have got to accept is that [the large-scale establishment or unit of control] has come to be the most powerful engine of [economic] progress and in particular of the long-run expansion of total output . . . . In this respect,

Governments and advocacy groups have claimed that dominant technology companies (collectively “Big Tech”) are operating outside of competitive constraints, leading to a host of problems that some propose can be solved by restoring an optimal level of competition to the technology marketplace.<sup>49</sup> Perhaps market competitive forces could be deployed to better regulate privacy.

But even in capitalist economies, markets are never the sole means by which decisions are made.<sup>50</sup> That is, there are historically areas within society that are set aside for extra-market valuation and determination of worth, where decisions regarding resource allocation are not entrusted to market norms for reasons of maintaining societal bonds, establishing or preserving equitable balances, protecting resources or relationships, or even enlightened self-interest.<sup>51</sup> Further, when markets do apply, there are political and social consequences to the operation of those markets, and those consequences should be factored into the legal and economic calculus of market thought.

We have historically set aside certain facets of life as too valuable, in the moral sense of the word, to be subject to market norms and commodification. For various reasons, critics of the universal (or near-universal) application of market values to aspects of everyday life have pointed out that these values are inappropriate in certain contexts, such as human organs and body parts and the adoption of children.<sup>52</sup> But why and when do we place certain items beyond the reach of markets or otherwise resist their commodification? A quick glance through U.S. legal history yields some surprising and unsavory results to contemporary minds, making it clear that rules regarding

---

perfect competition is not only impossible but inferior, and has no title to being set up as a model of economic efficiency.

JOSEPH A. SCHUMPETER, *CAPITALISM, SOCIALISM, AND DEMOCRACY* 106 (Routledge 1976) (1943).

49. See, e.g., James Clayton, *UK Government Sets Out Plans to Rein in Big Tech*, BBC (May 5, 2022), [<https://perma.cc/GP75-BDVN>]; Natasha Lomas, *EU's New Rules for Big Tech Will Come Into Force in Spring 2023, Says Vestager*, TECHCRUNCH (May 5, 2022, 6:26 AM), [<https://perma.cc/4WW8-AQZG>]; Katanga Johnson, *In Fiery Senate Hearing, U.S. CFPB Chief Focuses on Big Tech Influence, Competition*, REUTERS (Apr. 26, 2022, 4:18 PM), [<https://perma.cc/FNS4-GLCB>].

50. See Perry, *supra* note 26, at 443-51.

51. SANDEL, *supra* note 29, at 10; KUTTNER, *supra* note 29, at 53.

52. See SANDEL, *supra* note 29, at 110, 111; KUTTNER, *supra* note 29, at 47.



commodification are not static, but rather reflect a society's shared ideas and moral outlook, even if those rules can lag behind those shared values, sometimes significantly.<sup>53</sup>

Most objections to the commodification of certain items lie in their moral worth and an underlying respect for human dignity.<sup>54</sup> The moral importance of human life provided the foundation for the abolition of slavery in nineteenth-century America, removing the hitherto accepted legal principle of the “twofold character” of those relegated to slavery, where they are both person and property that could be legally bought and sold.<sup>55</sup> The Thirteenth and Fourteenth Amendments dissolved this concept, replacing it with a “free labor” concept of personhood under the principle that embodied the moral importance of an individual human life while still leaving room for the American ideals of liberty and self-determination by allowing one to sell their labor as they see fit.<sup>56</sup> Similarly, following years of legal doctrine preventing Congress from regulating many economic issues according to shared ethical values, the Supreme Court overturned its earlier decision preventing federal regulation of child labor and upholding the Fair Labor Standards Act, citing the earlier jurisprudence as “a departure from the principles which have prevailed in the interpretation of the Commerce Clause” which allow for regulation where commerce “may conceive to be injurious to the public health, morals or welfare.”<sup>57</sup>

Not every candidate for commodification is as generally uncontroversial as slavery or child labor, however.<sup>58</sup> For example, while the application of market values to surrogate motherhood has raised moral concerns for some, others see

---

53. See generally Igor Kopytoff, *The Cultural Biography of Things: Commoditization as Process*, in *THE SOCIAL LIFE OF THINGS: COMMODITIES IN CULTURAL PERSPECTIVE* 64, 77 (Arjun Appadurai ed., 1986).

54. See Cass R. Sunstein, *The Limits of Quantification*, 102 *CAL. L. REV.* 1369, 1369, 1376 (2014).

55. *United States v. Amy*, 24 F. Cas. 792, 810 (C.C.D. Va. 1859) (No. 14,445).

56. See Jedediah Purdy, *People as Resources: Recruitment and Reciprocity in the Freedom-Promoting Approach to Property*, 56 *DUKE L.J.* 1047, 1068-70 (2007).

57. *United States v. Darby*, 312 U.S. 100, 114, 116-17 (1941); *Hammer v. Dagenhart*, 247 U.S. 251 (1918).

58. Child labor is not as uncontroversial an issue as slavery, however. See, e.g., Michael Sainato, *Child Labor Laws in Some States May Be Weakened as US Industries Look to Hire Teens*, *GUARDIAN* (Nov. 2, 2021, 4:00 AM), [<https://perma.cc/7TEX-Q3F4>].

market values as leading to better outcomes, leading to an ongoing debate over the commodification of surrogacy.<sup>59</sup> Likewise, conversations regarding the commodification of medicine, pharmaceuticals, and healthcare generally are also filled with disagreement over their subjection to market values, especially if those conversations happen to take place in the United States.<sup>60</sup>

When markets commoditize certain items, such as human organs, or result in dangerous or corrosive externalities, like the funding of oppressive regimes or the restriction of life-saving medicines, many view these markets as repellent to core human values or, to use Debra Satz's term, noxious.<sup>61</sup> More specifically, the noxiousness of a market can be measured by evaluating four parameters: "vulnerability, weak [information/]agency, extremely harmful outcomes for individuals, and extremely harmful outcomes for society."<sup>62</sup> Vulnerability and weak information/agency are measures of a market's sources. That is, these parameters examine the elements that go into a particular market and its transactions.<sup>63</sup> Parameters that examine harms to both individuals and societies are measures of a market's outcomes.<sup>64</sup> It can be useful to evaluate markets along these axes, as they can help assess the varying ways a market's inputs and outputs can have negative effects without artificially limiting ourselves to evaluating a market based solely on the social meaning of the goods exchanged within it. This kind of analysis is especially useful when analyzing the effects markets have on less tangible things, such as privacy.

A market's inputs help frame a market's character. When we look at underlying vulnerabilities on the part of one or more market participants, we can better understand the power dynamics of that market.<sup>65</sup> It is understood, of course, that every market

---

59. See, e.g., Elizabeth S. Anderson, *Is Women's Labor a Commodity?*, 19 PHIL. & PUB. AFFS. 71, 74, 75 (1990).

60. See, e.g., Julia D. Mahoney, *The Market for Human Tissue*, 86 VA. L. REV. 163, 164, 169 (2000).

61. SATZ, *supra* note 3, at 3.

62. *Id.* at 9.

63. *Id.*

64. *Id.*

65. *Id.* at 97.

will have some degree of unequal footing between participants, where those inequalities may stem from past market choices or bad luck in the face of market risks, with predominant market-based thought viewing these relationships as unjust only when they significantly disrupt the security or stability necessary for an individual to maintain generally egalitarian relationships with others.<sup>66</sup> Evaluation of a market along the vulnerability axis of analysis occurs when, for example, someone in extreme poverty is forced to sell a valuable asset at a severely reduced price, even when the proceeds of that sale keep them from starving. That is, it is not necessarily the outcome of the transaction that measures the noxiousness of a market—after all, the seller’s overall well-being improved through the exchange—but also includes an assessment of the circumstances under which the seller made the choice to accept the outcome when a less vulnerable seller would not.<sup>67</sup>

Like vulnerability, the weak information/agency parameter also looks at the power dynamics of market participants, this time focusing on the availability of information relevant to the transaction as well as the transaction’s indirect effects on third parties who are not part of the market exchange.<sup>68</sup> General assumptions about market efficiency often include both the availability and awareness of information not only about the goods in question but also the consequences of the exchange itself.<sup>69</sup> These assumptions rarely hold in real-world markets, however, and assessing how those information imbalances generate harmful results helps us understand that market’s toxicity. Because every (real-world) market has information asymmetries inherent to its structure, however, it is necessary, as with the vulnerability parameter, to measure the degree of the harmful consequences rather than their mere existence.

---

66. See, e.g., Elizabeth Anderson, *How Should Egalitarians Cope with Market Risks?*, 9 THEORETICAL INQUIRIES L. 239, 240-41 (2008).

67. SATZ, *supra* note 3, at 97.

68. *Id.* at 96.

69. These kinds of assumptions are often so obviously flawed that they become elements of punch lines to jokes among economists. See, e.g., Ronald J. Gilson & Reinier H. Kraakman, *The Mechanisms of Market Efficiency*, 70 VA. L. REV. 549, 552 (1984).

An example of this kind of parametric assessment can be found in the child surrogacy market.<sup>70</sup> In this market, a contractual arrangement is made between a woman who is selling her ability to carry a child and prospective parents who are unable to conceive a child themselves.<sup>71</sup> In such an arrangement, it is possible, even likely, that the surrogate mother may lack the kind of information necessary to enter into a contractual agreement prior to her delivery of the child, especially if the woman has never been pregnant. But there are many contractual relationships that are entered into with this kind of information gap, and because it would be impossible to invalidate all such contracts, assessing this parameter becomes one of the levels of harm.

The agency aspect of this parameter arises when a market transaction affects third parties who are not directly involved in the transaction but depend on others to conduct the exchange on their behalf.<sup>72</sup> These third parties are therefore at a disadvantage in assessing how the transaction will directly or indirectly affect them. The arrangement and use of child labor provide an example of this market assessment, where a child's parents or other adults bargain over the child's labor, where the child herself will likely see little, if any, benefit.<sup>73</sup> Further, that child will likely bear the burden of harm that they had no opportunity to consider as a fully empowered participant in a market transaction.

When we look at a market's outcomes, in order to assess its noxiousness, we can first look to its harm to individuals.<sup>74</sup> This parameter is similar to the information/agency parameter discussed above but examines a market through the lens of its outcomes rather than its inputs. Many market transactions result in negative outcomes for individual participants or third parties, so we are interested in the degree of harm. For example, pharmaceutical markets that prevent those without means from purchasing necessary medicines garner disapproval, even when

---

70. See generally Debora L. Spar, *For Love and Money: The Political Economy of Commercial Surrogacy*, 12 REV. INT'L POL. ECON. 287 (2005).

71. See *id.* at 287-88.

72. See SATZ, *supra* note 3, at 97.

73. See generally Kathleen Beegle, Rajeev Dehejia & Roberta Gatti, *Why Should We Care About Child Labor? The Education, Labor Market, and Health Consequences of Child Labor*, 44 J. HUM. RES. 871 (2009).

74. See SATZ, *supra* note 3, at 94.

those markets are based on prices set by the usual rules of supply and demand.<sup>75</sup> Amartya Sen points out the “duality” of the person, defined in terms of agency as well as in well-being, that illustrates the different and separable kinds of harm that can arise along this axis.<sup>76</sup>

Potential harms from market outcomes are not limited in scope to individuals, but can also be harmful to societies in general, where market activity negatively affects political or social frameworks.<sup>77</sup> These market outcomes can be corrosive to democratic governance or values or induce or promote submissive, apathetic, or dependent attitudes throughout a populace, all of which can be harmful to the fundamental relationships and conditions necessary for healthy societies.<sup>78</sup> For example, we might evaluate a system that controls access to primary and secondary education through market mechanisms along this axis by assessing the societal importance of education to a healthy and functional society, measuring how such a market negatively affects access to primary and secondary educational opportunities, and gauging to what extent these outcomes erode those established societal norms.<sup>79</sup>

But what does one do with these metrics? After all, many markets will fare poorly along at least one of these axes. Which of these do we consider noxious? Surely, a market that performs especially poorly along any one axis, such as the markets for blood diamonds or child trafficking, will elicit feelings of strong discomfort or even revulsion such that these markets are highly restricted or banned outright.<sup>80</sup> But outside of some extreme examples, there is no bright-line rule that we can apply. How do we consider markets that may not stand out along any one axis

---

75. See, e.g., Keelia Silvis, M. Gilbertson, Y. Chen, J. Huape & D. Marshall, *The Insulin Affordability Crisis: A Policy Proposal to Protect Minnesotans*, PUB. HEALTH REV., Dec. 2020, at 1, 1.

76. AMARTYA SEN, ON ETHICS AND ECONOMICS 41 (John M. Letiche ed., 1988). As Satz so deftly puts it, “A benign dictator, for example, could meet all my basic welfare interests.” SATZ, *supra* note 3, at 95.

77. See SATZ, *supra* note 3, at 95.

78. *Id.* at 99-101.

79. *Id.* at 101-02.

80. See, e.g., Ravi Kanbur, *On Obnoxious Markets*, in GLOBALIZATION, CULTURE AND THE LIMITS OF THE MARKET: ESSAYS IN ECONOMICS AND PHILOSOPHY 39, 39 (Stephen Cullenberg & Prasanta K. Pattanaik eds., 2004).

but perform poorly in multiple parameters? As Satz puts it, these parameters help set up a framework to think about a market's noxiousness, not a blueprint.<sup>81</sup> And as a framework, these parameters are quite helpful in demonstrating the noxious effects the commodification of privacy can have.

When considering Satz's framework for noxious markets, it is important to understand the potential cumulative effect of the four axes, especially when considering areas where harm tends to be less tangible, such as privacy. Informally, one can think of this measurement as a point or vector in a four-dimensional graph whose coordinates correspond to the "score" associated with each of Satz's factors. We can associate this informal geometry to the moral costs of a transaction, which can vary between individuals and societies but tend to have valence within a society of shared norms and culture, even when any one of the "scores" within the Satz matrix is either low or difficult to measure. Examples of this can show up in what Margaret Radin calls "market-inalienability"—applying to those items that we may give away as gifts but have a high moral transaction cost when offered for sale.<sup>82</sup>

An important facet of noxious markets is the fact that they are resistant to correction by normal market-oriented means. More specifically, the factors that define a noxious market are not typically improved through a reevaluation of property rights or government interventions to preserve or protect competitive incentives. To apply Posner's "free baby market" as an example, the specific issues that most would find repellant, or at least discomforting, about such a market—the commodification of a child's life—would not be ameliorated by improving that market's competitive landscape.<sup>83</sup> Similarly, the market created through the commodification of privacy contains corrosive elements that market mechanisms will not correct.

---

81. See SATZ, *supra* note 3, at 10-11.

82. See Margaret Jane Radin, *Market-Inalienability*, 100 HARV. L. REV. 1849, 1853-54 (1987).

83. See *supra* notes 15-16 and accompanying text.

*1. Privacy and Vulnerability*

A real-world (read: non-ideal) market will undoubtedly have some amount of variance among its participants in their resources and capacities to fully understand the implications of their transactions. Because of this inevitability, we tolerate some amount of these differences between market participants. When these differing capacities result in unequal vulnerabilities to the extent that weaker parties are somehow exploited, however, we often take a harder look at that market with an eye toward correcting or eliminating the inequities.<sup>84</sup> Unfortunately, the commodification of privacy has largely been built upon just these kinds of unequal relationships.

Perhaps the most straightforward evidence of this transactional vulnerability can be found in the “pay for privacy” market, where individuals with means can purchase additional privacy protections from companies.<sup>85</sup> This market explicitly recognizes the value of information privacy and offers more privacy and data protection at premium prices, often marketing this luxury model as a feature to users.<sup>86</sup> The existence of such a market not only confirms privacy’s value to users of a company’s products and services but also implies the existence of lower-tier options for those unable to afford these premium privacy protections.<sup>87</sup> These lower-tier options are often the default monetization model for firms, where each customer’s data are taken as payment in exchange for free or reduced-cost use of the product or service offered.<sup>88</sup> The data collected on these “data as

---

84. Despite the predilection in American jurisprudence to favor markets and protect an individual’s freedom to contract, state and federal governments have been regulating the employment market since the late nineteenth century in order to protect vulnerable market participants. These regulations restricted employers and shielded workers from employer coercion through the setting of minimum wages, maximum hours, workplace safety, child labor laws, and protections for employee labor unions. *See, e.g.*, William B. Shaw, *Social and Economic Legislation of the States in 1890*, 5 Q.J. ECON. 385, 385 (1891).

85. *See, e.g.*, Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1387-88 (2017); Kenneth A. Bamberger et al., *Can You Pay for Privacy? Consumer Expectations and the Behavior of Free and Paid Apps*, 35 BERKELEY TECH. L.J. 327 (2020).

86. *See Elvy, supra* note 85, at 1388-89.

87. *See id.* at 1384-86.

88. *Id.*

payment” customers often include internet browsing habits, including on third-party sites through tracking mechanisms like web cookies or web beacons, even when the product or service is not actively in use.<sup>89</sup>

Further, because most of the details of these transactions are hidden by black box engineering practices, customers unable to purchase premium privacy protections are often poorly positioned to fully understand the implications of the transaction.<sup>90</sup> While related to the weak information/agency parameter, income-related and class-related disparities in knowledge regarding the availability of privacy-protecting laws and technologies exacerbate party vulnerability, putting lower-income users of technologies at a significant disadvantage when selecting and using these technologies.<sup>91</sup>

And while these vulnerabilities inherent in privacy transactions are significant on their own, the generally heightened surveillance of the poor, especially in the United States, further deepens the power differentials at hand.<sup>92</sup> Among the sources of the tendency toward heightened surveillance of the poor is the distinction we make—implicitly or explicitly—between the “deserving” and the “undeserving” poor.<sup>93</sup> Increased surveillance

---

89. See Janice C. Sipior, Burke T. Ward & Ruben A. Mendoza, *Online Privacy Concerns Associated with Cookies, Flash Cookies, and Web Beacons*, 10 J. INTERNET COM. 1, 1 (2011).

