Privacy Mismanagement: Privacy Harms, Digital Market Monopolies, and Antitrust Law

KRISTIE LAM[†]

Privacy self-management fails to protect consumer privacy. In the advent of the Internet, individuals had the option to tailor how their personal data was used throughout digital markets. However, since the digital markets are dominated by a few large conglomerates, namely Meta and Google, consumers have little choice to determine how they will use the internet in the face of the blatantly decreasing quality of privacy protection. The lack of adequate privacy protections in the digital markets harms consumers and erodes democratic institutions. Given the societal ramifications of consolidated digital markets on consumers, antitrust laws are the appropriate mechanism to remedy privacy harms and rebuild the guardrails of privacy protections, and the Federal Trade Commission should aggressively enforce these laws. Antitrust and privacy litigation should work in tandem to protect consumers who have had their personal information stolen and misappropriated, and to rebuild trust in democratic institutions.

[†] J.D. Candidate, Class of 2024, University of California College of the Law, San Francisco; Senior Notes Editor, *UC Law Journal*. The Author would like to thank David Rudolph, Brian Weikel, and fellow *UCLJ* members for their invaluable feedback.

TABLE OF CONTENTS

INTRODUCTION

For the foreseeable future, Americans will be met with a familiar onslaught of political messaging during election season. Throughout the internet ecosystem—which, for most part, is limited to simply Meta and Google—Americans will be inundated with political ads carefully tailored to their personal preferences. Political campaigns, armed with the treasure trove of personal data repositories, can engineer online algorithms so that just the right individual sees an advertisement and reacts in just the right way.[1] Although targeted political advertising is not a new phenomenon, modern data collection practices can micro-target individuals in ways unimaginable merely two decades ago.

There is no clearer example of the engineering marvel that is political microtargeting than the Cambridge Analytica scandal. In 2018, news outlets broke the story that the data analytics firm harvested personal data from nearly 87 million Facebook users.[2] Cambridge Analytica compiled psychographic profiles with the ultimate goal of influencing the American electorate.[3] The sheer scale of this dataset meant it could be exploited to "'predict virtually any trait.[4] Armed with an arsenal of weapons to fight [a] culture war political campaigns like Trump for America and Cruz for President capitalized on this dataset to politically manipulate the masses.[5] Tools like Meta Pixel and Google Analytics tracked every click and every page viewed on the Internet. Through online activity, data brokers compiled dossiers filled with details far beyond what individuals willingly shared.[6] What was once an opportunity to connect and find community was suddenly a tool for corporate and political surveillance.

Seemingly overnight, consumer sentiment shifted as the scandal tapped into internet users' anxieties around data protection, and passive acquiescence to trading their personal data in exchange for an online experience became unthinkable.[7] Recognizing that their curated online experiences were made possible by the unceasing collection and commodification of their own data, consumers found ways to combat the invasive privacy practices of "Big Tech"

---

1. Nathan E. Sanders & Bruce Schneier, *Just Wait Until Trump Is a Chatbot*, ATLANTIC (Apr. 28, 2023), https://www.theatlantic.com/technology/archive/2023/04/ai-generated-political-ads-election-candidate-voter-interaction-transparency/673893.

2. Aja Romano, *The Facebook Data Breach Wasn't a Hack. It Was a Wake-Up Call.*, VOX (Mar. 20, 2018, 4:50 PM EDT), https://www.vox.com/2018/3/20/17138756/facebook-data-breach-cambridge-analytica-explained.

3. *Id.*

4. Julia Carrie Wong, *The Cambridge Analytica Scandal Changed the World—But It Didn't Change Facebook*, GUARDIAN (Mar. 18, 2019, 1:00 AM EDT), https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook.

5. *See* Romano, *supra* note 2.

6. Natasha Singer, *What You Don't Know About How Facebook Uses Your Data*, N.Y. TIMES (Apr. 11, 2018), https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html.

7. Diana Baptisa, *Data Privacy Rights Stronger After Cambridge Analytica Scandal*, CONTEXT (Oct. 26, 2022), https://www.context.news/digital-rights/data-privacy-rights-stronger-after-cambridge-analytica-scandal.

(Meta, Google, Apple, and Amazon). Congressional hearings compared Big Tech to Big Tobacco and accused the firms of engaging in monopolistic practices that reduced the quality of consumer privacy protections.[8] An onslaught of litigation began. At first, courts refused to acknowledge the privacy harm through a variety of approaches. There was no standing.[9] There was no financial harm.[10] Consumers consented to the privacy invasion.[11]

These privacy harms continue to reverberate throughout the American political system. Consumers do not have real choice in determining how their personal data is collected, retained, used, and monetized because digital markets are dominated by Big Tech. Not only does this leave individuals vulnerable and exposed to data harms, but the mass collection of data has dire implications for American democracy. The limited scale of individual privacy actions is insufficient to deal with overarching data privacy practices that impact every individual who uses the internet. As such, there is growing consensus that antitrust law provides an optimal framework to address large scale privacy harms that result from a degradation of the quality of privacy.[12] The federal government, through the Federal Trade Commission (FTC), has a duty to preserve consumer privacy and consumers from the oligopolistic practices of Big Tech companies.