90. See, e.g., Julie E. Cohen, *Privacy, Visibility, Transparency, and Exposure*, 75 U. CHI. L. REV. 181 (2008); Laurence Diver & Burkhard Schafer, *Opening the Black Box: Petri Nets and Privacy by Design*, 31 INT'L REV. L., COMPUTS. & TECH. 68, 69-70 (2017); FRANK PASQUALE, *THE BLACK BOX SOCIETY* 1-4 (2015).

91. See Mary Madden et al., *Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans*, 95 WASH. U. L. REV. 53, 56-57 (2017).

92. See generally Nathan Newman, *The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google*, 40 WM. MITCHELL L. REV. 849 (2014); JOE SOSS, RICHARD C. FORDING & SANFORD. F. SCHRAM, *DISCIPLINING THE POOR* (2011); Virginia Eubanks, *Want to Predict the Future of Surveillance? Ask Poor Communities*, AM. PROSPECT (Jan. 15, 2014), [<https://perma.cc/WZC8-ZCTS>]; JOHN GILLIOM, *OVERSEERS OF THE POOR: SURVEILLANCE, RESISTANCE, AND THE LIMITS OF PRIVACY* (2001); Michele Estrin Gilman, *The Class Differential in Privacy Law*, 77 BROOK. L. REV. 1389 (2012); Virginia Eubanks, *Technologies of Citizenship: Surveillance and Political Learning in the Welfare System*, in *SURVEILLANCE AND SECURITY: TECHNOLOGICAL POLITICS AND POWER IN EVERYDAY LIFE* 89 (Torin Monahan ed., 2006); Michele Gilman & Rebecca Green, *The Surveillance Gap: The Harms of Extreme Privacy and Data Marginalization*, 42 N.Y.U. REV. L. & SOC. CHANGE 253 (2018).

93. See Michele Estrin Gilman, *The Return of the Welfare Queen*, 22 AM. U. J. GENDER, SOC. POL'Y & L. 247, 257 (2014); Kaaryn Gustafson, *Degradation Ceremonies*



burdens, and the diminished information privacy protections that follow from them, have also fallen disproportionately on minority populations, creating privacy vulnerabilities that share multiple aspects with civil rights concerns.<sup>94</sup> Historical patterns of class-based and racially-based surveillance, coupled with the emergence of surveillance capitalism, have created structural privacy vulnerabilities that many are unable to escape.

For many, the privacy choices that are left to them are to accept the lopsided terms that come attached to affordable technologies or do without them, essentially opting out of modern life.<sup>95</sup> Access to many technologies, especially internet-connected devices and applications, is essential for most employment, educational, and social opportunities today, and while low-cost technology products and services can provide beneficial access to those opportunities to those who would

---

*and the Criminalization of Low-Income Women*, 3 U.C. IRVINE L. REV. 297, 307, 336 (2013); KAARYN S. GUSTAFSON, CHEATING WELFARE: PUBLIC ASSISTANCE AND THE CRIMINALIZATION OF POVERTY 21-22 (2011); Khiara M. Bridges, *Privacy Rights and Public Families*, 34 HARV. J.L. & GENDER 113, 114-15 (2011); Jordan C. Budd, *A Fourth Amendment for the Poor Alone: Subconstitutional Status and the Myth of the Inviolable Home*, 85 IND. L.J. 355, 404-05 (2010); KHIARA M. BRIDGES, THE POVERTY OF PRIVACY RIGHTS 140 (2017).

94. See generally Anita L. Allen, *Dismantling the “Black Opticon”: Privacy, Race Equity, and Online Data-Protection Reform*, 131 YALE L.J. F. 907 (2022); Dorothy E. Roberts, *Prison, Foster Care, and the Systemic Punishment of Black Mothers*, 59 UCLA L. REV. 1474 (2012); Chaz Arnett, *Race, Surveillance, Resistance*, 81 OHIO ST. L.J. 1103 (2020); Dawinder S. Sidhu, *The Chilling Effect of Government Surveillance Programs on the Use of the Internet By Muslim-Americans*, 7 U. MD. L.J. RACE, RELIGION, GENDER & CLASS 375 (2007); Tressie McMillan Cottom, *Where Platform Capitalism and Racial Capitalism Meet: The Sociology of Race and Racism in the Digital Society*, 6 SOCIO. RACE & ETHNICITY 441 (2020); Nancy Leong, *Racial Capitalism*, 126 HARV. L. REV. 2151, 2152-53 (2013).

95. See Elvy, *supra* note 85, at 1388, 1402 (describing the “privacy-as-a-luxury model,” where “a company could offer three types of products to consumers: (1) a free product, (2) a basic paid product (freemium), and (3) a [privacy at a premium] product that combines the basic paid product with more privacy and data controls,” with customers unable to afford the higher-tiered products having fewer product options, and being “subjected to increased data collection and a lack of privacy and control with respect to their data”); Madden et al., *supra* note 91, at 67 (noting that “[i]nternet access has become an essential conduit for commerce, educational information, job opportunities, government services, and to maintain social connections to friends and family,” and thus “[s]imply opting out from using social media and other digital technologies to avoid these risks is not an option in today’s digital world, and may be impossible for some forms of surveillance. . . . If low-income users were to opt out of using certain websites or applications due to privacy concerns, they would also lose the ability to access the myriad opportunities associated with engagement in online life”).

otherwise be unable to afford them, they very often come with a privacy cost that can be difficult to measure solely in monetary terms.<sup>96</sup> This kind of transactional vulnerability can be further exacerbated by the fact that many low-income technology customers are at a disadvantage when it comes to knowledge of more privacy-protective products and services and the overall privacy harms they are subjected to through these pay-for-privacy models.<sup>97</sup>

Further differentiating and worsening this vulnerability is the difficult problem of providing privacy-protecting tools and resources to users, many (or perhaps most) of whom do not have the necessary background information to fully understand and deploy these resources effectively in increasingly complicated contexts, a problem that is especially pernicious among low-income and marginalized consumers.<sup>98</sup> In fact, much of the premise behind the “notice-and-consent” model favored by most federal and state privacy laws in the United States relies on an individual’s willingness and capacity for privacy self-help.<sup>99</sup> This

---

96. See generally Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793 (2022) (describing the spectrum of different harms that can arise from poor privacy protections, including physical, economic, reputational, discriminatory, relationship, autonomy, and psychological harms); Newman, *supra* note 92; Ryan Calo, *Privacy Harm Exceptionalism*, 12 COLO. TECH. L.J. 361 (2014) (articulating the seemingly heightened standards courts have applied when privacy plaintiffs are required to show “special” harm in order to have standing to sue).

97. See Bamberger et al., *supra* note 85, at 330 (“Properly understood, ‘free’ transactions are anything but. They are, instead, exchanges between consumers and services collecting their data—unequal exchanges, moreover, in which users possess limited awareness of the real costs incurred, and little ability to manage their privacy preferences.”); Lokke Moerel & Christine Lyon, *Commoditization of Data is the Problem, Not the Solution—Why Placing a Price Tag on Personal Information May Harm Rather Than Protect Consumer Privacy*, FUTURE OF PRIV. F. (June 24, 2020), [<https://perma.cc/RM5U-LQXV>] (observing that “companies deliberately make it difficult for consumers to make their actual [privacy] choice and seem to have little awareness of doing something wrong”); Madden et al., *supra* note 91, at 117-18 (noting the possibility that “privacy education, or increased privacy literacy, may help solve the [digital literacy] problems of low-income Internet users”).

98. See Madden et al., *supra* note 91, at 56, 58, 60; Elvy, *supra* note 85, at 1373.

99. See Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1880 (2013) (“Under the current approach, the law provides people with a set of rights to enable them to make decisions about how to manage their data. . . . The goal of this bundle of rights is to provide people with control over their personal data, and through this control people can decide for themselves how to weigh the costs and benefits of the collection, use, or disclosure of their information.”).

premise quickly begins to crumble when one examines the actual means available to individual users to self-manage their privacy, which are already significantly limited due to the sheer scope and complexity of the data marketplace, as well as confusion and outright deception baked into many nominal privacy protection tools.<sup>100</sup> The privacy self-help premise is even less credible when it comes to low-income and marginalized consumers, especially when these users are limited to older, cheaper technologies, many of which lack updated privacy protections and are more vulnerable to data theft.<sup>101</sup> Making matters worse, policymakers have interpreted user inability to self-manage their own privacy as a lack of concern over privacy matters generally, which fits neatly, if incorrectly, into the “notice-and-consent” model.<sup>102</sup> This framework overlooks the significant number of users who, due to a lack of sufficient or usable privacy-protective tools and resources, become a new category unto themselves, one made up of individuals who are left with no choice but to accept the privacy deal before them, irrespective of their actual desires.

## 2. *Privacy and Weak Information/Agency*

“Notice and choice” is the predominant mode of privacy governance in the United States, and while its name and intent might imply a robust and thorough exchange of information between parties in the wide spectrum of market transactions that involve user data, more often, the opposite holds.<sup>103</sup> As Paul Schwartz observed,

---

100. See WOODROW HARTZOG, *PRIVACY’S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES* 95-96 (2018).

101. See Madden et al., *supra* note 91, at 73-74.

102. See Chris Jay Hoofnagle & Jennifer M. Urban, *Alan Westin’s Privacy Homo Economicus*, 49 WAKE FOREST L. REV. 261, 267 (2014) (discussing Westin’s privacy segmentation of users into three groups: privacy fundamentalists who demonstrate “high privacy concern and high distrust in government, business, and technology,” privacy pragmatists who show “mid-level concern and distrust,” and privacy unconcerned who show “no or low concern or distrust”).

103. Schwartz, *supra* note 2, at 822 (“[W]idespread information asymmetries exist regarding personal data processing . . .”); see also Masooda Bashir, April D. Lambert, Carol Hays & Jay P. Kesan, *Online Privacy and Informed Consent: The Dilemma of Information Asymmetry*, in 52 PROC. OF THE ASS’N FOR INFO. SCI. & TECH. 1, 1 (2016); Geoffrey Lightfoot & Tomasz Piotr Wisniewski, *Information Asymmetry and Power in a Surveillance Society*, 24 INFO. AND ORG. 214, 214, 231 (2014).

[I]ndividuals are likely to know little or nothing about the circumstances under which their personal data are captured, sold, or processed. This widespread individual ignorance hinders development through the privacy marketplace of appropriate norms about personal data use. The result of this asymmetrical knowledge will be one-sided bargains that benefit data processors.<sup>104</sup>

Not only are the technological knowledge barriers quite steep for most people, but the “black box” approach to technology design can make it difficult, if not impossible, for users to know how their data is collected, stored, used, shared, and sold.<sup>105</sup>

Even when individuals wish to increase their control over which of their data is collected, by whom, and for what purposes, the information asymmetries can be quite stark. The enormous amount of data collection over the years has resulted in the establishment of a large and lucrative third-party data economy, where the collection, sale, and use of user data is distributed across a highly complex web of data collectors, managers, and brokers.<sup>106</sup> Further complicating matters, new sets of data can be generated from the data that have already been collected through sophisticated big data analytical methods, building increasingly detailed pictures of those who generated the original data.<sup>107</sup>

---

104. Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1683 (1999).

105. See Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 521-22 (2006).

106. See Anita L. Allen, *Protecting One's Own Privacy in a Big Data Economy*, 130 HARV. L. REV. F. 71, 71 (2016); Elvy, *supra* note 85, at 1371-72; Heiko Richter & Peter R. Slowinski, *The Data Sharing Economy: On the Emergence of New Intermediaries*, 50 INT'L REV. INTELL. PROP. & COMPETITION L. 4, 6, 10-11 (2019); Justin Sherman, *Data Brokers Are a Threat to Democracy*, WIRED (Apr. 13, 2021, 9:00 AM), [<https://perma.cc/3KRC-V628>]; Ryan Christensen, *The End of the Data Broker Model and the Rise of the Data Marketplace*, DATANAMI (Jan. 7, 2021), [<https://perma.cc/XX8D-AB62>]; *What Information Do Data Brokers Have on Consumers, and How Do They Use It?: Hearing Before the S. Comm. on Com., Sci., and Transp.*, 113th Cong. 3 (2013).

107. Allen, *supra* note 106, at 71; Priyank Jain, Manasi Gyanchandani & Nilay Khare, *Big Data Privacy: A Technological Perspective and Review*, 3 J. BIG DATA 25, 25 (2016); Lemi Baruh & Mihaela Popescu, *Big Data Analytics and the Limits of Privacy Self-Management*, 19 NEW MEDIA & SOC'Y 579, 582 (2017); Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239, 239 (2013); Gordon Hull, *Successful Failure: What Foucault Can Teach Us About Privacy Self-Management in a World of Facebook and Big Data*, 17 ETHICS & INFO. TECH. 89, 91 (2015); Solove, *supra* note 99, at 1889-90; Jonathan A. Obar, *Big Data*

Thus, those individuals interested in greater privacy control through monitoring, curation, or even selective self-censorship must somehow understand and navigate this opaque world where data fuels a complex economic machine.<sup>108</sup> Sometimes, consumers are able to accomplish some part of this goal through tools provided by third parties or through some facet of government regulation, but these methods are usually limited and put additional burdens on individuals, burdens that some will be unwilling or unable to bear.<sup>109</sup>

Privacy-related information asymmetries can be found in many places, but among the more commonly experienced manifestations of this phenomenon is the “click to agree” model of terms of service.<sup>110</sup> Under this framework of “privacy self-management,” itself a core element of U.S. privacy regulation, individuals are empowered with rights to notice, access, and consent, all of which are laudable goals, but implementations of this framework far too often work counter to the spirit of the original idea by hiding bad practices behind a veil of user consent based on little or no understanding of what is being consented to.<sup>111</sup> A self-determinative approach to privacy is attractive to

---

and *The Phantom Public: Walter Lippmann and the Fallacy of Data Privacy Self-Management*, *BIG DATA & SOC’Y*, July-Dec. 2015, at 1, 5.

108. See Allen, *supra* note 106, at 73-74; Elvy, *supra* note 85, at 1380, 1382-83.

109. See, e.g., Lorrie Faith Cranor, *Privacy Tools*, in *E-PRIVACY: DATENSCHUTZ IM INTERNET* 107 (Helmut Bäumler ed., 2000); Joel R. Reidenberg, N. Cameron Russell, Vlad Herta, William Sierra-Rocafort & Thomas B. Norton, *Trustworthy Privacy Indicators: Grades, Labels, Certifications, and Dashboards*, 96 *WASH. U. L. REV.* 1409, 1415 (2019); Lorrie Faith Cranor, *Necessary But Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice*, 10 *J. TELECOMM. & HIGH TECH. L.* 273, 274-75 (2012); Joshua A.T. Fairfield & Christoph Engel, *Privacy as a Public Good*, 65 *DUKE L.J.* 385, 456-57 (2015); Ira S. Rubinstein, *Regulating Privacy by Design*, 26 *BERKELEY TECH. L.J.* 1409, 1453 (2011).

110. See Jonathan A. Obar & Anne Oeldorf-Hirsch, *Clickwrap Impact: Quick-Join Options and Ignoring Privacy and Terms of Service Policies of Social Networking Policies* 2 (Aug. 4, 2017) (unpublished manuscript) [<https://perma.cc/L32Y-WK96>]; Ali Sunyaev et al., *Availability and Quality of Mobile Health App Privacy Policies*, 22 *J. AM. MED. INFORMATICS ASS’N.* e28, e31 (2015); Robert H. Sloan & Richard Warner, *Beyond Notice and Choice: Privacy, Norms, and Consent*, 14 *J. HIGH TECH. L.* 370, 373-74 (2014); Jonathan A. Obar & Anne Oeldorf-Hirsch, *The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services*, 23 *INFO., COMM’N & SOC’Y* 128, 140 (2020).

111. See Solove, *supra* note 107, at 1881; Yoan Hermstrüwer, *Contracting Around Privacy: The (Behavioral) Law and Economics of Consent and Big Data*, 8 *J. INTELL. PROP., INFO. TECH. & ELEC. COM. L.* 9, 9, 26 (2017); Woodrow Hartzog, *The Inadequate*,

long-established American social, political, and legal norms, but a reliance on notice, consent, and transparency is not only not enough to correct for complex privacy information gaps between parties, but it can actually serve to exacerbate them by overwhelming users with terms and agreements, confusing them with deceptive design patterns, or generally instilling a sense of privacy nihilism among technology consumers.<sup>112</sup> Because of the inherent complexities of technologies, their opaque nature, as well as the ability (or tendency) of technology firms to confuse, underinform, or misinform users, individuals are in a significantly weaker position with respect to privacy transactions.

In addition to this information imbalance, individual consumers are in weak agency positions in privacy-related transactions due in large part to the sizeable, robust, and largely invisible network of data brokers that buy, analyze, transform, repackage, and sell consumer information at global scales.<sup>113</sup> In fact, “data broker” is something of a generic term used to describe the wide array of firms built around the buying and selling of consumer information, and can include large, recognizable companies like Equifax and Experian, but applies just as well to thousands of companies, large and small, that can specialize along business lines such as marketing, risk analysis and mitigation, and identity verification.<sup>114</sup> The majority of these data brokers operate beyond the view of most consumers and are able to piece

---

*Invaluable Fair Information Practices*, 76 MD. L. REV. 952, 982 (2017); Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1503 (2019).

112. See Woodrow Hartzog, *What is Privacy? That's the Wrong Question*, 88 U. CHI. L. REV. 1677, 1684-85 (2021); Jeffrey L. Vagle, *Cybersecurity and Moral Hazard*, 23 STAN. TECH. L. REV. 71, 108 (2020); Ian Bogost, *Welcome to the Age of Privacy Nihilism*, ATLANTIC (Aug. 23, 2018), [<https://perma.cc/D3DK-B7UK>]; Fairfield & Engel, *supra* note 109, at 389-90, 393, 410; Ari Ezra Waldman, *Privacy, Notice & Design*, 21 STAN. TECH. L. REV. 74, 77 (2018).

113. See Matthew Crain, *The Limits of Transparency: Data Brokers and Commodification*, 20 NEW MEDIA & SOC'Y 88, 90 (2018); Aziz Z. Huq, *The Public Trust in Data*, 110 GEO. L. J. 333, 346-47 (2021); Sarah Myers West, *Data Capitalism: Redefining the Logics of Surveillance and Privacy*, 58 BUS. & SOC'Y 20, 29-30 (2019); JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 62 (2019); Ashley Kuempel, *The Invisible Middlemen: A Critique and Call for Reform of the Data Broker Industry*, 36 NW. J. INT'L L. & BUS. 207, 207 (2016).

114. See e.g., FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY, at i-ii (2014), [<https://perma.cc/UTR5-Q6C3>].

together startlingly accurate pictures of individuals through the collection and composite analysis of that person's data, gathered through complex transactions with other data collectors—offline and online—and brokers.<sup>115</sup> While the products and services provided by data brokers can provide benefits to consumers through fraud detection and prevention and the improvement of consumer products and their delivery, there are also potential harms to individual consumers that can stem from this shadow data marketplace, many times without a means of recourse for those harmed.<sup>116</sup> But underlying the data broker market is the diminished or non-existent agency the individual consumer has to understand or control the millions of transactions that include their data and affect their everyday lives.

A sobering illustration of the weak agency relationship between individuals and data brokers can be found in the common use of aggregated data products in pre-employment background investigations.<sup>117</sup> Included in these reports is any information regarding an applicant's criminal history, collected from federal, state, and local government databases and aggregated for presentation and sale by data brokers.<sup>118</sup> This information is thus neatly packaged into a convenient and accessible format that makes these data products attractive for employers and lucrative for data brokers, who have marketed these services to hiring companies as a means of "Explor[ing] Beyond the Resume."<sup>119</sup> While slickly presented through an easy-to-use web form, the data

---

115. *Id.*

116. *Id.* at v.

117. See, e.g., *Two Data Brokers Settle FTC Charges That They Sold Consumer Data Without Complying with Protections Required Under the Fair Credit Reporting Act*, FED. TRADE COMM'N (Apr. 9, 2014), [<https://perma.cc/9AKG-5JVL>]; Melanie Hicken, *Data Brokers Settle Charges Over Background Checks*, CNN (Apr. 9, 2014, 6:26 PM), [<https://perma.cc/9AJL-HEFC>]; Logan Danielle Wayne, *The Data-Broker Threat: Proposing Federal Legislation to Protect Post-Expungement Privacy*, 102 J. CRIM. L. & CRIMINOLOGY 253, 262-63 (2012).

118. See David McElhattan, *Punitive Ambiguity: State-Level Criminal Record Data Quality in the Era of Widespread Background Screening*, 24 PUNISHMENT & SOC'Y 367, 368-69 (2022); Megan Denver et al., *A New Look at the Employment and Recidivism Relationship Through the Lens of a Criminal Background Check*, 55 CRIMINOLOGY 174, 175 (2017).

119. Wayne, *supra* note 117, at 263; Bob Sullivan, *FYI EVERYONE: Spokeo Fined, but It's Still Really Spooky*, NBC NEWS (June 13, 2012, 12:07 PM), [<https://perma.cc/VU49-PL3E>].

that make up these reports are not always accurate, often failing to account for updates, corrections, or expungement, or are based upon government information that was incorrect in the first place.<sup>120</sup> Understanding, correcting, or otherwise controlling the relevant data about them that may exist in one data source—or, more likely, multiple data sources—is, at best, a daunting task, and more often an impossible one for most individuals, creating a significant agency problem in itself.<sup>121</sup> And while some regulations have been created to help correct this imbalance, the results have been far from perfect.<sup>122</sup>

### 3. *Privacy and Harmful Outcomes to Individuals*

The noxiousness of a market under Satz's framework looks not only at that market's sources but also its outcomes.<sup>123</sup> Specifically, we must ask whether the market is the cause of extreme harm to individuals or to society generally. The vast and complex data market—perhaps more accurately, a superset of many data markets—is a market that can be so characterized. Satz notes that noxious markets, that is, markets that have extremely harmful outcomes, evoke strong reactions of discomfort or even revulsion.<sup>124</sup> But in many instances, the general reaction to information privacy commodification has been, if not positive, then something of a resigned apathy driven by overwhelming complexity, a sense of helplessness, cynicism,

---

120. See DANIEL J. SOLOVE, *THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE* 46-47 (2004) (relaying the story of a Maryland woman who was fired from jobs as a substitute teacher and a child care director after her wrongful arrest for burglary was not cleared from the state's criminal databases); Susan Gardner et al., *Does Your Background Checker Put You in Jeopardy?: A Case for Best Practices and Due Diligence*, 11 J. LEGAL ETHICAL & REGUL. ISSUES, no. 2, 2008, at 111, 119-20 (citing studies showing criminal record information as "notorious for being 'outdated, inaccurate and incomplete,'" where "human errors, court delays, processing lags, and staffing shortages" impair the quality of the data," and quoting the president of a data broker as saying, "[w]e're not in the business of authenticating the identity of individuals. All we do is report the data that's supplied to us from the courts" (citations omitted)).

121. Nora A. Draper, *From Privacy Pragmatist to Privacy Resigned: Challenging Narratives of Rational Choice in Digital Privacy Debates*, 9 POL'Y & INTERNET 232, 245 (2017).

122. Kuempel, *supra* note 113, at 215-16; Crain, *supra* note 113, at 91-92.

123. See *supra* Section I.B.

124. See *supra* text accompanying note 61.



or a kind of Sisyphean fatigue.<sup>125</sup> These factors may mask or mute our discomfort with the harms, both individual and societal, that stem from commodified privacy, but despite the seemingly paradoxical differences between privacy attitudes and privacy behaviors, individuals care deeply about privacy protections, but the privacy choices that are usually offered to them are not really choices at all.<sup>126</sup>

So, where are the extreme harms to individuals arising from privacy commodification? For decades, scholars and practitioners have been pointing out the existence of serious privacy harms, often in the face of laws and regulatory frameworks that downplay, deny, or ignore those claims.<sup>127</sup> Part

---

125. See Eszter Hargittai & Alice Marwick, “What Can I Really Do?” *Explaining the Privacy Paradox with Online Apathy*, 10 INT’L J. COMM’N 3737, 3738, 3745 (2016) (examining the “privacy paradox” as the “gulf between self-reported privacy attitudes and actual privacy behaviors,” as an awareness of the risks of loss of privacy coupled with a feeling among individuals that “they lacked control over personal information posted online,” and frustration over complex and difficult to control privacy controls); Jessica Vitak et al., *Privacy Attitudes and Data Valuation Among Fitness Tracker Users*, in PROCEEDINGS OF THE 13TH INTERNATIONAL CONFERENCE ON INFORMATION: TRANSFORMING DIGITAL WORLDS 229, 230 (Gobinda Chowdhury et al. eds., 2018) (analyzing privacy attitudes and practices of fitness device users, where users’ lack of knowledge regarding data collection, use, and sale contributed to lax privacy habits).

126. The original notion of the “privacy paradox,” the idea that describes the gap between individual attitudes toward information privacy and their actual behaviors, is widely questioned as it fails to measure what matters when it comes to privacy protection. See Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 446 (2016) (“Users given a blunt choice between protecting their data and participating in modern society really have no choice at all, especially when the terms of any such choice are clouded by confusing technology and legal mumbo-jumbo, where long-term interests in privacy are hard to value, or where meaningful choice is an illusion.”); Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. 1, 22 (2021) (“[T]he very notion that people may have *actual or true* [privacy] preferences must be qualified. Whether measured via stated attitudes or behavior, preferences themselves are not static; they are highly contextual, subject to distortion, and malleable.”).

127. See, e.g., Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877, 877 (2003) (“The American legal system has generally rejected legal rights for data privacy and relies instead on market self-regulation and the litigation process to establish norms of appropriate behavior in society.”); Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1090 (2002) (“Judges, politicians, and scholars have often failed to adequately conceptualize the problems that privacy law is asked to redress. Privacy problems are often not well articulated, and as a result, we frequently do not have a compelling account of what is at stake when privacy is threatened and what precisely the law must do to solve these problems.”); Cohen, *supra* note 90, at 189 (“In a society committed at least to the desirability of the liberal ideal of self-determination . . . pervasive transparency is troubling because it constrains the range of motion for the development of subjectivity

of our broad ambivalence regarding privacy harms comes from our long-running inability to properly articulate these harms in a way that resonates beyond the legal academy.<sup>128</sup> And this ambivalence has made redressing these harms quite difficult, especially in U.S. courts.<sup>129</sup> But irrespective of the general treatment of privacy injuries under U.S. law, individual privacy harms are quite real.<sup>130</sup>

Common examples of individual privacy harms cross a wide spectrum, from injuries arising out of existing contract or tort jurisprudence to the increased risk of unknowable and future harms, such as identity theft, fraud, or even physical attack.<sup>131</sup> Even more stark—yet still under-recognized within the U.S. legal framework—are the privacy injuries sustained by individuals coming from minority or otherwise marginalized backgrounds.<sup>132</sup> Some of these harms come from the heightened surveillance certain subgroups are often subjected to, such as public aid recipients, immigrants, homeless people, and those with records of criminal convictions, with the majority of these burdens falling on poor, minority, and otherwise marginalized populations.<sup>133</sup>

---

through both criticism and performance, and it does not automatically cease to be troubling when the subjects of surveillance have indicated their willing surrender.”).

128. Solove, *supra* note 127, at 1088 (“Time and again philosophers, legal theorists, and jurists have lamented the great difficulty in reaching a satisfying conception of privacy.”); Hartzog, *supra* note 112, at 1678 (“[F]rom the early 1900s to the present day, lawmakers and judges have regularly been compelled to give the term ‘privacy’ a broad and consistent legal meaning. It hasn’t gone well.”).

129. Calo, *supra* note 96, at 361 (“[C]ourts and some scholars require a showing of harm in privacy out of proportion with other areas of law.”); Ryan Calo, *Privacy Law’s Indeterminacy*, 20 THEORETICAL INQUIRIES L. 33, 47 (2019) (“[M]any judges, and therefore the courts they sit upon, do not understand privacy loss as a cognizable injury, even as they recognize ephemeral harms in other contexts.”).

130. See generally Citron & Solove, *supra* note 96; NEIL RICHARDS, WHY PRIVACY MATTERS (2022); Hartzog, *supra* note 112, at 1684-85; Scott Skinner-Thompson, *Agonistic Privacy & Equitable Democracy*, 131 YALE L.J. F. 454, 454-55 (2021).

131. See Citron & Solove, *supra* note 96, at 817-18, 834-35.

132. See Allen, *supra* note 94, at 907; Arnett, *supra* note 94, at 1103-04; Sidhu, *supra* note 94, at 375-76; Cottom, *supra* note 94, at 441; Leong, *supra* note 94, at 2152-53.

133. See Gilman & Green, *supra* note 92, at 253; Dorothy E. Roberts, *Foreword: Race, Vagueness, and the Social Meaning of Order-Maintenance Policing*, 89 J. CRIM. L. & CRIMINOLOGY 775, 779-80 (1999); BRIDGES, *supra* note 93, at 32-33; Madden et al., *supra* note 91, at 61 (“[T]he harms to the poor from surveillance regimes reach far beyond generalized anxiety. This is because many surveillance systems that surround the poor are purposefully designed to deliver a message of stigma to the subject while reinforcing societal

Even outside of these particular circumstances, poor and marginalized people are faced with the prospect of submitting to individual privacy harms or opting out of modern society.<sup>134</sup>

But are these individual injuries actually harmful enough to warrant Satz's "extreme harm" categorization? If the examples of privacy injuries cited thus far were so deleterious, we would surely be seeing more of a hue and cry from individual users rather than what appears to be isolated pockets of privacy advocacy from a particularly zealous, though perhaps well-meaning, group of privacy scholars, practitioners, and consumer advocates. Some argue that, while privacy may be perceived as harmful in individual cases, this is based on subjective circumstances and preferences and does not rise to the level of "extreme harm."<sup>135</sup> Further, by treating potential privacy harm as a one-size-fits-all problem rather than a matter of individual choice, we risk stifling innovation and reducing overall product convenience for everyone.<sup>136</sup>

---

stereotypes about dependency. . . . Even if they are not always visible, privacy harms to the poor are real and can have physical and psychological impacts.”)

134. See Lior Jacob Strahilevitz, *Toward a Positive Theory of Privacy Law*, 126 HARV. L. REV. 2010, 2027-33 (2013); Elvy, *supra* note 85, at 1402 (“[I]n today’s digital age, low-income and minority consumers continue to have fewer options for online access. . . . Even when these groups of consumers obtain access to the Internet, they may be subjected to increased data collection and a lack of privacy and control with respect to their data unless they are able to pay for the products and concerns offered by [pay-for-privacy] companies to minimize these concerns.” (internal quotation omitted)).

135. Bobbie Johnson, *Privacy No Longer a Social Norm, Says Facebook Founder*, GUARDIAN (Jan. 10, 2010, 8:58 PM), [https://perma.cc/36VQ-5GUQ] (quoting Facebook founder Mark Zuckerberg who observed that “[p]eople have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people” and that privacy is “something that has evolved over time”); Jacob Kastrenakes, *Google’s Chief Internet Evangelist Says ‘Privacy May Actually Be An Anomaly,’* VERGE (Nov. 20, 2013, 11:10 AM), [https://perma.cc/MDX8-S9V4] (quoting Vint Cerf, Google’s chief internet evangelist, as stating that privacy has never been guaranteed, and may have been temporarily created through technology); M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1131 (2011) (distinguishing subjective privacy harms, or the perceptions of unwanted observations, from objective privacy harms, or the “unanticipated or coerced use of information concerning a person against that person”).

136. See, e.g., Jennifer Huddleston, Comment Letter on The Importance of Balancing Privacy with Innovation, Consumer Benefits, and Other Rights in the FTC’s Approach to Consumer Data Privacy (May 31, 2019), [https://perma.cc/28VM-R4JX] (public interest comment of Jennifer Huddleston, Research Fellow, Mercatus Center at George Mason University); Tal Z. Zarsky, *The Privacy-Innovation Conundrum*, 19 LEWIS & CLARK L. REV. 115, 125-26 (2015) (calling a “regulatory response” to privacy norms “ill-advised,” as technologies and privacy norms will rapidly change, and a more acceptable legal paradigm

The growing spectrum of individual privacy harms continues to be documented as new circumstances arise, new technologies are developed and deployed, and as our understanding of all of the above evolves, a thread that runs throughout the sources of these injuries is the relationship between privacy and power.<sup>137</sup> The power dynamic between the collectors of information and those from which it is collected is quite one-sided, where individuals are disempowered by information asymmetries, technology black boxes, and the lack of any real choices when it comes to privacy protections.<sup>138</sup> The harms—perhaps extreme harms—that emerge from these kinds of power imbalances surely rise to the level of Satz's characterization of noxious markets.<sup>139</sup>

---

take into account both “market innovation” and “social innovation”); Omer Tene & Jules Polonetsky, *Privacy in the Age of Big Data: A Time for Big Decisions*, 64 STAN. L. REV. ONLINE 63, 63-64 (observing that an overconcentration on privacy harms “could stir a regulatory backlash, dampening the data economy and stifling innovation”).

137. See RICHARDS, *supra* note 130, at 2, 3 (“We live in a society in which information is power, and ‘privacy’ is the word we use to talk about the struggles over personal information, personal power, and personal control. If we think of it this way, privacy is very much alive—but very much hanging in the balance.”).

[T]he legal framework within which collection, processing, and use of personal data occur is not simply a reactive framework, nor is it simply concerned with the relationship between commercial or law enforcement activities and privacy. The data flows extracted from people play an increasingly important role as *raw material* in the political economy of informational capitalism. Personal data processing has become the newest form of bioprospecting, as entities of all sizes . . . compete to discover new patterns and extract their marketplace value.

COHEN, *supra* note 113, at 48.