This Note argues that, absent an omnibus federal privacy legislation, aggressive agency enforcement of antitrust and unfair competition laws is the most successful path forward for consumers whose information was taken, exploited, and monetized by tech corporations. This is not to say that litigating privacy rights is without merit—rather, antitrust and privacy claims should be asserted concurrently to protect the public from privacy harms by large tech corporations. Doing so is both in line with the principles of antitrust law and will bolster individual privacy rights. Part I of this Note establishes the shortcomings of the current privacy self-management analytical framework and details how these failures exploit an individual's personal data and harm democratic institutions. Part II provides an overview of current antitrust litigation by both private plaintiffs and federal agencies. Part III argues that agency-led litigation will provide the injunctive relief that the public desires.

8. Tripp Mickle, *Big Tech Draws Comparison to Big Tobacco*, WALL ST. J. (Mar. 25, 2021, 12:04 PM), https://www.wsj.com/livecoverage/tech-misinformation-hearing-facebook-twitter-google/card/UUM0f9iceWEjnakqbzkT.

9. *See* Spokeo, Inc. v. Robins, 578 U.S. 330, 342–43 (2016); *cf.* Katz-Lacabe v. Oracle Am., Inc., 668 F. Supp. 3d 928, 941, 943–44 (N.D. Cal. 2023) (holding that Plaintiffs had standing under Article III, but not under the California Unfair Competition Law).

10. *See* TransUnion LLC v. Ramirez, 594 U.S. 413, 437–39 (2021).

11. *See* In re DoubleClick Inc. Priv. Litig., 154 F. Supp. 2d 497, 518 (S.D.N.Y. 2001).

12. Maurice E. Stucke, *Addressing Personal Data Collection as Unfair Methods of Competition*, 38 BERKELEY TECH. L.J. 715, 718 (2023).

I. THE LIMITATIONS OF PRIVACY SELF-MANAGEMENT

The fundamental principle of American privacy law is "the right to be let alone."[13] While privacy protections have been invoked in a variety of circumstances, in the context of tech companies, privacy is primarily concerned with the collection, use, and transference of personal data, where personal data is defined as "any information relating to an identified or identifiable natural person."[14]

Modern privacy law is rooted in two basic assumptions: that tech companies can be trusted to develop and comply with internal data management procedures[15] and that individuals can exert sufficient control over their own personal data.[16] This paradigm was formerly known as "notice and choice": Businesses provide consumers with "notice" through a presentation of terms and informed consumers freely "consent" to accept these terms.[17] Under this regime, individuals have a set of rights over their personal data, such as notice, control, and security, that enable them to make personal data management decisions.[18]

Notice and choice, now known as privacy self-management[19] or the control principle,[20] is a corporation-developed and government-adopted legal framework that manufactures consent for privacy intrusions.[21] It is largely a self-regulatory approach: Corporations can protect as much or as little consumer privacy without culpability from the markets or the government.[22] The ubiquitous privacy policy was born from the privacy self-management regime.[23]

---

13. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

14. Matthew Sipe, *Covering Prying Eyes with an Invisible Hand: Privacy, Antitrust, and the New Brandeis Movement*, 36 HARV. J.L. & TECH. 359, 366 (2023) (citing Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 4(1), 2016 O.J. (L 119) 1).

15. Ari E. Waldman, *The New Privacy Law*, 55 U.C. DAVIS L. REV. ONLINE 19, 26 (2021).

16. Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1880 (2013).

17. Robert H. Sloan & Richard Warner, *Beyond Notice and Choice: Privacy, Norms, and Consent*, 14 J. HIGH TECH. L. 370, 373–74 (2014).

18. See Solove, *supra* note 16, at 1880, and Waldman, *supra* note 15, at 27 for a discussion on this regime, which is based on Fair Information Practices ("FIPs"). For more information on FIPs, see generally Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952 (2017).

19. Solove, *supra* note 16, at 1882.

20. Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 444 (2016).

21. Notice and choice is based on Fair Information Practices ("FIPs"), a set of principles developed by the U.S. Department of Health, Education, and Welfare, meant to protect the privacy of personal data in electronic databases in the late 1970s. Hartzog, *supra* note 18, at 957. The FTC subsequently adopted the control framework associated with FIPs when it started to regulate privacy in the late 1990s. Richards & Hartzog, *supra* note 20, at 444.

22. Paul M. Schwartz & Daniel Solove, *Notice and Choice: Implications for Digital Marketing to Youth*, CHANGELAB SOLUTIONS 2 (2009), https://www.changelabsolutions.org/sites/default/files/documents/Notice_and_choice.pdf.

23. Richards & Hartzog, *supra* note 20, at 444*; see also* Ari E. Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 773, 816 ("Since the mid-1990s, the FTC has enforced a largely self-regulatory privacy regime, which has allowed industry to set the terms of the debate.").

By simply presenting consumers with boilerplate clauses for invasive data collection practices, corporations could efficiently manufacture consent.[24] These privacy policies have an opt-in default; consumers themselves have the burden to opt out.

In the early stages of the internet, legislators gave corporations wide latitude to determine the optimal market balance between profit maximization and unfettered consumer choices, believing that government regulation threatened innovation.[25] The Federal Trade Commission's (FTC) policy is such that corporations only need to notify consumers about data collection practices and provide an opt-out option.[26] So long as corporations comply with these two conditions, they essentially absolve themselves of liability.[27] Through this regime, internal corporate structures have the burden of regulating data managerial systems, not state actors.[28]

The absence of state action in the developmental stages of privacy law continues to harm consumers on an individual and societal level. First, the vast majority of consumers do not have the information necessary to make rational decisions regarding privacy self-management.[29] Second, the privacy self-management regime fails to account for the social value of privacy and the societal harms that result from the mass collection of personal information at scale.[30]

A. INDIVIDUAL LEVEL HARMS

Corporation-generated notice is woefully inadequate because consumers are unlikely to be fully informed about their privacy rights, and therefore cannot provide informed consent. Without truly informed consent, consumers cannot reasonably opt out of privacy policies because they do not have a viable alternative. This coerced consent to privacy policies leaves consumers vulnerable to predatory data collection practices, even if the practices are permissible under the privacy self-management framework. Moreover, the lack of meaningful alternatives has led to a decrease in consumers' trust of digital markets.

There is a fundamental information imbalance between the corporations that generate privacy policies and the consumers that provide consent. This information imbalance has been characterized as a "cognitive problem."[31] There are four distinct issues with privacy self-management: (i) individuals do not read privacy policies; (ii) even if individuals do read privacy policies, they do not

24. Hartzog, *supra* note 18, at 964; *see also* Waldman, *supra* note 15, at 33.
25. Waldman, *supra* note 15, at 34.
26. Richards & Hartzog, *supra* note 20, at 444.
27. *Id.*
28. Waldman, *supra* note 15, at 31.
29. Solove, *supra* note 16, at 1880.
30. Salomé Viljoen, *A Relational Theory of Data Governance*, 131 YALE L.J. 573, 600 (2021).
31. Solove, *supra* note 16, at 1883–85.

understand them; (iii) if individuals do read and understand privacy policies, they largely lack the background knowledge to make an informed decision; and (iv) if individuals do read, understand, and can make an informed decision, their decisions are often skewed.[32] As Jon Leibowitz, former Commissioner of the FTC, noted, "Initially, privacy policies seemed like a good idea. But in practice, they often leave a lot to be desired. In many cases, consumers don't notice, read, or understand privacy policies."[33]

Corporations and consumers participate in an unequal exchange through the notice and choice framework. Consumers cannot provide free and informed consent because consumers only gain short-term benefits in exchange for allowing corporations to potentially retain their personal information in perpetuity.[34] The complexity of data collection practices is such that it is "practically impossible" for an informed consumer, let alone an average consumer, to understand a corporation's technical and institutional policies.[35] In addition, it is common practice for data farmers to collect and aggregate as much data as possible for as long as their servers allow.[36] This perpetual data retention inevitably leads to unpredictable future purposes, and impossibly requires data collectors to provide notice of future uses that they themselves do not know.[37] More importantly, the notice and choice framework legitimizes a fundamentally unequal exchange of commodities.[38] Personal data has been characterized by the World Economic Forum as a "new asset class touching all aspects of society."[39] When consumers accept the terms of a privacy policy or the use of cookies through the notice and choice paradigm, they exchange a relatively short-term benefit for the loss of informational privacy.[40]

The lack of meaningful choice within the privacy self-management system leaves individuals vulnerable and exposed. As a result, consumers have a pessimistic view of privacy law and decreased trust in digital markets.[41] The narrow set of harms recognized by modern American privacy law has encouraged companies to "set up the terms of information relationships any way they wish."[42] Companies are aware of the ticking clock on corporation-led privacy regulation and have an incentive to harvest as much personal data as

32. *Id.* at 1884–85.

33. *Id.* at 1885 (citing Jon Leibowitz, *So Private, So Public: Individuals, the Internet & the Paradox of Behavioral Marketing, Remarks at the FTC Town Hall Meeting on "Ehavioral Advertising: Tracking, Targeting, & Technology"*, FED. TRADE COMM'N (Nov. 1, 2007), https://www.ftc.gov/sites/default/files/documents/public_statements/so-private-so-public-individuals-internet-paradox-behavioral-marketing/071031ehavior_0.pdf.

34. Sloan & Warner, *supra* note 17, at 390.

35. *Id.* at 393.

36. Viljoen, *supra* note 30, at 612.

37. Sloan & Warner, *supra* note 17, at 394.

38. *Id.* at 406.

39. *Id.*

40. *Id.* at 390.

41. Richards & Hartzog, *supra* note 20, at 434.

42. *Id.*

possible in an ever-decreasing timeframe.[43] This perverse incentive has damaging effects on consumer trust, which manifest especially through free expression and political engagement online.[44]

Consumers rightfully have a deep distrust of corporate privacy policies because of the corporation-developed privacy self-management regime. Consumers are faced with a black box of a privacy policy: They do not know how their personal data is collected, retained, used, or monetized. The protection of informational privacy is vital because it is the protection of personal autonomy. It is, as expressed by Justice Brandeis and Samuel Warren, the "right to an inviolate personality"[45]—a marker of individual agency and determination for how a person who engages with society. Under current privacy laws, however, any "assumption that users have actual notice or meaningful choice is an illusion."[46]