138. See RICHARDS, *supra* note 130, at 3 (describing struggles over information privacy as “fights over social power because information is power, and in any society, information about the people in it confers social power”); SOSHANA ZUBOFF, *THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER* 8 (2019) (“[S]urveillance capitalism births a new species of power that I call *instrumentarianism*. Instrumentarian power knows and shapes human behavior toward others’ ends. Instead of armaments and armies, it works its will through the automated medium of an increasingly ubiquitous computational architecture of ‘smart’ networked devices, things, and spaces.”); Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1912 (2013) (“If . . . the capacity for critical subjectivity shrinks in conditions of diminished privacy, what happens to the capacity for democratic self-government? Conditions of diminished privacy shrink the latter capacity as well, because they impair the practice of citizenship.”).

139. SATZ, *supra* note 3, at 95 (“[M]arkets can also be extremely harmful to individuals in ways that go beyond destitution. . . . We can define a set of basic interests for people,

#### 4. *Privacy and Harmful Outcomes to Society*

Just as weak information privacy protections can yield extremely harmful outcomes for individuals, so they can also result in extremely harmful outcomes for society as a whole. For example, scholars have long recognized information privacy's importance to a healthy democratic society.<sup>140</sup> In order for such societies to function—and thrive—certain basic needs must be met in order to allow individual citizens to reason, participate, and trust one another.<sup>141</sup> These harms can become particularly acute when inflicted on minority or otherwise marginalized segments of society.<sup>142</sup>

As Satz frames it, extreme societal harms from markets “can undermine the social framework needed for people to interact *as equals*, as individuals with equal standing.”<sup>143</sup> Admittedly, there

interest in minimum levels of well-being and agency, and define extremely harmful market outcomes as outcomes that leave these *basic* interests unsatisfied.”).

140. See Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 497 (1995) (“Politically, adequate standards for the treatment of personal information are a necessary condition for citizen participation in a democracy.”); Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 556 (1995) (“On the level of constitutional law, data protection in the United States is most successful when it is allied with the concept of deliberative democracy.”); Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877, 882-83 (2003) (“Society as a whole has an important stake in the contours of the protection of personal information.”); Schwartz, *supra* note 2, at 815.

141. See RICHARDS, *supra* note 130, at 9 (“[P]rivacy values . . . enable us to act in the various roles we play in society. Identity allows us to be thinking, self-defining humans; freedom lets us be citizens; and protection safeguards our roles as situated consumers and workers, allowing us, as members of society, to trust and rely on other people so that we can live our lives and hopefully build a better future together.”); COHEN, *supra* note 113, at 66 (identifying privacy-corrosive informational capitalism as having “profound implications both for individuals pursuing self-determination and for society more generally”); Elvy, *supra* note 85, at 1415-16 (“In addition to the potential harms to individual consumers, one must also consider that privacy is also a public value (of value to the democratic political system) and it is a collective value.” (quotation omitted)).

142. See Allen, *supra* note 94, at 913-14 (“African Americans dwell under the attentive eye of a Black Opticon, a threefold system of societal disadvantage comprised of discriminatory oversurveillance (the panopticon), exclusion (the ban-opticon), and predation (the con-opticon). This disadvantage—propelled by algorithms and machine-learning technologies that are potentially unfair and perpetuate group bias—is inimical to data privacy and an ideal of data processing that respects the data subject’s claim to human dignity and equality.”); Elvy, *supra* note 85, at 1423.

143. SATZ, *supra* note 3, at 95.

is room for fair-minded debate as to the working definition of terms like “equality,” but as information, and the use of that information, is a key component of exercised power, that power can, and is, used in ways that create, amplify, or otherwise worsen inequality among and between members of society.<sup>144</sup> In fact, history is replete with examples where information about individuals has been used, usually, but not exclusively, by governments to identify, separate, and even eliminate those people from society.<sup>145</sup>

But not every example of privacy injury needs to rise (or sink) to the level of mass internment or genocide to be considered an extreme harm in this framing. In fact, scholars have long made the point that a lack of privacy protections often has less obvious effects, quietly weaving themselves into societal norms until the damage has been done.<sup>146</sup> These sorts of societal injuries,

---

144. See, e.g., Madden et al., *supra* note 91, at 57 (“Not only are the poor subject to more surveillance than other subpopulations, and at higher stakes, but in addition, poor Americans’ patterns of privacy-relevant behaviors and device use open them up to greater vulnerability.”); Andrew W. Siegel, *Inequality, Privacy, and Mental Health*, 31 INT’L J.L. & PSYCHIATRY 150, 150-51 (2008) (discussing the effects privacy and mental health have on one another); Shoshana Zuboff, *Caveat Usor: Surveillance Capitalism as Epistemic Inequality*, in AFTER THE DIGITAL TORNADO: NETWORKS, ALGORITHMS, HUMANITY 174, 179-80 (Kevin Werbach ed., 2020) (discussing how data collection combined with a lack of adequate privacy protections means that “many societies enter the third decade of the twenty-first century marked by an extremely new form of social inequality that threatens to remake the social order as it unmakes democracy”).

145. Quite chillingly, as our facility for information collection and processing has improved, so has the brutal efficiency of mass detention and extermination. See, e.g., GRACE BALLOR & ADRIAN BROWN, THOMAS J. WATSON, IBM & NAZI GERMANY (2007); JR Minkel, *Confirmed: The U.S. Census Bureau Gave Up Names Japanese-Americans in WWII*, SCI. AM. (Mar. 30, 2007), [<https://perma.cc/S7XY-W6BL>]; Jim Fussell, *Indangamuntu 1994: Ten Years Ago Rwanda This Identity Card Cost Woman Her Life*, PREVENT GENOCIDE INT’L, [<https://perma.cc/57F4-F8HY>] (last visited Nov. 15, 2023); Natalie Brinham, “Genocide Cards”: Rohingya Refugees on Why They Risked Their Lives to Refuse ID Cards, OPENDEMOCRACY (Oct. 21, 2018), [<https://perma.cc/MJ2Y-2G8V>]; *China: Big Data Program Targets Xinjiang’s Muslims*, HUM. RTS. WATCH (Dec. 9, 2020), [<https://perma.cc/G47L-WR8N>].

146. See, e.g., Citron & Solove, *supra* note 96, at 847 (discussing the use of data to manipulate individuals as an autonomy injury, “exploiting a bias or vulnerability” to “circumvent[] the subject’s rational decision-making process”); Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 1030 (2014) (“All that is necessary to trigger . . . privacy harm is the belief or actuality that the person is being disadvantaged—that her experience is changing in subtle and material ways to her disadvantage.”); Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1423-24 (2001) (“[C]ertain uses of databases foster a state of powerlessness and vulnerability created by people’s lack of any meaningful form of participation in the

including discouraging individual participation in deliberative democracy, reducing individuals' autonomy and capacity for self-governance, and socially corrosive practices that profit or otherwise benefit from dividing and cataloging populations by groups, though perhaps less immediately drastic than Nazi Germany's Nuremberg Laws, still deserve to be considered extreme societal harms stemming from information markets.<sup>147</sup>

---

collection and use of their personal information. . . . Databases do not cause the disempowering effects of bureaucracy; they exacerbated it—not merely by magnifying of existing power imbalances but by transforming these relationships in profound ways that implicate our freedom.”); Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1935 (“[S]urveillance is harmful because it can chill the exercise of our civil liberties. . . . [B]ecause it can cause people not to experiment with new, controversial, or deviant ideas. . . . [And] its effect on the power dynamic between the watcher and the watched. This disparity creates the risk of a variety of harms, such as discrimination, coercion, and the threat of selective enforcement . . . .”); Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. 961, 985 (2021) (“A company that causes small injuries to millions of its customers can argue that each injury is *de minimis*, even though its vast market capitalization is the aggregate of billions of even tinier transactions.”).

147. See Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 196 (1890) (“The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man . . . has become more sensitive to publicity . . . but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.”); Reidenberg, *supra* note 140, at 896 (“The very breach of a recognized fair information practice standard inherently wrongs the individual. Such ‘unfair’ information practices are autonomous wrongful acts that do not depend on financial consequences for their harm. The wrongful disclosure in and of itself is an ‘actual harm’ to the individual. More broadly, the corrosive effect of information trafficking on society does not depend on the monetary damages potentially caused to particular victims.”); Neil Richards & Woodrow Hartzog, *Privacy’s Trust Gap: A Review*, 126 YALE L.J. 1180, 1200-01 (2017) (“Missing from the individual view of privacy and security law is the more nuanced understanding that in a connected society, privacy is not just an individual concern, but a major building block for society as a whole. This is privacy’s trust gap. Our dominant legal framework is frequently insufficient or incapable of comprehending the real and important injuries to the trust we need to flourish in our networked, digital society. If privacy is just a matter of individual concern, behaviors and forms of surveillance that breed suspicion raise no cognizable legal issues, even though they undermine our civil liberties or our willingness to connect to others in ways that produce social value. Privacy’s trust gap thus contributes to the sense of fatalism dominating our rhetoric and hindering our policy, particularly as the law conceives of us all as individuals on our own privacy islands, rather than emphasizing our interconnections.”).

### C. Why Market Failure Theory Is Insufficient Here

There are, of course, market-based means of dealing with market failures. We can observe that a market has flaws or externally borne costs, but we have means of accounting for those costs. Markets can arise and operate without full consideration of all relevant variables at the outset, and we generally do not eliminate those markets when unanticipated costs arise from related harms, especially if the benefits from those markets are worth preserving.<sup>148</sup> Rather, we find ways to account for and correct those costs, such as compensating those harmed, or otherwise restoring market optimality.<sup>149</sup> Even if data markets are flawed, is it not better to modify those markets through accepted tools and mechanisms, like laws or regulations that adjust pricing through taxes and fees, protect consumers from particularly egregious market actors, or preserve competitive playing fields for both new and existing firms? We do, in fact, apply a number of these methods with the goal of privacy protection, but the fundamental problem with these market-based approaches is their shared acceptance of privacy's commodification as an immutable fact.

Most economists are reluctant to categorically rule out particular marketplaces when they produce undesirable results or otherwise go awry but choose instead to account for that market's failures. For example, a market may result in environmental harms that are not limited to the parties directly involved in a transaction. These harms are seen as negative externalities, the costs of which are unaccounted for, and reveal a failure of that market. Market failures also arise from monopolies, monopsonies, and transaction costs that eliminate all but the largest market players. The term "market failure" implies a kind of rarity to the phenomenon, but unaccounted-for costs to third parties to a market transaction are quite common, as one might

---

148. See, e.g., Francis M. Bator, *The Anatomy of Market Failure*, 72 Q. J. ECON. 351 (1958).

149. A common example of this can be found in the various state models for regulating and reducing greenhouse gas emissions through policies such as a carbon tax. See, e.g., Brian Andrew, *Market Failure, Government Failure and Externalities in Climate Change Mitigation: The Case for a Carbon Tax*, 28 PUB. ADMIN. & DEV. 393 (2008).



expect in an increasingly complex and interconnected world. The solution to market failure due to negative externalities, say some market libertarians, is not to prohibit the market activities in question, but rather to properly account for those externalities through proper market pricing—if the costs due to externalities outweigh the benefits of the activity, the offending goods will effectively price themselves out of the market.<sup>150</sup>

But because pricing corrections for market failures rely on the use of economic tools that are meant to preserve as much of that market as possible, a market institutional framing of the problem can leave out aspects of the transaction that might be extraneous to market calculus, but quite important to those affected. Satz's "*Titanic* problem" illustrates this idea well.<sup>151</sup> In this thought experiment, we begin with the fact that there were only enough lifeboats for first-class passengers on the *Titanic*, leaving those who could not afford a first-class ticket with the choice to either risk their lives or avoid travel, a market framework we might now reject in its starkest forms, but in fact still tolerate in more subtle guises.<sup>152</sup>

Further, there is often a nearly insurmountable power imbalance between those conducting activities that yield negative externalities and those affected by them. Attempts to regulate market activities to compensate those harmed by negative externalities are often made quite difficult by market players whose profits or property are threatened by such efforts through industry capture or other rent-seeking behaviors.<sup>153</sup> Government attempts at climate policy, for example, are nearly always accompanied by stories of powerful industries exerting influence to protect their profit margins, influence that most of those

---

150. See NOZICK, *supra* note 13, at 79-81.

151. See SATZ *supra* note 3, at 84-89.

152. *Id.* at 84-85. A common example of this kind of market choice can be found in automobile safety, where cheaper cars come equipped with fewer safety features than more expensive ones. We see this in data markets, as well, where those with means can pay for more privacy than those without. See *supra* Section I.B.1.

153. See, e.g., Dieter Helm, *Government Failure, Rent-Seeking, and Capture: The Design of Climate Change Policy*, 26 OXFORD REV. ECON. POL'Y 182 (2010).

negatively affected by pollution from those industries are unable to exert.<sup>154</sup>

Another impression market failure theory leaves is one of neutrality. Externalities occur, economists assert, whenever unaccounted-for costs result in harm to those outside of a market transaction. But this is not—and cannot—be the case. Our individual religious preferences may, for example, be violated by a great many transactions, but we usually do not define these offenses as harms rising to the level of market failure.<sup>155</sup> In fact, economists tend to ignore many harms that do not meet the standards set by liberal theory, where a violation of personal preference is not a cost that must be accounted for. But this is not a neutral assertion, economically or morally, and assumes some kind of prior moral theory.

This dismissal of, or perhaps more charitably, failure to account for, moral considerations raised by the particulars of a market dulls our ability to critically evaluate that market and its effects. Some of the earliest proponents of market-based economic systems recognized the potential dangers inherent in such a morality-agnostic approach.<sup>156</sup> For example, Marx's labor theory of value was not intended merely as a method to explain pricing but was an explicit connection between economic theory and moral philosophy.<sup>157</sup> A person's labor is inextricably tied to her creativity, her physical well-being, and her social ties—

---

154. Jane Mayer provides a vivid example of industry capture by the Koch brothers' efforts to stop or delay government policies to curb or tax pollutants. See JANE MAYER, *DARK MONEY: THE HIDDEN HISTORY OF THE BILLIONAIRES BEHIND THE RISE OF THE RADICAL RIGHT* 8-15 (2017).

155. *But see* Lawrence Hurley, *Supreme Court Rules for Web Designer Who Refused to Work on Same-Sex Weddings*, NBC NEWS (June 30, 2023, 1:12 PM), [<https://perma.cc/AM5X-A7CC>].

156. See 1 ADAM SMITH, *AN INQUIRY INTO THE NATURE AND CAUSES OF THE WEALTH OF NATIONS* 372 (9th ed. 1799) ("The interest of the dealers . . . in any particular branch of trade or manufactures, is always in some respects different from, and even opposite to, that of the public. To widen the market and to narrow the competition is always the interest of the dealers. To widen the market may frequently be agreeable enough to the interest of the public; but to narrow the competition must always be against it, and can serve only to enable the dealers, by raising their profits above what they naturally would be, to levy, for their own benefit, an absurd tax upon the rest of their fellow citizens.").

157. See 1 MARX, *supra* note 14, at 156-94. It should be noted here that Marx was not the sole originator of the labor theory of value. Versions of this theory show up in varied forms in multiple sources, including Aquinas, Locke, Smith, and Ricardo.

essentially, labor is tightly wrapped up in how we are defined, and define ourselves, as human individuals. Marx asserted that when we pay for this labor with money, that money is symbolic of the market's acknowledgment of value, simultaneously reflecting both more than and less than an economist's theory of value.<sup>158</sup> To use market failure—especially in its limited scope as defined by post-marginal revolution economists—as a framework for acknowledging what is lost through privacy's commodification, we are artificially truncating the moral and ethical aspects of a data market. To put it another way, even if a market can be argued to be operating as intended, free of any serious failures, we can still label it as morally unsupportable.

## II. TECHNOLOGY AND THE RENEWAL OF ANTITRUST

### A. The Changing Face of Antitrust

When considering the applicability of antitrust law to remedy problems that arise out of privacy concerns, it is useful to understand what problems antitrust law was intended to solve in the first place. Understanding antitrust law's goals, however, is not as straightforward a proposition as one might expect. Herbert Hovenkamp observed, "Few people dispute that antitrust's core mission is protecting consumers' right to low prices, innovation, and diverse production that competition promises."<sup>159</sup> But there is significant disagreement regarding the means by which antitrust law should achieve those goals, as well as some rather heated debate over Hovenkamp's initial proposition.<sup>160</sup>

---

158. *Id.* at 156-57.

159. HERBERT HOVENKAMP, *THE ANTITRUST ENTERPRISE: PRINCIPLE AND EXECUTION* 1 (2005).

160. Richard Posner observed,

There are federal antitrust statutes, and they are brief and readable compared to the Internal Revenue Code. But their operative terms—"restraint of trade," "substantially to lessen competition," "monopolize"—are opaque; and the congressional debates and reports that preceded their enactment, and other relevant historical materials, cast only a dim light on the intended meaning of the key terms. The courts have spent many years interpreting, or perhaps more accurately supplying, that meaning. But the course of judicial interpretation has not always run true. And the rules of law as they are articulated and as

In fact, much of the debate over antitrust policy stems from disagreement about its purpose, which creates differing schools of thought as to how to achieve those purposes.<sup>161</sup> A significant source of the disagreement can be found in the fact that the only explicitly articulated purpose of antitrust policy is to benefit consumers through competitive markets. Louis Brandeis, having observed the effects of industrial concentration that helped define the Gilded Age, saw competition policy as part of a larger socioeconomic and political question for the United States, one where concentrated private power was weighed against its effects on equality, freedom, and democracy itself.<sup>162</sup> Theodore Roosevelt made antitrust a central issue of his presidency, rejecting President William McKinley's *laissez-faire* policies, which had largely left the nascent Sherman Antitrust Act of 1890 to gather dust, preferring instead to let market forces exercise their own sovereignty.<sup>163</sup> The Roosevelt Administration wasted no time in enforcing the Sherman Act's provisions, seeing the effort as necessary to counter the monopoly threat to democratic rule.<sup>164</sup> In the government's suit against Standard Oil, the Supreme Court affirmed the lower court's decision to break the firm into thirty-four parts, agreeing the company was exactly the sort of anticompetitive trust that the Sherman Act was meant to prevent.<sup>165</sup> In his concurrence, Justice Harlan articulated the

---

they are applied to alter behavior are often and in this instance two quite different things.