B. SOCIAL LEVEL HARMS TO DEMOCRATIC INSTITUTIONS

Privacy self-management addresses individual privacy harms that result from isolated transactions.[47] It was never intended to address mass privacy intrusions wholesale from its corporate developers. Today, tech conglomerates like Meta and Google largely use personal data for advertising purposes. It is a lucrative business—advertising accounted for 79 percent of Google's 2022 revenue, or $224.47 billion,[48] and 97 percent of Meta's 2022 revenue, or $113.6 billion.[49] What started as simple categorization is now a behemoth of behavioral advertising. Companies have developed psychographic techniques that link objective demographic characteristics to abstract characteristics. Age, gender, race, and internet use can be extrapolated and tied to peer group's interests, ideas, and opinions.[50] The framework developed in the early 2000s fails to account for the social value of privacy and the cumulation of privacy harms at scale from these evolving behavioral targeting practices. Additionally, the harms resulting from the absence of government-led regulation contribute to the decline of democratic institutions. Specifically, the mass collection of data without regard for individual privacy rights or the social value of privacy can result in political manipulation, social inequality amplification, and erosion of public trust in democratic institutions.

---

43. *Id.*

44. *Id.* at 454–55.

45. Warren & Brandeis, *supra* note 13, at 211.

46. Richards & Hartzog, *supra* note 20, at 444.

47. Solove, *supra* note 16, at 1881.

48. Tiago Bianchi, *Google: Annual Advertising Revenue 2001-2023*, STATISTA (Feb. 1, 2024), https://www.statista.com/statistics/266249/advertising-revenue-of-google.

49. Stacy Jo Dixon, *Meta: Annual Revenue and Net Income 2007-2023*, STATISTA (Mar. 4, 2024), https://www.statista.com/statistics/277229/facebooks-annual-revenue-and-net-income.

50. Shaun B. Spencer, *The Problem of Online Manipulation*, 2020 U. ILL. L. REV. 959, 973 (2020).

Strong privacy protections must be understood as a desirable societal value.[51] Not only do such guardrails provide individuals with the opportunity to develop self-autonomy, but they also ensure that citizens can act autonomously and fully participate in a flourishing democracy.[52] Instead of understanding data through an individual lens, data should be understood as a subset of a larger framework.[53] Data collection is only relevant because it illustrates the meaningful ways that individuals relate to each other, either biologically, interpersonally, politically, or economically.[54] Again, this exchange of commodities is fundamentally imbalanced. Individuals exchange personal information centrally important to their own autonomy for a unique, personalized internet experience from tech companies. Tech companies can only provide this short-term experience due to the sheer amount of data they have aggregated over the years, and may retain this personal information in perpetuity.[55] The widespread, population-level interests in maintaining individual autonomy and privacy are irreducible to the individual-level interests that notice and choice address.[56]

1. *Political Manipulation and Digital Gerrymandering*

Privacy self-management provides the platform for political manipulators to exert undue influence over voters on a mass scale. In the context of this Note, manipulation is an attempt to change someone's future behavior absent the manipulator's direct interventions.[57] To manipulate someone is to subvert their capacity for self-government—to "undermine or disrupt the ways of choosing that they themselves would critically endorse if they considered the matter in a way that is lucid and free of error."[58] Critically, manipulation is different from simple persuasion or coercion. Methods of persuasion or coercion attempt to influence an individual without undermining their decision-making powers.[59] Persuasion techniques still leave the target the arbitrator of their own agency,[60] while coercion forces an individual to intentionally abandon their self-determined goals.[61] In contrast, manipulators alienate a target from their own decision making powers such that they are uncertain about their own agency. [62]

51. Viljoen, *supra* note 30, at 602.
52. *Id.*
53. *Id.* at 580.
54. *Id.* at 610.
55. *Id.* at 581.
56. *Id.* at 611.
57. Daniel Susser, Beate Roessler & Helen Nissenbaum, *Online Manipulation: Hidden Influences in a Digital World*, 4 GEO. L. TECH. REV. 1, 13 (2019).
58. *Id.* at 16.
59. *Id.* at 16–17.
60. *Id.* at 15.
61. *Id.* at 16.
62. *Id.* at 17–18.

Manipulated targets do not understand the logic behind their actions, nor do they understand if their actions served their own needs or someone else's.[63]

The sophistication of online manipulation techniques presents an immediate and growing threat to individual autonomy, privacy, and democracy.[64] Online political manipulation robs voters of their political autonomy because it deprives them of their ability to make free and unimpaired decisions.[65] Aggregated together, individual harms will have a significant impact on democracy.[66] Yet current privacy law is unequipped to protect democratic institutions from the "dispersed and cumulative nature" of online manipulation harms.[67] Consumers do not have the ability assess, weigh, or judge their own privacy harm, and subsequently do not have an incentive to pursue legal action to redress such harm.[68]

Political campaigns can use microtargeted political ads to leverage individual vulnerabilities and personality traits with the ultimate goal of influencing an election.[69] Through Google and Facebook's data aggregation practices,[70] data brokers can build dossiers[71] and sell that information to campaigns. These campaigns subsequently target vulnerable populations, avoid scrutiny from critics, and hide their work from dissenting voices.[72] Through a process known as political gerrymandering, campaigns possess the power to target one person in one specific household with a specific ad, whereas a different person in that same household would see something entirely.[73] Digital gerrymandering is defined as "the selective presentation of information by an intermediary to meet its agenda rather than to serve its users."[74] For example, in 2010, Facebook designed a message meant to convince users to vote by showing that their friends had already voted.[75] Facebook wanted to test whether a graphic on the platform could induce someone to vote in the 2010 congressional midterm elections when they otherwise would not have.[76] From a sample of sixty million

63. *Id.*

64. Ido Kilovaty, *Legally Cognizable Manipulation*, 34 BERKELEY TECH. L.J. 449, 449 (2019).

65. *Id.* at 470.

66. *Id.*

67. *Id.* at 471.

68. *Id.*

69. *Id.* at 462–63.

70. Barbara Ortutay & Amanda Seitz, *How Microtargeted Political Ads Are Wreaking Havoc on Our Elections*, L.A. TIMES (Feb. 1, 2020, 5:00 AM PT), https://www.latimes.com/business/technology/story/2020-02-01/how-microtargeted-political-ads-are-wreaking-havoc-on-our-elections.

71. Kilovaty, *supra* note 64, at 462–63.

72. John M. King, *Microtargeted Political Ads: An Intractable Problem*, 102 B.U. L. REV. 1129, 1133 (2022).

73. Ortutay & Seitz, *supra* note 70.

74. Jonathan Zittrain, Response, *Engineering an Election*, 127 HARV. L. REV. 335, 336 (2014).

75. *Id.* at 335.

76. *Id.*

voters, individuals who were shown the message were 0.39 percent more likely to vote.[77]

Various presidential campaigns have already played on "deeply held beliefs in the electorate" through technological manipulation to increase their chances of electoral success without political accountability.[78] For example, Cambridge Analytica developed a "psychographic profiling technique" that could disaggregate a dataset such that it could generate a profile with four to five thousand datapoints on nearly any adult in the United States.[79] Political campaigns could use these generated profiles to target messages to voters, and the Trump for America and Cruz for President campaigns employed these techniques to sway the voting preferences of nearly forty-five thousand likely Iowa Republican persuadable targets.[80] Although there are doubts as to whether Cambridge Analytica successfully employed its profiling technique, it is clear that future campaigns and data aggregators will use these methods to rig elections.[81]

2. *Amplifier of Social Inequality*

The social effects of notice and choice include the creation of political silos. When corporations extract mass amounts of personal data to present users with a curated personal experience, such data surveillance technology amplifies identarian polarization, aggression, and violence.[82]

Further, "informational capitalism . . . puts marginalized populations at unique risks."[83] Marginalized individuals "experience privacy differently than most Americans" because their challenges are obscured and further entrenched.[84] Marginalized populations, such as undocumented immigrants, day laborers, homeless people, and individuals with felony convictions, "experience [the] privacy extremes [of] being . . . tracked too much or too little."[85] Digital institutions replicate the mechanisms by which the administrative state categorizes individuals, such as race, gender, tax bracket, and disability.[86] As a result, both an individual's digital footprint, as well as the structural power imbalances they are subject to, have been uploaded into the metaverse.[87] For example, the City of Boston implemented an app that allowed city residents to

77. *Id.* at 336.

78. Kilovaty, *supra* note 64, at 462–63.

79. *Id.* at 467.

80. *Id.*

81. *Id.* at 468.

82. Viljoen, *supra* note 30, at 580–81 ("Digital-surveillance technologies used to enhance user experience for the rich simultaneously provide methods of discipline and punishment for the poor.").

83. Waldman, *supra* note 15, at 38.

84. Michele Gilman & Rebecca Green, *The Surveillance Gap: The Harms of Extreme Privacy and Data Marginalization*, 42 N.Y.U. REV. L. & SOC. CHANGE 253, 254–55 (2018).

85. *Id.* at 255.

86. *Id.* at 284, 255 n.201.

87. *Id.* at 284–85.

report potholes and inform the city which streets needed the most repair. [88] Yet the app had an inverse effect: residents of affluent parts of the city were more likely to install the app and report potholes.[89] This distorted the scope of street repair needs throughout the city and exacerbated already existing disparities in Boston street quality.[90]

The inability to provide consent under privacy self-management is felt particularly harshly within marginalized communities. As discussed previously, privacy self-management assumes that individuals can make informed decisions to negotiate their own privacy boundaries. Yet marginalized communities often possess little or no political power due to decades of political disenfranchisement.[91] The structure of the Internet facilitates a mob mentality that allows anonymous groups to come together and deny women, people of color, religious minorities, and LGBTQ+ individuals access to opportunities both on and offline,[92] constraining the choices of members of marginalized communities and limiting their individual agency.[93] Anonymous online groups target vulnerable populations with "a destructive combination of threats, damaging statements aimed to interfere with their employment opportunities, privacy invasions, and denial-of-service attacks because of their gender or race." [94] Site operators that refuse to dismantle these attacks "reinforce, and effectively encourage, negative behavior."[95] Moreover, such website operators generally have access to the information necessary to identify anonymous abusers but make the conscious decision not to retain that information.[96] Since site operators have "blanket immunity" for the content posted on their platforms, they lack incentive to quell high rates of abusive website activity. [97] As such, "objectionable posts remain online and searchable by employers, often migrating across the Web to become effectively irretrievable, while plaintiffs continue to be unable to find and recover damages from wrongdoers."[98] Added to which, social media companies have a financial incentive to create political silos, promote radical content, and retain a user's attention, further enabling abusive online activity.[99] Thus, the absolution of digital market platforms' liability through privacy self-management has directly led to the rise in online