RICHARD A. POSNER, *ANTITRUST LAW: AN ECONOMIC PERSPECTIVE* 1 (2d ed. 2001). See, e.g., Maurice E. Stucke, *Reconsidering Antitrust's Goals*, 53 B.C. L. REV. 551 (2012); Thomas J. Horton, *Restoring American Antitrust's Moral Arc*, 62 S.D. L. REV. 11 (2017); Barak Orbach, *Foreword: Antitrust's Pursuit Purpose*, 81 FORDHAM L. REV. 2151 (2013).

161. Compare POSNER, *supra* note 160, at 1-2 (asserting that antitrust law is primarily concerned with promoting social welfare), with Robert H. Lande, *Wealth Transfers as the Original and Primary Concern of Antitrust: The Efficiency Interpretation Challenged*, 34 HASTINGS L.J. 65, 68 (1982) (arguing that Congress passed the antitrust laws to further economic objectives, but primarily objectives of a distributive nature rather than of an efficiency nature).

162. See LOUIS D. BRANDEIS, *THE CURSE OF BIGNESS* 38-39 (Osmond K. Fraenkel ed., 1935).

163. See Wayne D. Collins, *Trusts and the Origins of Antitrust Legislation*, 81 FORDHAM L. REV. 2279, 2346 (2013).

164. See GERALD BERK, *LOUIS D. BRANDEIS AND THE MAKING OF REGULATED COMPETITION, 1900-1932*, at 35-40 (2009).

165. *Standard Oil Co. v. United States*, 221 U.S. 1 (1911).

original goals of antitrust law by “stat[ing] the circumstances under which Congress passed the Antitrust Act”:

All who recall the condition of the country in 1890 will remember that there was everywhere, among the people generally, a deep feeling of unrest. The Nation had been rid of human slavery—fortunately, as all now feel—but the conviction was universal that the country was in real danger from another kind of slavery sought to be fastened on the American people, namely, the slavery that would result from aggregations of capital in the hands of a few individuals and corporations controlling, for their own profit and advantage exclusively, the entire business of the country, including the production and sale of the necessities of life. Such a danger was thought to be then imminent, and all felt that it must be met firmly and by such statutory regulations as would adequately protect the people against oppression and wrong. Congress therefore took up the matter and gave the whole subject the fullest consideration. . . . Guided by these considerations, and to the end that the people, *so far as interstate commerce* was concerned, might not be dominated by vast combinations and monopolies, having power to advance their own selfish ends, regardless of the general interests and welfare, Congress passed the Anti-trust Act of 1890 . . . .<sup>166</sup>

This message resonated with federal antitrust enforcement through the mid-twentieth century, identifying competition policy as larger than a mere economic question, but rather as a necessary part of a functional democracy.<sup>167</sup> The Warren Court continued in this vein and often upheld antitrust actions before them, even if that sometimes meant higher consumer prices (after larger firms artificially lowered prices in order to squeeze out smaller competitors).<sup>168</sup> But to many economists, especially those aligned with the Chicago School, this approach to antitrust was, at best, a confused law and policy mess and, at worst, a significant drag on the economic factors competition policy was meant to protect.<sup>169</sup> Chicago School economists argued that the antitrust

---

166. *Id.* at 83-84 (Harlan, J., concurring in part and dissenting in part).

167. See TIM WU, THE CURSE OF BIGNESS: ANTITRUST IN THE NEW GILDED AGE 30-31 (2018).

168. See HOVENKAMP, *supra* note 159, at 1.

169. See WU *supra* note 167, at 31-32; HOVENKAMP *supra* note 159, at 1-10.

enforcement policies that had emerged as dominant since the first Roosevelt Administration were actually bad for consumers and did not enhance competition, but rather propped up inefficient companies that would have otherwise been unable to compete with their more efficient peers.<sup>170</sup> Instead of punishing efficiency, which may result in fewer, larger firms, antitrust policy should concentrate on fostering benefits for the consumer.<sup>171</sup>

Robert Bork, one of the more severe critics of the Warren Court's approach, argued that the courts had been reading antitrust policy incorrectly and posited that the true legislative intent behind the Antitrust Act was not the preservation of competition but consumer welfare.<sup>172</sup> Under this rubric, antitrust actions would be required to prove that anticompetitive behavior resulted in higher prices for consumers—anything else would fall short of the behavior Congress intended to proscribe in the Act.<sup>173</sup> With the publication of Bork's *The Antitrust Paradox*, an emerging antitrust counterrevolution found its voice, and a dismantling of the Brandeisian/Rooseveltian approach to antitrust began in earnest.<sup>174</sup>

Antitrust enforcement decreased throughout the 1970s, with the last major action against AT&T, then the largest company in the world.<sup>175</sup> From the Reagan Administration forward, the *laissez-faire* doctrine of the McKinley Administration resumed its place in antitrust policy.<sup>176</sup> The Chicago/Borkian consumer welfare standard emerged as the winner of the antitrust culture war that had been brewing for decades.<sup>177</sup> By 2004, the idea of monopolistic firms was no longer anathema. In fact, monopolies may be a good thing. In a 2004 Supreme Court decision, Justice Antonin Scalia observed that

---

170. See WU, *supra* note 167, at 31.

171. *Id.* at 137-39.

172. *Id.* at 17.

173. *Id.*

174. See ROBERT H. BORK, *THE ANTITRUST PARADOX: A POLICY AT WAR WITH ITSELF* 418-23 (1978).

175. See *United States v. AT&T*, 552 F. Supp. 131, 131, 151-52 (D.D.C. 1982).

176. See WU, *supra* note 167, at 44.

177. See John J. Flynn, *The Reagan Administration's Antitrust Policy, "Original Intent," and the Legislative History of the Sherman Act*, 33 *ANTITRUST BULL.* 259, 262-64 (1988).

[t]he mere possession of monopoly power, and the concomitant charging of monopoly prices, is not only not unlawful; it is an important element of the free-market system. The opportunity to charge monopoly prices—at least for a short period—is what attracts “business acumen” in the first place; it induces risk taking that produces innovation and economic growth. To safeguard the incentive to innovate, the possession of monopoly power will not be found unlawful unless it is accompanied by an element of anticompetitive *conduct*.<sup>178</sup>

However, over the past few years, a renewed focus on political economy, inequality, and threats to democracy has brought with it new attention to antitrust policy as a tool to address some of these issues.<sup>179</sup> Specifically, these re-evaluations of antitrust’s goals examine some of its earliest justifications, especially the role of monopoly and oligopoly in regressive wealth distribution and economic inequality, the outsized political power exercised by large firms, the attendant effects on democratic society, and the moral questions that underlie all of these topics.<sup>180</sup> A central thesis of these recent inquiries observes the fact that the system of capitalism from which these issues have arisen is not inevitable, but one that was designed and built as “a legal ordering: the bargains at the heart of capitalism are products of law.”<sup>181</sup> This reflection has emerged with study of the neoliberal legal-political-economic system described above.<sup>182</sup>

This renewed philosophy of antitrust law and policy retains its original focus on maintaining competitive markets, but includes with that focus an expanded view of what effects monopoly’s concentration of wealth and power can have on areas of life that fall outside the scope of the Chicago/Bork view of

---

178. *Verizon Commc’ns Inc. v. L. Offs. of Curtis V. Trinko, LLP*, 540 U.S. 398, 407 (2004).

179. See, e.g., Lina Khan & Sandeep Vaheesan, *Market Power and Inequality: The Antitrust Counterrevolution and Its Discontents*, 11 HARV. L. & POL’Y REV. 235, 235-37 (2017); Jonathan B. Baker & Steven C. Salop, *Antitrust, Competition Policy, and Inequality*, 104 GEO. L. J. ONLINE 1, 4-5 (2015).

180. See, e.g., Maurice E. Stucke, *Morality and Antitrust*, 2006 COLUM. BUS. L. REV. 443, 444-49 (2006).

181. David Singh Grewal, *The Laws of Capitalism*, 128 HARV. L. REV. 626, 652 (2014).

182. See *supra* Section I.B.

antitrust.<sup>183</sup> To incorporate this larger view, antitrust scholars and practitioners see a need to reestablish antitrust law's original goals and displace the current focus on market efficiency and pricing.<sup>184</sup> Harms from monopolies and oligopolies are not limited only to consumer prices, and antitrust law and policy should reflect that.

### B. How to Solve a Problem Like Big Tech

A recent target of this renewed antitrust philosophy has been the technology industry, specifically very large multinational firms such as Amazon, Facebook (now Meta), Google (or its post-reorganization parent company, Alphabet), and Apple, often generically included in the broadly defined term "Big Tech."<sup>185</sup> As various new digital technologies have been introduced over the past few decades, they have become integral parts of everyday life, sometimes in trivial ways, but just as often directly affect our livelihoods, social interactions, and political positions and activities in ways that we have not seen with prior technological revolutions.<sup>186</sup> Because of this technology ubiquity—and dependence—a small number of technology companies have grown into some of the largest firms the world has ever seen, overtaking historical behemoths like AT&T, Standard Oil, and United States Steel.<sup>187</sup>

---

183. See, e.g., Joseph Fishkin & William Forbath, *The Anti-Oligarchy Constitution*, 94 B.U. L. REV. 669 (2014).

184. See Khan & Vaheesan, *supra* note 179, at 235-37.

185. See, e.g., Joshua P. Zoffer, *Short-Termism and Antitrust's Innovation Paradox*, 71 STAN. L. REV. ONLINE 308, 309 (2019).

186. See, e.g., Lina M. Khan, *The Separation of Platforms and Commerce*, 119 COLUM. L. REV. 973, 983-84 (2019).

187. In terms of net annual income (adjusted for inflation), today's large technology companies take in more in profit than their nineteenth- and early twentieth-century peers. For example, when the Standard Oil Corporation was at its largest and most powerful, controlling between eighty-eight and ninety-one percent of all United States oil production, the firm earned roughly \$1 billion per year, adjusted for inflation. See Gene Quinn & Steve Brachmann, *Tech Super Giants Maintain Standard Oil Sized Monopolies*, IPWATCHDOG (Feb. 28, 2018, 7:15 AM), [<https://perma.cc/V76C-7MC9>]. Apple, in comparison, earned \$94.68 billion in net income in 2021. Federica Laricchia, *Apple's Net Income in the Company's Fiscal Years from 2005 to 2023*, STATISTA (Nov. 6, 2023), [<https://perma.cc/G37L-MGMY>]. Similarly, Amazon took in over \$21.4 billion in net income in 2020, and Facebook earned over \$28.1 billion in net sales that year. *Amazon's*,



Over their years of growth since the explosion of home computing technologies, the widespread adoption of the internet, and the advent of web-based applications, including digital commerce, many of these companies enjoyed high levels of approval and satisfaction from customers, many of whom saw this new breed of firm in favorable comparison to the image of the avaricious and remorseless corporations of the nineteenth and early twentieth centuries.<sup>188</sup> This overall anti-corporate image was fostered in large part by the peculiar culture that had emerged in and around Silicon Valley, which rejected the traditional hierarchies of establishment corporate and political thinking, blending with the countercultural movement that had been brewing for years in postwar California.<sup>189</sup> After a period of distrust, a small cohort within the counterculture movement began to see the possibilities digital technologies presented to challenge existing power structures, where computers could be a useful tool to spread liberation rather than as an Orwellian oppressor.<sup>190</sup> As some of these technology futurists began to start companies, they brought with them their own brand of optimism that sometimes became integrated into their corporate values and more often showed up in their external marketing.<sup>191</sup>

Over time, however, it has become clear that technology firms are not all that different from their predecessors, irrespective of whatever initial countercultural leanings they may have had.<sup>192</sup> Quite rapidly, technology companies that were once

---

*Facebook's, Google's Q4 Earnings*, VESTED, [https://perma.cc/CYQ2-ZEKK] (last visited Nov. 16, 2023).

188. This view was often shared, at least initially, by some of the founders of these very companies. Steve Jobs, for example, was famous for his Buddhist influences and his vision of “insanely great” computers for the masses (although not as many of the masses could afford his “insanely great” products as he might have preferred). *See, e.g.*, WALTER ISAACSON, *STEVE JOBS* 35, 110 (2011). Google’s founders also adopted similarly anti-corporate public stances, incorporating the rather difficult-to-define-and-enforce motto “don’t be evil” in the company’s statement of values in their 2004 IPO prospectus. Google Inc., Prospectus (Form 424B4), at 32 (Aug. 18, 2004), [https://perma.cc/MF9E-4WSK].

189. *See, e.g.*, Mike Colagrossi, *How the ‘60s Counterculture Created Silicon Valley*, BIG THINK (Jan. 29, 2019), [https://perma.cc/7N2N-7BL8].

190. *See* ISAACSON, *supra* note 188, at 162.

191. *See id.* at 162-64.

192. Steve Jobs, for example, despite his embrace of Buddhist teachings and public pronouncements of a desire to bring computing to the masses, was known to be quite ruthless, even vicious, when it came to business decisions. *See* ISAACSON, *supra* note 188, at 35, 107.

underdog startups that many assumed would end in bankruptcy have grown to establish significant positions of market dominance, not just in the United States, but also globally.<sup>193</sup> This aggressive growth was achieved in large part due to the Chicago/Bork antitrust policy dominant since the Reagan Administration, where short-term interests like consumer prices were the sole tests for enforcement.<sup>194</sup> Because the funding model for technology companies that had developed since the 1990s rewarded new companies for customer growth, even when those companies lost money in pursuit of those customers, often for many years, firms like Amazon and Facebook were able to expand their respective empires without any significant interference from antitrust enforcement.<sup>195</sup>

The results we have seen from the emergence of large technology companies resonate with the original concerns behind antitrust policy, where a concentration of wealth and power through monopoly and oligopoly can bring with it a number of societal harms, even when the most apparent short-term effects seem to be beneficial to consumers.<sup>196</sup> Some of these harms align with traditional market competition concerns. For example, Amazon has long adopted an aggressive approach to competition, applying a long-term philosophy that undercuts competitors by maintaining very small profit margins and leveraging the scale of supporting technologies and businesses that it has been building and continues to build.<sup>197</sup> This approach has worked. By sacrificing short-term profit for years, Amazon has been able to force out competition and dominate multiple industries through predatory pricing schemes.<sup>198</sup>

---

Amazon, the bookselling startup that everyone seemed to love, was internally very aggressive and predatory toward their competition. David Streitfeld, *A New Book Portrays Amazon as Bully*, N.Y. TIMES (Oct. 22, 2013, 6:00 AM), [<https://perma.cc/DJ27-P4PJ>].

193. See Jason Feifer, *6 Giant Companies That Nearly Flopped*, ENTREPRENEUR (Dec. 1, 2020), [<https://perma.cc/G4DT-E7DN>].

194. See, e.g., Zoffer, *supra* note 185, at 308-11.

195. See Lina M. Khan, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710, 747-53 (2017).

196. See, e.g., Khan, *supra* note 186, at 985-89.

197. See Khan, *supra* note 195, at 710, 747.

198. See *id.* at 747-53.

Similarly, Facebook also adopted the growth-over-profit model, to the apparent satisfaction of its funders.<sup>199</sup> And, like Amazon, Facebook used its size and position to aggressively force competitors out of the market, often using predatory techniques.<sup>200</sup> But Facebook's dominance in social media and adjacent markets created other problems, ones which would likely be ignored as irrelevant by Chicago/Bork antitrust theory, but were just the sort of harms that were being pointed out by scholars advocating for a return to antitrust's original purposes.<sup>201</sup> While Facebook was remorseless when it came to extinguishing its competition, many of the most disturbing effects of its market dominance emerged directly from its core business model, the collection, analysis, and use of user data.<sup>202</sup> Facebook does not charge its customers to use its services, instead getting its revenue from the information its users provide, both explicitly and implicitly, both on Facebook as well as on other sites that employ Facebook technology to aid in this data collection process.<sup>203</sup> This information was carefully analyzed and packaged by Facebook for sale to advertisers who could use this valuable behavioral data to pinpoint potential customers and tailor messages based on an individual's revealed preferences, made available by Facebook at a level of detail never before seen.<sup>204</sup>

Facebook's business model, therefore, depended on attracting as many customers to its product as possible and keeping them on its site for as long as possible.<sup>205</sup> Facebook achieved this first goal by using a "buy-or-bury" approach to

---

199. See Dina Srinivasan, *The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumer's Preference for Privacy*, 16 BERKELEY BUS. L.J. 39, 54 (2019).

200. New York State Attorney General Letitia James observed in a public statement announcing their lawsuit against Facebook, "Instead of competing on the merits, Facebook used its power to suppress competition so it could take advantage of users and make billions by converting personal data into a cash cow." *Attorney General James Leads Multistate Lawsuit Seeking to End Facebook's Illegal Monopoly*, N.Y. STATE ATT'Y GEN. (Dec. 9, 2020), [<https://perma.cc/S3KP-K4YG>].