88. *Id.* at 285.
89. *Id.*
90. *Id.*
91. *Id.* at 294.
92. Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 68 (2009).
93. *Id.* at 69.
94. *Id.* at 68–69.
95. *Id.* at 84.
96. *Id.* at 118.
97. *Id.* at 119.
98. *Id.*
99. Karen Hao, *How Facebook Got Addicted to Spreading Misinformation*, MIT TECH. REV. (Mar. 11, 2021), https://www.technologyreview.com/2021/03/11/1020600/facebook-responsible-ai-misinformation.

extremism, the price of which falls most heavily on marginalized communities.[100]

3. *Erosion of Trust in Democratic Institutions*

The federal government's complacency with privacy self-management and apparent lack of privacy rights enforcement has led to eroding trust in democratic institutions. With unfettered access to the digital fingerprints of billions of users, only a handful of corporations control the free flow of information online. The corporate surveillance conducted by companies like Google and Meta include reliable indicators of an individual's political inclinations.[101] There is always a risk that these dossiers could be used to unduly influence political opinions or manipulate election results.[102] For example, with an algorithm built to capitalize on an individual's attention, digital platforms can create echo chambers that "filter the range of available information and limit communication . . . to like-minded individuals."[103] Dissatisfied Americans, recognizing these harmful developments but who lack any real alternatives in the digital market, blame the government.

Polling consistently shows that Americans' declining trust in democratic institutions parallels the perceived power and influence that Big Tech exerts over society and government institutions.[104] In a 2020 Pew Research Center poll of Americans' attitudes toward tech companies, around three-quarters of Americans believed that they are "not too confident or not at all confident" that tech companies would prevent misuse of their platforms to influence the 2020 presidential election.[105] In addition, nearly three-quarters of Americans believed it was likely that social media sites intentionally censor political opinions that the platform objected to.[106] The American public recognized the influence that these tech companies have on American democratic institutions, and this influence is fueled in part by the monetization and exploitation of personal data. Further, in 2022, Variety Intelligence Platform partnered with GetWizer Consumer Insights to ask seventeen hundred Americans about their attitudes regarding the influence of "Big Tech" companies such as Alphabet/Google, Amazon, Apple, and Meta/Facebook.[107] Two-thirds of those surveyed believed

100. Citron, *supra* note 92, at 114, 118.

101. Ashutosh Bhagwat, *The Law of Facebook*, 54 U.C. DAVIS L. REV. 2353, 2360 (2021).

102. *Id.*

103. Viktoria H.S.E. Robertson, *Antitrust, Big Tech, and Democracy: A Research Agenda*, 62 ANTITRUST BULL. 259, 260 (2022).

104. Brian F. Shaffner, *Public Demand for Regulating Big Tech*, TECH OVERSIGHT PROJ. 3 (June 6, 2022), https://techoversight.org/wp-content/uploads/2022/06/Schaffner-Big-Tech-Polling.pdf.

105. Brook Auxier, *How Americans See U.S. Tech Companies as Government Scrutiny Increases*, PEW RSCH. CTR. (Oct. 27, 2020), https://www.pewresearch.org/fact-tank/2020/10/27/how-americans-see-u-s-tech-companies-as-government-scrutiny-increases.

106. *Id.*

107. Gavin Bridge, *Survey: U.S. Consumers Fear Power of Big Tech*, VARIETY (Mar. 31, 2022, 6:00 AM PT), https://variety.com/vip/survey-u-s-consumers-fear-power-of-big-tech-1235219203.

that these companies wield "too much power over the public," and over two-thirds of those surveyed thought "the government [should] keep tabs on Big Tech more closely."[108] The lack of strong data privacy and security protection legislation led to a rise in election-denier misinformation campaigns and ultimately damaged trust in the integrity of the 2020 election.[109]

The privacy self-management regime has had consequential impacts on individual privacy rights and on American democratic institutions. It allows for the mass corporate collection of data without regard for individual privacy rights or the social value of privacy. This unending flow of personal data by large tech conglomerates robs individuals of their individual privacy and autonomy. At the same time, unregulated data collection can result in political manipulation, social inequality amplification, and erosion of public trust in democratic institutions.

II. ANTITRUST LAWSUITS ARE A VIABLE LITIGATION STRATEGY

Despite the individual informational privacy harms and threats to the democratic political process that are tied to the notice and choice framework, the development of comprehensive federal legislation as an alternative remains at a standstill.[110] Short of industry-shifting privacy reform, antitrust and unfair competition litigation is a viable means to remedy individual and societal level privacy harms. Antitrust actions are an established and proven mechanism to address large scale harms, particularly when enforced by the FTC. This Part will provide a brief background of antitrust law, discuss how aggressive antitrust enforcement strengthens democracy, and contextualize current antitrust privacy actions. In particular, this Part will argue that cases like *Klein v. Facebook*[111] demonstrate that courts are sympathetic to privacy harm claims asserted through an antitrust framework.

A. WHY NOT PRIVACY LITIGATION?

There are two primary reasons why plaintiffs should address privacy harms against large tech companies through antitrust claims rather than under right-to-privacy tort laws. First, privacy litigation has not proved to be a fruitful endeavor. Second, antitrust actions are by contrast a proven mechanism to protect consumers from large scale harms caused by functional monopolies and are capable of establishing injunctive remedies that will prevent future harm.