201. See Srinivasan, *supra* note 199, at 40.

202. See *id.* at 43-44.

203. See *id.*

204. See *id.* at 41-43.

205. See SHEERA FRENKEL & CECILIA KANG, AN UGLY TRUTH: INSIDE FACEBOOK'S BATTLE FOR DOMINATION 28 (2021).

eliminating their competition.<sup>206</sup> Achieving the second goal was made possible through the use of the same raw materials—user data—it was packaging and reselling to advertisers. By analyzing an individual customer's preferences through the data they generated, Facebook developed code that would maximize user engagement by manipulating the topics and stories that a person would most likely be interested in, thus keeping the user on Facebook for longer periods, generating even more data, and feeding this cyclical process.<sup>207</sup>

As a dominant social media platform, Facebook's manipulative algorithmic approach to their customers—numbering around three billion in 2021<sup>208</sup>—brought with it some of the corrosive effects that concerned the original antitrust law drafters. Two of these problems became apparent during the runup to the 2016 U.S. presidential election and the years that followed. First, it was revealed that political operatives, some acting on behalf of the Russian government, were able to manipulate the Facebook advertising network and its user engagement algorithms to spread misinformation and propaganda on a large scale while still being able to individually tailor these messages to increase their resonance with individual users.<sup>209</sup> Second, right-wing activists were spreading false or misleading “news” via Facebook's site advocating violence, sexism, and racism, again using Facebook's user engagement coding to tailor these messages to particular users.<sup>210</sup> Further, it was later revealed that Facebook executives were aware of these and many other related issues, yet either failed to act or quietly provided only minimal changes to their system, as the increased user engagement and advertising revenue associated with these problems was good for Facebook's bottom line.<sup>211</sup>

Facebook is not the only technology firm that relies on the collection of user data as a kind of raw material from which to

---

206. *Id.* at 2.

207. *See id.* at 58-63.

208. *See* Meta Platforms, Inc., Meta Reports Fourth Quarter and Full Year 2021 Results, at 1 (Feb. 2, 2022), [<https://perma.cc/PB96-DQ3V>].

209. *See* FRENKEL & KANG, *supra* note 205, at 96-99, 106.

210. *See id.* at 106-109, 122, 138.

211. *See* Srinivasan, *supra* note 199, at 69-71.

generate revenue.<sup>212</sup> In fact, large portions of the web-based ecosystem were built and still rely upon this business model.<sup>213</sup> The negative effects (or externalities) of this model, which Shoshanna Zuboff has called “surveillance capitalism,” come from the market dominance of the firms involved and the relative invisibility of its mechanisms to most users of these systems.<sup>214</sup> Just as most people are not able to judge the efficacy and safety of, say, pharmaceuticals or commercial aircraft, most users of digital technologies are unable to assess the internals of those technologies or understand the wider implications of their use.<sup>215</sup> Unlike pharmaceuticals and commercial air travel, however, both of which are highly regulated industries, consumer technology industries fall under relatively few regulatory restrictions.<sup>216</sup>

As more of the negative externalities associated with technology monopolies, monopsonies, and oligopolies have become more widely apparent, numerous calls for additional technology regulation have been raised worldwide.<sup>217</sup> While some nations have established technology regulatory regimes (to varying degrees of success), the United States has been slower to adopt additional regulation in this area due in large part to legal and ideological restrictions.<sup>218</sup> The past few years have seen multiple hearings before Congress to address technology regulation, sometimes revealing unusual symmetries across party lines where lawmakers agree that large technology firms must be somehow regulated, but disagree significantly as to the reasons why this should be the case or which incentives matter in the process, with little to no actual legislative actions coming from any of it.<sup>219</sup>

But antitrust scholars have been pointing out a path to Big Tech regulation that would not require the creation of new law—

---

212. See Zuboff, *supra* note 144, at 180-82; Cohen, *supra* note 138, at 1914-16.

213. See Zuboff, *supra* note 144, at 180-82.

214. *Id.* at 178-79.

215. *Id.* at 180-82.

216. *Id.* at 209.

217. See *supra* text accompanying notes 175-84.

218. See James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L. J. 1151, 1153-60 (2004).

219. See, e.g., Cecilia Kang, *Congress, Far from 'A Series of Tubes,' Is Still Nowhere near Reining in Big Tech*, N.Y. TIMES (Dec. 11, 2021), [<https://perma.cc/BDD6-DPUD>].

a highly unlikely prospect in today's fractured political climate—but could instead be achieved through a return to antitrust policy's original goals. Where current doctrine has embraced efficiency and consumer prices as its sole antitrust lodestars, these scholars argue that in order to rein in the abuses and other negative effects of technology monopolies, the doctrine must shift back to traditional antitrust trigger points, such as predatory pricing and anticompetitive vertical integration, two areas that have been largely ignored since the Chicago/Bork antitrust counterrevolution, to the great benefit of technology giants like Amazon and Facebook.<sup>220</sup>

Technology reform advocates have seen the greater benefits of such an application of antitrust law to large technology firms.<sup>221</sup> Perhaps unsurprisingly, given the heavy reliance of the technology industry on the collection, analysis, and use of user data, this list of possible areas of regulatory reform includes privacy.<sup>222</sup> While information privacy laws exist in the United States, they are anything but comprehensive, often narrowly tailored to address a particular industry or type of data use, difficult to enforce or seek remedies, and are unevenly distributed across federal and state government jurisdictions.<sup>223</sup> Some privacy regulation is accomplished through state and federal regulatory bodies, such as the Federal Trade Commission (“FTC”), but administrative agencies such as the FTC tend to be understaffed and underfunded, so they are forced to pick their information privacy battles carefully.

Applying antitrust policy to achieve information privacy goals is therefore an attractive possibility, especially when such enforcement actions could potentially provide solutions to the other negative externalities presented by large technology firms. Because monopolies, monopsonies, and oligopolies often exercise disproportionate levels of power over their customers,

---

220. See Srinivasan, *supra* note 199, at 99-101.

221. *Id.*

222. See, e.g., Frank Pasquale, *Privacy Antitrust, and Power*, 20 GEO. MASON L. REV. 1009, 1009-11, 1022 (2013); Garrett Glasgow & Chris Stomberg, *Consumer Welfare and Privacy in Antitrust Cases—An Economic Perspective*, ANTITRUST, Fall 2020, at 46, 46; Khan & Vaheesan, *supra* note 179, at 291-94; Khan, *supra* note 195, at 802-05.

223. See Citron & Solove, *supra* note 96, at 796-99.

they face few pressures to improve aspects of their product that users may be asking for and are especially disinclined to make any changes involving user privacy that may negatively impact their ability to generate revenue from the data that users generate on their platforms.<sup>224</sup> Antitrust/privacy theory asserts, therefore, that among the many harms that stem from technology monopoly, information privacy harms are especially pernicious, as the mechanisms for abuse are largely hidden from users within inscrutable technology platforms and networks, and their establishment has flown under antitrust enforcement radar for decades.<sup>225</sup>

But is antitrust law an appropriate tool for addressing information privacy harm? Large technology firms certainly have engaged in behavior that, due in part to their scale and dominance, have resulted in privacy abuses at many levels, but can competition policy provide the kinds of incentives necessary to address these harms? Further, does treating information privacy as a negative externality resulting from market concentration and insufficient competition address privacy's full personal, political, and societal value? Will a reliance on competition between firms protect privacy as well as privacy regulation that stands on its own? Are there subtleties in technology markets that might make antitrust enforcement result in exacerbations of privacy harm?

### C. Applying Antitrust to Privacy

As the interest in antitrust law as applied to Big Tech has expanded, scholars and advocates have explored the possibility that a renewed regulation of competition might provide a useful—if perhaps unexpected—method of privacy protection. Since much of U.S. regulation of information privacy to this point has been a variation on the theme of *caveat emptor*, where the consumer is expected to bear a significant part of the privacy burden through notice-and-consent and opt-out mechanisms, some scholars began to explore the links between existing antitrust and privacy law, especially with respect to their

---

224. See Khan, *supra* note 195, at 257-63.

225. See *id.* at 291-93; *supra* note 90 and accompanying text.

respective shortcomings, seeing some common foundations as well as a few key differences.<sup>226</sup> Further, as technology firms got increasingly larger, with corresponding growth in computing power and access to personal data, it was perhaps natural for questions to arise regarding the value of data in a technologically rooted economy where information has replaced money as the way we pay for many products and services.<sup>227</sup>

For example, Frank Pasquale observed that since “[t]he primary purpose of privacy law (as applied to corporations) and antitrust law is to deter and punish unfair, deceptive, or harmful behavior. Improving market processes” through antitrust regulation may be a way to begin to level the uneven privacy playing field.<sup>228</sup> Pasquale notes that, despite firms’ claims to the contrary, competition has proven a largely ineffective means of protecting privacy since most of said competition addresses only short-term consumer privacy concerns, not accounting for the complexities of the data marketplace that are beyond most consumers’ abilities or interest, and what passes for consumer privacy preferences are actually just responses to finely-tuned manipulations by Big Tech companies.<sup>229</sup> Because all of this adds up to an enormous imbalance of power between technology firms and their customers, Pasquale argues that expanding the existing notions of anticompetitive behavior could be a means of “bring[ing] antitrust enforcement into the twenty-first century” in order to “ensure that the companies that occupy such commanding heights in the Internet ecosystem do not use their dominant positions to exclude and discourage firms operating in adjacent fields” and thus leave consumers with no real choices with respect to their privacy.<sup>230</sup>

---

226. See, e.g., Pasquale, *supra* note 222, at 1009-11; Julie Brill, *The Intersection of Consumer Protection and Competition in the New World of Privacy*, 7 COMPETITION POL’Y INT’L 7, 7-8 (2011); Robert H. Lande, *The Microsoft-Yahoo Merger: Yes, Privacy Is an Antitrust Concern*, FTC: WATCH, Feb. 25, 2008, at 1-2; Glasgow & Stomberg, *supra* note 222, at 46; Erika M. Douglas, *Monopolization Remedies and Data Privacy*, 24 VA. J.L. & TECH. 1 (2020); Erika M. Douglas, *The New Antitrust/Data Privacy Law Interface*, 130 YALE L.J. F. 647 (2021); James C. Cooper, *Privacy and Antitrust: Underpants Gnomes, The First Amendment, and Subjectivity*, 20 GEO MASON L. REV. 1129 (2013).

227. See Elvy, *supra* note 85, at 1371-754.

228. See Pasquale, *supra* note 222, at 1011.

229. *Id.* at 1013-15.

230. *Id.* at 1021-22.



Following similar lines of thought, Gregory Day and Abbey Stemler noted the lack of competitive incentives for companies operating large platforms, which allowed these firms to ignore calls for increased privacy protections while externalizing the costs associated with reduced privacy to society.<sup>231</sup> The larger the platform a company controls, the greater their access to data as well their ability to use those data to manipulate user behavior, resulting in significant economic benefits while at the same time forcing individuals and governments to bear the costs of protecting privacy from breaches and abuse of those same data.<sup>232</sup> Day and Stemler assert that these under-competitive or uncompetitive conditions have grown under the current antitrust policy due to the fact that these platforms are not using retail prices for their services in the conventional sense, relying instead on a “free” model that monetizes the consumer data collected through these services.<sup>233</sup> Existing antitrust jurisprudence fails to realize that privacy should also be considered a quality metric and that the paying-with-data model has largely shielded these enormous platforms from antitrust scrutiny.<sup>234</sup> Day and Stemler argue that modern antitrust policy “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.”<sup>235</sup>

FTC Commissioner Julie Brill approached the topic of privacy and antitrust as part of the natural balance of two core missions of the FTC—consumer protection and competition law.<sup>236</sup> As Brill notes, privacy and antitrust problems can both be seen as market failures but with potentially different levels of impact on the consumer.<sup>237</sup> After accounting for the tensions between consumer protection and competition law that can often

---

231. See Gregory Day & Abbey Stemler, *Infracompetitive Privacy*, 105 IOWA L. REV. 61, 63-65 (2019).

232. *Id.* at 64.

233. *Id.* at 63-66.

234. *Id.* at 65-66.

235. *Id.* at 66.

236. See Brill, *supra* note 226, at 8.

237. *Id.* at 8-9.

occur, Brill goes on to articulate a method through which privacy protection can be served by antitrust law through the FTC's 2010 action against Intel that combined consumer protection and competition law.<sup>238</sup> If privacy protection is a key component of the FTC's consumer protection mission, the Intel case model could be applied more broadly to encourage firms "to compete based on how they collect, use, store, and dispose of consumers' information—that is, to engage in competition based on privacy."<sup>239</sup> This model, according to Brill, would not be a barrier to market entry by small players, but would rather be a benefit to new entrants by giving them a road map for building "business models that address privacy concerns from the outset, rather than as an afterthought," which may even be realized as an advantage over existing players who may have to redesign portions of their business.<sup>240</sup>

This fused approach to applying and expanding competition theory to account for privacy concerns has found resonance among some scholars and practitioners. Garrett Glasgow and Chris Stomberg assert that "[t]he most obvious type of privacy-related harm to consumers that arises from a lack of competition is the 'forced' sharing of personal information."<sup>241</sup> Robert H. Lande argues that "[a]ntitrust is actually about consumer choice, and price is only one type of choice," with privacy protection being yet another area of consumer choice.<sup>242</sup> If antitrust law can ensure competitive markets, "any information-heavy firm that does not respect consumers' privacy rights will pay a penalty."<sup>243</sup>

At first glance, fusionist approaches between antitrust and privacy protection make some sense. After all, if many of the technological products and services we use today are no longer strictly tied to consumer pricing as a competitive lever but are instead increasingly dependent upon user data as their new lifeblood, should we not consider the tools that may already exist within the antitrust kit to better apply market competition to

---

238. *Id.* at 14-15.

239. *Id.* at 18.

240. *Id.* at 18-19.

241. Glasgow & Stomberg, *supra* note 222, at 46.

242. *See* Lande, *supra* note 226, at 1.

243. *Id.*

correct for data use imbalances? Ought we not use naturally occurring market mechanisms—guided by judicious application of antitrust policy—to shape privacy protections in ways that U.S. law has failed to do so far? I will consider these questions in the following Part, paying close attention not only to whether antitrust law *can* be applied to protect privacy but also whether it *should*.

### III. ANTITRUST ALONE CANNOT PROTECT PRIVACY

Despite their potential for reigning in some of the abusive practices and negative externalities associated with the concentration of market power in digital technology, antitrust law and policy is an inappropriate tool for addressing privacy harm for three reasons. First, privacy's value is intrinsically diminished by its commodification, and an antitrust approach to addressing information privacy harm depends, at least in part, on the acceptance of user data solely as a commodity to be bought and sold. Second, a dependence upon competition to provide sufficient incentive for companies to protect information privacy is a weak foundation for information privacy protection, especially given the current dependence the technology industry has on the collection and use of user data. Third, certain aspects of the technology industry may mean that the application of antitrust policy to privacy can make the problem even worse than it is.

This is not to say that antitrust policy does not have an important role to play in the regulation of technology industries, but the protection of information privacy should be based squarely on law and policy that stands on its own merits, which would allow for comprehensive privacy protection while also being available for application in tandem with other technology regulation, including antitrust. Therefore, I argue that antitrust is not an appropriate tool for privacy protection for three reasons. First, the use of antitrust law to regulate privacy requires the subjection of privacy to market norms and directly accepts the commodification of privacy. For the reasons articulated in Part I, privacy's commodification leads to a noxious market and

therefore should not be required as part of any legal regime meant to protect privacy. Second, even if we accept the use of market mechanisms to regulate privacy, current U.S. privacy law has demonstrated that market norms, which may be applied elsewhere with some success, are not well-suited to factors that are unique to information privacy issues, and place unreasonable burdens upon individual users who are most often the least well-positioned to properly assess, address, or remediate those privacy burdens. Third, because of the nature of information privacy and the relationships between its various players, an antitrust approach to privacy regulation may in fact serve to complicate the landscape and exacerbate privacy harms.

Scholars have proposed other middle ways of affording consumer protections for sensitive public goods such as privacy by addressing privacy-related market externalities through a “public priority principle.”<sup>244</sup> Such approaches agree that many of our antitrust tools either do not properly address the concerns surrounding Satz’s noxious markets or serve to further the commodification of those goods. But these approaches are wary of dismissing economic thought entirely. To let the pendulum swing too far away from the economics surrounding topics like privacy runs the risk of missing some very good arguments that could help bolster privacy interests.<sup>245</sup> I do not disagree with such approaches and find them to be complementary to the arguments in this Article. Much depends on how a comprehensive approach to privacy regulation is implemented and how well we take into account what is lost by giving too much sway to market-based thinking.

## A. We Should Not Accept Privacy’s Commodification

### 1. *Extra-Market Norms and Privacy*

The current neoliberal form of market fundamentalism is based on the conviction that markets, coupled with certain government activities that establish, support, or bolster these

---

244. See, e.g., Rory Van Loo, *The Public Stakes of Consumer Law: The Environment, the Economy, Health, Disinformation, and Beyond*, 107 MINN. L. REV. 2039, 2047 (2023).