There is no singular federal law or scheme that addresses data privacy. Instead, privacy practitioners have stitched together an amalgamation of state data privacy laws, combining laws that address specific types of data and privacy

108. *Id.*

109. Wayne Unger, *How the Poor Data Privacy Regime Contributes to Misinformation Spread and Democratic Erosion*, 22 COLUM. SCI. & TECH. L. REV. 308, 333–34 (2021).

110. Allison Grande, *States Pile on Privacy Law Patchwork as Congress Stagnates*, LAW360 (May 5, 2023, 10:55 PM EDT), https://www.law360.com/articles/1604817/states-pile-on-privacy-law-patchwork-as-congress-stagnates.

111. Klein v. Facebook, Inc., 580 F. Supp. 3d 743, 759 (N.D. Cal. 2022).

tort without providing an overarching framework.[112] Perhaps due to the lack of statutory cohesion and the focus on individual privacy self-management, class-action privacy claims have fallen short in litigation.[113] For example, the Northern District of California denied as moot the plaintiffs' Motion for Class Certification in *Calhoun v. Google*, where plaintiffs alleged that Google's data collection practices violated California's Invasion of Privacy Act and tort claims such as intrusion upon seclusion, breach of contract, and statutory larceny.[114] The Southern District of New York granted the motion to dismiss in *In re DoubleClick Inc. Privacy Litigation*, where plaintiffs brought a class action under the Electronic Communications Privacy Act and common law invasion of privacy.[115] While there are privacy-specific claims that have recently passed the motion to dismiss and class certification hurdles,[116] it may be some time before binding case law is established. Cases may be dismissed at the summary judgment stage or settle, establishing as precedent only the initial complaint. There is also no indication that Congress will pass federal privacy legislation granting a private right of action. Comprehensive privacy litigation legislation, such as the Online Privacy Act (OPA), has been repeatedly introduced without success.[117]

Given the large scale of privacy harms, antitrust actions present the best path forward for litigants. Antitrust actions inherently focus on consumer welfare and are "rooted in a deep suspicion of concentrated private power,"[118] such as the power of utility-level companies like Meta and Google. Antitrust actions are an established and proven mechanism to address large-scale harms from corporate misrepresentations that can fill in the void in the absence of federal privacy legislation. Indeed, there is already evidence that class action privacy harm claims may be successful under antitrust law. For example, in *In re iPhone Application Litigation*, Judge Koh dismissed claims under the Stored Communications Act and right to privacy, but found that the class stated a claim

112. Grande, *supra* note 110.

113. *See* In re Meta Pixel Healthcare Litig., 647 F. Supp. 3d 778, 784 (N.D. Cal. 2022) (order denying preliminary injunction).

114. Calhoun v. Google, LLC, 645 F. Supp. 3d 916, 920 (N.D. Cal. 2022) (granting motion for summary judgment and denying motion for class certification as moot).

115. In re DoubleClick Inc. Privacy Litig., 154 F. Supp 2d. 497, 526 (S.D.N.Y. 2001).

116. *See* Fed. Trade Comm'n v. Kochava, Inc., 671 F. Supp. 3d 1161, 1176 (D. Idaho 2023); In re Google RTB Consumer Priv. Litig., 606 F. Supp. 3d 935, 947 (N.D. Cal. 2022).

117. Silicon Valley Congresswomen Reintroduce Comprehensive Privacy Legislation, U.S. CONGRESSWOMAN ZOE LOFGREN (Apr. 19, 2023), https://lofgren.house.gov/media/press-releases/silicon-valley-congresswomen-reintroduce-comprehensive-privacy-legislation; *see also* Lee Tien, Adam Schwartz, & Hayley Tsukayama, *Why the EFF Doesn't Support California Proposition 24*, ELECTRONIC FRONTIER FOUND. (July 29, 2020), https://www.eff.org/deeplinks/2020/07/why-eff-doesnt-support-cal-prop-24 (critiquing the California Consumer Privacy Act of 2018 in part because it did not contain a robust private right of action).

118. David Streitfeld, *Amazon's Antitrust Antagonist Has a Breakthrough Idea*, N.Y. TIMES (Sept. 7, 2018), https://www.nytimes.com/2018/09/07/technology/monopoly-antitrust-lina-khan-amazon.html.

under California's Unfair Competition Law.[119] The next Subpart will discuss why this approach is more viable.

B. WHY ANTITRUST AND UNFAIR COMPETITION?

The core purpose of antitrust and unfair competition laws is to "protect the process of competition for the benefit of consumers" and ensure that there are strong incentives for businesses to operate efficiently.[120] The three core federal antitrust laws—the Sherman Act, the Clayton Act, and the Federal Trade Commission Act—were enacted at the end of the Gilded Age, a period of gross materialism and monopolistic business practices.[121] Suspicious of consolidated industries,[122] Congress sought to curtail the exercise of democratically unaccountable corporate power over the American populous through antitrust laws.[123]