245. See Rory Van Loo, *Privacy Pretexts*, 108 CORNELL L. REV. 1, 8 (2022).

markets, are the best means for obtaining optimal levels of liberty and prosperity.<sup>246</sup> But there can be some items or facets of life for which their subjection to market values is seen as irresponsible, debasing, or corrosive, either to the items themselves or as a potential source of collateral damage to other, possibly larger, concerns.<sup>247</sup> The commodification of areas such as medicine, public health, and public safety—exceptional areas argued as subject to non-market norms—has yielded multiple examples where marketplace norms have resulted in moral harms.<sup>248</sup> Attempts to somehow reestablish these non-market norms by using the legal frameworks associated with antitrust may offer some solutions, but because it is a market-preserving regime, antitrust law's use requires an implicit acceptance of the commodification of the items in question, and it therefore undermines the foundational moral premise of the item's exceptionalism. Rather, the preservation of extra-market norms requires law that stands on its own, outside the marketplace. Information privacy falls within this zone of extra-market norms as well.<sup>249</sup>

As I illustrated in Part I, the commodification of privacy—the collecting, buying, and selling of personal information—creates what Debra Satz called a noxious market.<sup>250</sup> A privacy market is one in which consumer vulnerability is combined with weak consumer information positions to yield harm not only to individuals but to society as well.<sup>251</sup> The character of the privacy marketplace has been demonstrated time and again as one of explosive growth and significant profit, based in large part on a foundation of information imbalance, black box and sometimes deceptive design principles, and unexpected (and unwelcome) surprises that so often accompany our default *laissez-faire* approach to new and unfamiliar markets and commodities we do not yet fully understand.<sup>252</sup>

---

246. See *supra* Section I.A.

247. See *supra* Section I.B.

248. See *supra* Section I.B.

249. See *supra* Part I.

250. See *supra* Part I.

251. See *supra* Section I.C.

252. See generally ZUBOFF, *supra* note 138; HARTZOG, *supra* note 100.

Privacy is an essential component of our everyday lives, from our inner thoughts and internal framings to our social interactions with close family members, friends, and companions; even among our more or less attenuated relationships with more remote or abstract entities and institutions, privacy is critical to the constant shaping and reshaping of our selves.<sup>253</sup> The details of this complex and multilayered process differ for everyone, but irrespective of individual experience, the need for a certain amount of free space in which to conduct these activities is necessary, and privacy is key to protecting that space.

Who we are depends first on our own ability to determine our identities, starting with the expression, to ourselves, of our own feelings, desires, values, and purpose, often experimentally, and frequently changing as our life experiences change. The protection of privacy is the protection of these facets of self, making it one of those relatively few items we tend to set aside as subject to extra-market norms.<sup>254</sup> Coming up with a reasonable privacy policy is difficult and further complicated because reasonable people can disagree as to the details of such policies; however, to accept the continued commodification of privacy is to foreclose much of that conversation before it even begins.

The reason information is so valuable is that it is an important source of power in the Information Age. National governments with more information about their citizens are better able to govern and provide for short-term and long-term needs, but they are also better able to closely monitor the activities of those citizens, control public messaging, and quash dissent.<sup>255</sup> Law enforcement agencies with more information about their jurisdictions can better ensure public safety, but they are also better at targeting disfavored populations, proactively and precisely chilling undesired First Amendment activity, and building compromising dossiers on political enemies. Companies with more information about customers and potential customers can better tailor their products and services to meet those customers' needs, but they are also better able to manipulate

---

253. *See supra* Section I.A.

254. *See supra* Section I.B.

255. *See, e.g., Khan, supra* note 186, at 1016-18, 1057-58, 1063-64.

individuals into additional purchases, unfairly adjust product pricing, or sell their data to third parties (including the aforementioned government entities). Technology platforms with more information about their users can use that information to provide greater utility and convenience to those users, but they are also better equipped to manipulate customer use patterns, create carefully curated information bubbles to spread misinformation and disinformation, and provide conduits to third parties to leverage users' interests, hopes, and fears to sell anything from pop culture to political parties.<sup>256</sup> The common denominator that information provides all of these examples is power, and the individual users have the least amount of it. The subjection of an extra-market item to market norms and values—privacy's commodification—is what has created both the informational power source as well as the severe imbalance of that power.

Courts applying antitrust specifically acknowledge the necessity of an item's commodification, where concerns over the application of market norms to areas arguably subject to extra-market norms are largely irrelevant.<sup>257</sup> While it is true that a fundamental goal of antitrust law and policy is serving the general welfare, that goal is limited by definition to questions of a commodity's offering or sale within the market and is therefore not concerned with questions as to whether that item should be bought and sold as a commodity in the first place.<sup>258</sup> This is not to say that antitrust policy can never provide remedies to public harms relating to commercialized items from extra-market moral domains, but the better solution in these instances is the application of the law—possibly in tandem with antitrust, though

---

256. See, e.g., FRENKEL & KANG, *supra* note 205, at 234-35.

257. See, e.g., *Hackett v. Metro. Gen. Hosp.*, 422 So. 2d 986, 987-88 (Fla. Dist. Ct. App. 1982) (considering the challenge of the application of state antitrust law to the practice of medicine, the court observed that the applicable state law defined "trade or commerce to include any economic activity of any type whatsoever involving any commodity or service whatsoever," holding that the "language of the statute is clearly broad enough to encompass a restraint upon the practice of medicine" (internal quotations omitted)).

258. See HOVENKAMP, *supra* note 159, at 229-30.

not dependent upon it—that stands on its own without a reliance on market mechanisms in its enforcement.<sup>259</sup>

But there remains the argument that the commodification of sensitive or exceptional areas yields optimal, if imperfect, solutions and that any extraneous regulatory meddling outside of those few laws necessary to ensure market fairness is at best unwise, and at worst partisan overconcern for those who may not fare well in that market.<sup>260</sup> An often unspoken part of this argument holds that there will always be winners and losers in life, with or without markets, but market mechanics, perhaps assisted here and there by laws designed to protect those markets, provide the most optimal, efficient, and fair venue to finding those winners and losers.<sup>261</sup> This argument is, of course, corollary to the question of whether markets have limits, a question relevant to this Article's own thesis. If, for example, one is not terribly concerned about the "explicit, income-correlated disparities" a commoditized health insurance marketplace generates with respect to access to quality medical care, a similar argument regarding the loss of privacy protections in a similarly commoditized information marketplace may not be convincing.<sup>262</sup> If, however, the significant privacy harms, at the individual and societal levels, that stem from user data commodification and privacy's subjection to market values are something one considers worth avoiding or ameliorating, the

---

259. See *supra* Section II.B; Clark C. Havighurst, *Trafficking in Human Blood: Timmuss (1970) and Products Liability*, L. & CONTEMP. PROBS., Summer 2009, at 1, 13-14 (arguing that, in the case of the collection and distribution of human blood, "treat[ing] blood as an ordinary commodity and its purveyors as ordinary competitors" would have saved lives).

260. See, e.g., Clark C. Havighurst & Barak D. Richman, *Distributive Injustice(s) in American Health Care*, L. & CONTEMP. PROBS., Autumn 2006, at 7, 79-81 (arguing that "managed competition" of insurance markets is a "common ground" solution, that may be "highly threatening to special interests," but comports with "American values" of market fundamentalism) ("It is highly possible, of course, that influential members of the body politic will never be permanently comfortable in the presence of explicit, income-correlated disparities in insured individuals' legal entitlements to medical care—even if those inequalities result from reasonable choices by consumers, spending not just their own limited resources but also whatever earmarked subsidies democratic legislatures choose to provide. For some observers (apparently), the symbolic significance of any such disparities will always trump efficiency and welfare concerns, overriding respect not only for private choices but also for government's legitimately established budgetary priorities.").

261. See Grewal, *supra* note 181, at 664-65.

262. See Havighurst & Richman, *supra* note 260, at 79-81.



creation of appropriate privacy law and policy that can stand on its own without depending upon market mechanisms will be compelling.

## *2. The Privacy Marketplace Is Fundamentally Flawed*

A comparative look back at the developments in antitrust law and privacy law provides additional evidence that their goals are not truly complementary. As Erika Douglas has pointed out, privacy is negatively correlated with the increased competition in our heavily information-based economy, where the availability of information is the basis for market viability.<sup>263</sup> That is, our neoliberal economic system is built around the gathering and analysis of data in order to both predict risk as well as minimize uncertainty, within which the search for personal information is closely aligned with the search for profit, and thus any move to restrict access to subsets of that information reduces the available raw materials from which new and existing companies can grow and compete.<sup>264</sup>

Further, as the scale and complexity of the information marketplace has grown, individual users' ability to control the collection, distribution, and use of their information in any meaningful way has been reduced in ways that make increased competition an unlikely source of privacy protection. Because our information economy has been built around the ubiquitous collection of user data as its raw materials, vast networks have been established in the pursuit of this resource, much of it invisible to the average person. For example, as internet-based and web-based technologies advanced through the 1990s, so did companies' levels of sophistication regarding the collection of user information.<sup>265</sup> Not only were the technologies for collecting user information becoming more prolific and efficient, while at the same time less visible to the individual user of technologies, but the analysis and packaging of collected data has arguably advanced even further through the rapid development and expanded use of machine learning and similar data analysis

---

263. See Douglas, *supra* note 226, at 656-58.

264. See *supra* Section II.B.

265. See *supra* Sections II.A, II.B.

techniques.<sup>266</sup> By applying these statistical analytic techniques to the enormous data sets generated by years of information collection, private companies (and many governments, often through the assistance of those private companies) were able to generate useful, if sometimes incorrect, inferences about the sources behind the user data, even when the data is “anonymous” or otherwise missing key parts, like putting together a puzzle in order to recreate the missing pieces based on the context provided by the pieces around the gaps.<sup>267</sup>

These advanced data analysis techniques do not require or depend upon the active participation of or explicit permission from individual users but instead trawl the vast seas of information invisibly generated through our everyday participation in any activity facilitated through connected technologies, much of which is quite outside an individual's ability to monitor or control.<sup>268</sup> These systems involve the buying, selling, and aggregation of data at scales unimaginable prior to the widespread availability of machine learning models and high-performance computing, an industry made quite lucrative due to the value of its end product—the automated behavioral analysis of customers and potential customers.<sup>269</sup> This

---

266. See *supra* Sections II.A, II.B.

267. See, e.g., Alicia Solow-Niederman, *Information Privacy and the Inference Economy*, 117 NW. U. L. REV. 357 (2022). A well-known early and relatively unsophisticated example of this phenomenon can be found in the 2002 story of how the Target Corporation used information collected about customer purchases to infer that a particular person was likely pregnant, information that could be used to tailor future advertisements and marketing products, thus increasing the possibility of increased sales. Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES MAG. (Feb. 16, 2012), [<https://perma.cc/DE56-7FUA>]. Governments have also seen the potential benefits of these techniques in support of national security or law enforcement missions. For example, Clearview AI, a small company that devised a data analysis system that would automatically scan the billions of photographs posted across the web, many of them taken without any explicit permission from the subjects, to develop a facial recognition database for law enforcement and national security agencies to help identify suspects in their investigations. Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Jan. 18, 2020), [<https://perma.cc/AY7P-7K8G>].

268. See, e.g., Solow-Niederman, *supra* note 267, at 381-82.

269. This is the general impetus driving “surveillance capitalism,” a system of organizational techniques “that operates by ‘unilaterally claim[ing] human experience as free raw material for translation into behavioral data,’ and processing that data to ‘anticipate what you will do now, soon, and later.’” Amy Kapczynski, *The Law of Informational Capitalism*, 129 YALE L.J. 1460, 1464 (2020) (alteration in original) (reviewing ZUBOFF, *supra* note 138 and COHEN, *supra* note 113).

system of surveillance capitalism derives directly from the natural evolution of the liberal self and market fundamentalism when technological advances in information collection are introduced without restriction and leave individual users as passive participants, whether they know it or not and whether they want it or not.<sup>270</sup> Protecting market competition within this system through antitrust law may help dislodge monopolistic players, but it will not protect privacy on its own. If an individual wishes to avoid participation in this system, they must effectively withdraw from modern life, an unacceptable proposition for most, and even then, antitrust law would be unable to provide the means to control their exposure. Only privacy laws that stand on their own can accomplish this.

Finally, it is difficult to see how increased competition will necessarily lead to increased protections for information privacy. While it is true that, left unchallenged, large technology companies will have little incentive to introduce or increase privacy protections, even when firms compete on privacy, users are often at a significant information deficit as to exactly what particular privacy protections mean in real terms. While a concentration of technology firms controlling a majority of consumer data is certainly a problem for privacy, increasing competition through antitrust or other actions will not necessarily lead to increased pressures to protect user privacy, as user data would still remain the driving force behind internet business models. Only privacy laws that directly address the incumbent data-fueled technology model will provide the kinds of protections necessary.

But before we dismiss competition as a tool to protect privacy, let us consider a thought experiment wherein a mixed commodification model was adopted. That is, what if we regulated privacy in a manner that sought to protect the individual and societal norms discussed in Part I while relying on some market mechanisms, like competition, to shore up those protections? We could, for example, take a page from the regulation of automobile safety in the United States, where federal rules were designed to establish minimum safety

---

270. See, e.g., Solow-Niederman, *supra* note 267, at 362-63.

standards, but manufacturers were free to compete with one another in ways that surpassed those baseline standards.<sup>271</sup> In this context, competition has driven increased consumer demand for automobile safety and even pushed automobile manufacturers to install passenger airbags ahead of regulatory deadlines.<sup>272</sup> Could such a hybrid model, using regulatory protections in combination with market-driven dynamics, be successfully applied in the context of information privacy?

Unfortunately, even a modified commodification model would be unlikely to resolve the issues raised by a noxious privacy market for four interrelated reasons. First, unlike the examples found in automobile and product safety regulation, much of what makes for sufficient privacy protections is unknowable to most consumers due to the black-box nature of software and connected devices.<sup>273</sup> Second, in addition to government regulators, a large, robust, and well-established network of automobile and product safety organizations has grown as cars became larger, faster, and more popular, providing independent research, analysis, and ratings systems designed to keep manufacturers honest and consumers well-informed.<sup>274</sup> An infrastructure with this level of influence and visibility does not (yet) exist in the privacy space, due in large part to opacity, complexity, and a lack of a cohesive theory of privacy harm.<sup>275</sup> Third, whereas automobile manufacturer claims regarding safety

---

271. See Dana P. Babb, *The Deployment of Car Manufacturers into a Sea of Product Liability? Recharacterizing Preemption as a Federal Regulatory Compliance Defense in Airbag Litigation*, 75 WASH. U. L.Q. 1677, 1704 (1997).

272. *Id.*

273. See *supra* Section I.B.

274. See generally Robert W. Hamilton, *The Role of Nongovernmental Standards in the Development of Mandatory Federal Standards Affecting Safety or Health*, 56 TEX. L. REV. 1329 (1978).

275. This is not to say that consumer privacy watchdog groups do not exist. In fact, there are a number of them working in various contexts, some overlapping. See *Privacy: Organizations*, PUBLIC VOICE, [<https://perma.cc/78PX-TLMW>] (last visited Nov. 17, 2023). These organizations do important work, but often do not have the ability to assess the collection, transmission, sale, and use of personal data, due mainly to the highly complex network of data sharing that companies have built as well as the sheer volume of data transactions that take place every second of every day. See James P. Nehf, *Incomparability and the Passive Virtues of Ad Hoc Privacy Policy*, 76 U. COLO. L. REV. 1, 20-22 (2005). Not only do automobile and consumer product safety organizations have far fewer data points to evaluate, but they are often better positioned to call attention to the safety flaws they identify, especially if physical harm may result from those flaws.

can be verified and communicated through the aforementioned network of safety organizations, no such equivalent network exists in the privacy space. Further, claims about information privacy are generally not fully assessable by the average consumer. Finally, even if all of these factors were sufficiently addressed, there is little agreement, especially within the United States, as to what baseline privacy protections actually look like, as evidenced in the ongoing debate over privacy harms.

### **B. The Privacy Protection Burden Should Not Rest Solely on the Individual**

In the United States, a consumer notice-and-consent model of privacy is the dominant paradigm when questions of privacy protection arise.<sup>276</sup> Yes, the thinking goes, there are privacy risks associated with data collection, but there are also potential benefits, and individual consumers should be allowed to choose where, when, and how their information is shared.<sup>277</sup> But a significant problem with that model lies in the opacity (to users) of data information collection systems and the incentives a notice-and-consent model presents to firms whose data collection is largely hidden behind that opacity, especially when those data are highly valuable to those firms. By itself, antitrust law is ill-equipped to deal with the strong potential for privacy abuses within such a system, as it is not meant to change the system itself. In fact, it is more likely that antitrust models would support or even further advance a privacy model that puts a disproportionate burden on the consumer.

The general choice-and-consent framework, pushing many consumer protection questions to the consumers themselves, is based on the liberal ideal self as a rational neoliberal subject.<sup>278</sup> But it is also recognized that we are not perfectly rational as individuals and often make decisions based on poor or incorrect information or emotional bases. Proponents of the choice-and-consent model often include with it some degree of “libertarian paternalism,” which provides for the possibility of some “light

---

276. See *supra* Section I.B.1.

277. See Solove, *supra* note 99, at 1880-81.

278. See *id.* at 1883.

touch” public or private regulation while, at the same time, respecting an individual’s freedom of choice as a neoliberal subject.<sup>279</sup> That is, because we are imperfect decision makers, some amount of “nudging” is sometimes appropriate to help individuals make the right decision as a consumer, and is preferable to more direct means of regulation, which are generally seen as inefficient and intrusive to market values.<sup>280</sup> Supporters of nudging thus assert that where a government-based paternalism erodes an individual’s freedom of choice, libertarian paternalism preserves that freedom while protecting consumers from the most egregious of outcomes.

The popularity of the concept of nudging lends itself well to the American form of market-oriented thought, a philosophy that has been closely intertwined with American political, economic, and cultural thought since its earliest days.<sup>281</sup> This concept, based on traditional liberal ideals of a limited state, respect for the individual, and a presupposition of rational choices by a self-interested and largely self-disciplined citizenry, has further developed into a neoliberal form that encourages a larger government role in actively maintaining certain kinds of markets. This revision of traditional liberal *laissez-faire* ideals transformed the individual citizen into a neoliberal subject, someone who looks at every decision through a rational lens, whose “moral autonomy is measured by their capacity for ‘self-care’—the ability to provide for their own needs and service their own ambitions.”<sup>282</sup> Nudging, as described by Thaler and Sunstein, is an “aspect of the choice architecture that alters people’s behavior in a predictable way without forbidding any options or significantly changing their economic incentives,” thus fitting quite well within the neoliberal model of *homo economicus* as citizen, fully empowered and expected to see to their own

---

279. See Cass R. Sunstein & Richard H. Thaler, *Libertarian Paternalism Is Not an Oxymoron*, 70 U. CHI. L. REV. 1159, 1162 (2003).

280. *Id.* at 1168-70.

281. See generally CHARLES SELLERS, *THE MARKET REVOLUTION: JACKSONIAN AMERICA, 1815-1846* (1991).

282. WENDY BROWN, *EDGEWORK: CRITICAL ESSAYS ON KNOWLEDGE AND POLITICS* 42 (2005).

needs.<sup>283</sup> Nudging is just the sort of mild libertarian paternalism that no reasonable neoliberal subject should find objectionable.<sup>284</sup>

Given this background, nudging individuals to do a better job of protecting their own privacy seems like a winning strategy. Who else could do a better job of deciding when to share data and when not to? A significant element of the neoliberal subject model is the rejection of “one-size-fits-all” systems, the worst kind of paternalism, which robs individuals of their right to make their own choices based on their own needs and ambitions.<sup>285</sup> Indeed, this sort of approach, where each individual is allowed—nay, expected—to make her own privacy choices resonates quite well with the market-oriented economic and political landscape in the United States.<sup>286</sup>

But as we now know, the superficially attractive notion of privacy self-management is deeply flawed.<sup>287</sup> Neoliberal paternalism responds by pointing out that for those fallible individuals who err in their privacy choices, the market will be there to protect them.<sup>288</sup> Besides, adds the market fundamentalist, even if a few people trip up, the risks are small and are clearly outweighed by the benefits inherent in a system that provides people with “the ability to make decisions about their data at a relevant time and context.”<sup>289</sup> If people are allowed to exercise “appropriate control” over their personal information, and in order to do so are presented with “clear and simple choices,” they

---

283. RICHARD H. THALER & CASS R. SUNSTEIN, *NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS* 6 (2008).

284. *See* CASS R. SUNSTEIN, *WHY NUDGE? THE POLITICS OF LIBERTARIAN PATERNALISM* 1-4 (2014).

285. *See, e.g.*, Cass R. Sunstein, *Deciding by Default*, 162 U. PA. L. REV. 1, 8-9 (2013) (“If choice architects lack an accurate understanding of people’s situations, or if they have their own agendas, it may be best to insist on active choosing [by the individual].”).

286. *See* RICHARD HOFSTADTER, *THE AMERICAN POLITICAL TRADITION AND THE MEN WHO MADE IT*, at xxxvi-ii (1973) (seeking a replacement for the historically dominant “ideology of self-help, free enterprise, competition, and beneficent cupidity upon which Americans have been nourished since the foundation of the Republic”).

287. *See supra* Section I.B.1.

288. *See* Cass R. Sunstein, *The Storrs Lectures: Behavioral Economics and Paternalism*, 122 YALE L.J. 1826, 1831 (2013) (“It is important to emphasize that free markets provide significant protection against such errors [in individual choice]. Most important, markets often deter exploitation of human fallibility.”).

289. FED. TRADE COMM’N, *PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS*, at i (2012), [<https://perma.cc/7HT3-2PG9>].

will be much better able to “make meaningful decisions about personal data collection, use, and disclosure” than any arbitrary, government-imposed rule.<sup>290</sup> Against this backdrop, it is difficult to see how market forces alone can be counted on to enforce privacy protections.

Even if such a system of privacy self-management were workable, aspects of the current nature of the information and surveillance economy can render the effects of competition alone rather toothless. Large information-based platforms such as Meta and Google are made up of a broad array of services, usually offered at no cost to the customer.<sup>291</sup> In exchange for these “free” services, consumers give up their personal data, which are then collected, stored, analyzed, and turned into revenue-generating products these platforms can market to third parties.<sup>292</sup> What differentiates platforms from the countless other businesses that follow the surveillance capitalism model is their breadth: Platform-based firms build their businesses on a horizontal model, building, or more commonly, buying services across often disparate verticals to capture as much data in as many contexts as possible, thus giving them the ability to paint more complete pictures of their individual consumers, thus making access to those pictures more valuable.

Standard models of antitrust regulation will have little effect on platform privacy for three reasons. First, the conventional “consumer welfare” approach to antitrust law would likely see little to work with at first glance. Because many, if not all, of a platform’s services are offered at little or no cost to the consumer, an antitrust regulator could very well see this as a benefit to the individual rather than a source of harm.<sup>293</sup> Second, in terms of

---

290. THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD 47 (2012), [<https://perma.cc/PZ76-6MVD>].

291. *But see* John M. Newman, *The Myth of Free*, 86 GEO. WASH. L. REV. 513, 555-60 (2018) (describing the flawed origins of the concept of “free” technology services).

292. *See* ZUBOFF, *supra* note 138, at 52; John Naughton, *The Goal Is to Automate Us: Welcome to the Age of Surveillance Capitalism*, GUARDIAN (Jan. 20, 2019, 2:00 AM), [<https://perma.cc/HB9W-UQA7>].

293. *See* Joshua D. Wright & Douglas H. Ginsburg, *The Goals of Antitrust: Welfare Trumps Choice*, 81 FORDHAM L. REV. 2405, 2406-07 (2013) (“Indeed, there is now widespread agreement that this evolution toward welfare and away from noneconomic considerations has benefitted consumers and the economy more broadly. Welfare-based standards have led to greater predictability in judicial and agency decision making.”).



overall efficiency, platform data use represents a market failure, where society as a whole suffers the deadweight loss from the collective costs associated with individual privacy self-management.<sup>294</sup> Further, the societal costs of privacy loss may be more difficult to directly translate into dollar amounts, but that does not make the harms any less real.<sup>295</sup> Finally, even if antitrust regulators were motivated to enforce competition policy by breaking up or otherwise forcing divestment of an information-based platform company, the privacy concerns would not be directly addressed, but merely split across multiple new firms.<sup>296</sup>

### C. The Application of Antitrust to Privacy Protection Can Make Things Worse

Due in large part to the complex nature of information-based and surveillance-based business models, antitrust remedies to Big Tech problems may end up exacerbating privacy problems. While some of these potential pitfalls arise out of factors associated with the large platforms that dominate the information/surveillance landscape, such as Google or Meta, the difficulties in assessing the actual privacy effects of technology product changes as well as the inevitable arguments regarding the definition of privacy as it pertains to product and consumer choices will drive up the costs of antitrust actions significantly, perhaps enough to dissuade some regulators from engaging at all, thus entrenching or expanding potential privacy harms.

The fact that giant technology platforms continue to dominate an increasing share of commerce and have become de facto gatekeepers in online communications worldwide has made the antitrust remedy of structural separation an attractive possibility.<sup>297</sup> Perhaps the most prominent example of its rare use

---

294. Because information platforms maintain enormous caches of personal data, they make tempting targets for hacking by criminals and governments. The aggregate costs associated with attempts to protect from or remedy these data breaches reaches well into the hundreds of billions of dollars annually. *See* Day & Stemler, *supra* note 231, at 64.

295. *See generally* Citron & Solove, *supra* note 96.

296. *See infra* Section III.C.

297. *See, e.g.,* Khan, *supra* note 186, at 980 (“The[] combined problems of discrimination and information appropriation invite recovering common carriage’s forgotten cousin: structural separations.”).

as an antitrust remedy can be found in the 1982 decision to break up AT&T.<sup>298</sup> Because of its unique initial position within the telecommunications industry, AT&T became a kind of natural monopoly.<sup>299</sup> As AT&T grew, it quickly acquired the financial resources to either buy or bury independent competitors, alarming a sufficient number of government regulators to push for an agreement with the firm. Essentially, AT&T agreed to state regulation of rates and services and to not acquire additional independent telephone companies, while the government agreed not to pursue further antitrust actions against it, making AT&T a regulated monopoly.<sup>300</sup> In 1982, the United States Department of Justice broke up AT&T after it was held liable for using exclusionary practices to maintain its monopoly, exchanging a national monopoly for seven regional monopolies, a process that led to multiple new fights between the new regional Bells and regulators.<sup>301</sup>

Likewise, a breakup of the giant technology platforms would not solve existing privacy problems, but would rather create a new set of privacy problems distributed across multiple new organizations.<sup>302</sup> In addition to some of the problems of deregulated competition like the kind presented post-AT&T breakup, there is little to no evidence that these newer, smaller companies would do anything more to protect user privacy, even if the breakup had nominally increased competition.<sup>303</sup> That is, because the current technology industry has established itself on the surveillance capitalism model, the technologies lend

---

298. See, e.g., *United States v. AT&T*, 552 F. Supp. 131 (D.D.C. 1982).

299. Paul J. Larkin, Jr., *Turning Points in Telecommunications History*, 29 J. MARSHALL J. COMPUT. & INFO. L. 513, 529 (2012).

300. Daniel F. Spulber & Christopher S. Yoo, *Mandating Access to Telecom and the Internet: The Hidden Side of Trinko*, 107 COLUM. L. REV. 1822, 1894-95 (2007).

301. See Larkin, *supra* note 299, at 530-33 (describing the later legislation made necessary in large part due to the problems arising from the incumbent local exchange carriers created by the AT&T breakup).

302. There is a popular aphorism from software development that describes the complications that can result from using the wrong tool to solve a problem: "Some people, when confronted with a problem, think 'I know, I'll use regular expressions.' Now they have two problems." Jeff Atwood, *Regular Expressions: Now You Have Two Problems*, CODING HORROR (June 27, 2008), [<https://perma.cc/RRP4-WVDW>].

303. See Mark MacCarthy, *Privacy as a Parameter of Competition in Merger Reviews*, 72 FED. COMM'NS L.J. 1, 10-11 (2020) (discussing the general lack of privacy considerations in antitrust review).

themselves to opacity with respect to data use, and, because individual consumers are often overburdened with constant privacy self-regulation tasks, is it unlikely that competition alone—absent separate, comprehensive privacy legislation—will address current privacy concerns.

Further complicating this issue is the emergence and rapid growth of the inference economy, based in large part on advances in computing technology, analytical tools and methods, and the availability of very large sets of data comprised of years of widespread personal data collection.<sup>304</sup> These large-scale inference engines raise serious questions about the assumptions inherent in the concept of firms competing on privacy as a measure of quality by skirting measures like data de-identification that have long been thought of as obstacles to many privacy harms.<sup>305</sup> Advanced machine learning algorithms running on increasingly powerful computers can use the many various scraps of data available, even if those data sets have been previously de-identified, to find correlated areas to reassemble a complete picture of an individual, often using statistical methods to predictively fill in, with some degree of accuracy, any gaps in the data that remain.<sup>306</sup> The availability of these tools enables firms to make honest claims about increased privacy (“the data we collect is de-identified, so no personal information is directly tied to you”) while at the same time mining aggregated data sets to recreate individual data portraits with high fidelity.<sup>307</sup> Privacy competition thus becomes a shell game of semantics, confusing consumers at best and, at worst, creating generations of privacy nihilists.

Finally, the definition of privacy is itself a source of disagreement among regulators generally, and this disagreement

---

304. See Priyank Jain, Manasi Gyanchandani & Nilay Khare, *Big Data Privacy: A Technological Perspective and Review*, J. BIG DATA, Nov. 2016, at 1, 3.

305. See, e.g., U.S. DEP’T OF HEALTH AND HUM. SERVS., GUIDANCE REGARDING METHODS FOR DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION IN ACCORDANCE WITH THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY RULE (2012), [<https://perma.cc/5XLR-D5QE>]; INFO. AND PRIV. COMM’R OF ONT., DE-IDENTIFICATION GUIDELINES FOR STRUCTURED DATA (2016), [<https://perma.cc/7QYW-3LQ2>].

306. See Solow-Niederman, *supra* note 267, at 361.

307. See *id.* at 357.

would likely be used by regulators, firms, and advocates as leverage to drive up the costs of antitrust actions to a point where government agencies may balk at enforcement measures.<sup>308</sup> Salient examples of this can be found in the efforts of large technology firms, including Meta, Apple, Amazon, and Google, to question the privacy implications of legislation, making sometimes contrary arguments to state and federal governments in order to minimize the potential impact those legislative efforts would have on them.<sup>309</sup> Of particular relevance to this Article, however, are the simultaneous calls for federal privacy legislation by these same technology companies, although their goals with respect to privacy regulation are still quite self-interested.<sup>310</sup>

## CONCLUSION

The serious issues raised by the rapid growth of technology companies—and the equally rapid adoption of data-generating technologies across wide swaths of society—have spurred

---

308. See, e.g., Timothy J. Muris, *17th Annual Antitrust Symposium: Keynote Panel Discussion*, 21 GEO. MASON L. REV. 1111, 1113 (2014) (“The [FTC] Commissioners were badly spilt on their definition of privacy, so we changed the subject. We moved from a model about notice and choice to a model that the average person doesn’t mind sharing information, if there is a benefit, but they care about their information being misused.”); Elizabeth K. Brill, *Privacy and Financial Institutions: Current Developments Concerning the Gramm-Leach-Bliley Act of 1999*, 21 ANN. REV. BANKING L. 167, 206 (2002) (“[I]t is virtually impossible to get [fifty] individual regulators, working under differing state laws, suffering from inadequate resources, and subject to unique political pressures, to do the same thing at the same time, especially with respect to a relatively new and very hot issue like privacy.” (alteration in original)).

309. See Cat Zakrzewski et al., *With Clock Ticking, Battle Over Tech Regulation Intensifies*, WASH. POST (June 27, 2022, 7:00 AM), [https://perma.cc/RH77-66YF]; Sandeep Vaheesan, *On Antitrust, Don’t Take Big Tech’s Word for It*, BOS. REV. (Mar. 15, 2022), [https://perma.cc/FK7H-U4MK].

310. See Brody Ford, *Big Tech to Congress: Forget About Antitrust, Pass a Privacy Law*, BLOOMBERG (Apr. 8, 2022, 8:00 AM), [https://perma.cc/625L-STDD]; Benjamin Powers, *How Big Tech Is Quietly Pushing for Watered-down State Privacy Laws*, MESSENGER (Apr. 11, 2022, 9:04 AM), [https://perma.cc/YN42-CU2L]; Todd Feathers, *Big Tech Is Pushing States to Pass Privacy Laws, and Yes, You Should Be Suspicious*, MARKUP (Apr. 15, 2021, 8:00 AM), [https://perma.cc/2TTK-6WLJ]; Todd Feathers & Alfred Ng, *Tech Industry Groups Are Watering Down Attempts at Privacy Regulation, One State at a Time*, MARKUP (May 26, 2022, 10:33 AM), [https://perma.cc/TN44-JCNJ]; Bennett Cyphers, *Big Tech’s Disingenuous Push for a Federal Privacy Law*, ELEC. FRONTIER FOUND. (Sept. 18, 2019), [https://perma.cc/W5V8-W855]; David Shepardson, *Tech Companies Back U.S. Privacy Law if It Preempts California’s*, REUTERS (Sept. 26, 2018, 7:39 PM), [https://perma.cc/2BJ4-CUSM].

policymakers to somehow address the short-term and long-term economic, social, and political implications of this changing landscape. One of the principal concerns raised in this environment is that of the protection of privacy: How can we encourage innovation and support beneficial technological advances that are based on our many connections while at the same time protecting the privacy of individuals, not as an end in itself, but as a means of protecting other, more fundamental human values? A recent revitalization of antitrust theory among scholars, policymakers, and regulators has brought with it interesting questions regarding its application to Big Tech, including the protection of privacy. And while there are significant relationships between antitrust and the digital economy, privacy protection is not well suited to antitrust.

This Article argues that privacy's commodification—the ubiquitous collection, storage, and sale of personal data—has created a noxious market, one that is defined by its market failures, unable to be corrected through normal market-based mechanisms, and runs contrary to deep moral and social values deemed necessary by free societies. Entire economies have been built upon the commodification of privacy, often without much thought or debate as to the implications of this choice, resulting in an entrenched technology industry dependent on personal data as its chief resource, which has had a caustic effect on multiple areas of our public and private lives. Because antitrust remedies depend upon the interrelationships between commodities and markets, and are meant as correctives to preserve the health of those markets, their application to privacy protection would, in fact, reinforce privacy's commodification, further exacerbating the problems associated with that noxious market.

That is not to say that privacy protections are not urgently required. Quite the contrary, the rapidly changing technology industry and our wide use of data-generating services and devices require a comprehensive approach to protecting privacy. This Article argues that such an approach cannot be rooted in antitrust but must be based on comprehensive privacy legislation that stands on its own.