The Sherman Act, the Clayton Act, and the Federal Trade Commission Act work in tandem to fulfill Congress's mandate "to protect the public from the failure of the market"[124] Section 1 of the Sherman Act prohibits "every contract, combination, or conspiracy in restraint of trade,"[125] while section 2 criminalizes "any monopolization, attempted monopolization, or conspiracy or combination to monopolize."[126] The Clayton Act strengthens the Sherman Act and provides a private right of action for conduct that violates either statute.[127] Additionally, the Clayton Act prohibits discriminatory and predatory pricing in transactions between merchants and requires corporations to notify the federal government when planning large mergers or acquisitions.[128] The Federal Trade Commission Act, which created the Federal Trade Commission (FTC), the primary enforcement agency of antitrust violations, prohibits "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce."[129] All violations of the Sherman Act are also violations of the Federal Trade Commission Act, and the FTC may seek

119. In re iPhone Application Litig., 844 F. Supp. 2d 1040, 1049 (N.D. Cal. 2012).

120. *The Antitrust Laws*, FED. TRADE COMM'N, https://www.ftc.gov/advice-guidance/competition-guidance/guide-antitrust-laws/antitrust-laws (last visited June 19, 2024).

121. Sandeep Vaheesan, *Accommodating Capital and Policing Labor: Antitrust in the Two Gilded Ages*, 78 MD. L. REV. 766, 767 (2019).

122. *See* Robert H. Bork, *Legislative Intent and the Policy of the Sherman Act*, 9 J.L. & ECON. 7, 8 (1966) (quoting United States v. Aluminum Co. of Am., 148 F.2d 416, 428 (2d Cir. 1945)) ("[G]reat industrial consolidations are inherently undesirable, regardless of their economic results. In the debates in Congress Senator Sherman himself . . . showed that among the purposes of Congress in 1890 was a desire to put an end to great aggregations of capital because of the helplessness of the individual before them." (emphasis omitted)).

123. Vaheesan, *supra* note 121, at 773.

124. Spectrum Sports, Inc. v. McQuillan, 506 U.S. 447, 458 (1993).

125. 15 U.S.C. § 1.

126. *Id.* § 2.

127. *Id.* § 18.

128. *Id.* § 18a(d).

129. *Id.* § 45.

consumer redress, civil penalties, or an injunction against offending corporations.[130]

There are two schools of thought concerning antitrust law. The Chicago School argues that antitrust law should focus on consumer welfare, or the short-term effects of anti-competitive conduct, by fixating on consumer prices.[131] Under this framework, price is the primary indicator of consumer purchase power.[132] The Harvard School, also known as the neo-Brandeis movement or the Hipster Antitrust movement, focuses on the broad societal harms caused by an oligopolistic economic structure and argues that high market concentration leads to anticompetitive behavior.[133] Popularized by Lina Khan, the current Chair of the FTC, the Harvard framework is based on the argument that antitrust laws "were rooted in deep suspicion of concentrated private power."[134] Followers of the neo-Brandeis movement argue that antitrust law should be used to prevent large market share by a limited number of actors and promote competitive markets.[135]

Critiques of the application of the neo-Brandeis vision of antitrust law to privacy regimes argue that increasing competition among tech corporations will decrease privacy protections.[136] Specifically, the argument is that increasing the number of data-collection focused companies will not promote personal data privacy; instead, it will lead to a greater likelihood of privacy breaches and create clarity and uniformity issues for legal enforcement.[137] Yet these critiques presume that the data companies themselves can be trusted to self-regulate. As demonstrated by increasingly aggressive antitrust enforcement from the Department of Justice and Federal Trade Commission, there is serious doubt that these companies will act in a manner that promotes social welfare and cohesion when their business model is at stake.[138]

1. *The Nexus Between Antitrust and Democracy*

"American antitrust [law] . . . is first about freedom."[139] The courts and legal scholars alike recognize that antitrust enforcement plays a vital role in maintaining democratic institutions.[140]

---

130. Herbert J. Hovenkamp, *The Federal Trade Commission and the Sherman Act*, 62 FLA. L. REV. 1, 3 (2010); *Notices of Penalty Offenses*, FED. TRADE COMM'N, https://www.ftc.gov/enforcement/penalty-offenses (last visited Aug. 2, 2024).

131. Lina M. Khan, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710, 719 (2017).

132. *Id.* at 721.

133. *Id.* at 740.

134. Streitfeld, *supra* note 118.

135. Khan, *supra* note 131, at 737.

136. Sipe, *supra* note 14, at 389.

137. *Id.*

138. Blair Levin & Larry Downes, *Microsoft, Google, and a New Era of Antitrust*, HARV. BUS. REV. (Feb. 17, 2023), https://hbr.org/2023/02/microsoft-google-and-a-new-era-of-antitrust.

139. Eleanor M. Fox, *The Sherman Antitrust Act and the World—Let Freedom Ring*, 59 ANTITRUST L.J. 109, 113 (1990).

140. Spencer Weber Waller, *Antitrust and Democracy*, 46 FLA. ST. U. L. REV. 807, 808 (2019).

Daniel Crane argues that antitrust has an important role in bolstering democracy.[141] According to Crane, antitrust law is an instrument of democracy through four dimensions: (i) antitrust law prevents the aggregation of undue economic power that can lead to excessive concentration of political power; (ii) it keeps open channels of political discourse and participation; (iii) it is relevant to government regulatory processes; and (iv) it creates democratic and social economic norms.[142]

By comparison, pervasive monopoly threatens democratic values. Prior to his appointment as FTC Commissioner, Robert Pitofsky wrote that non-economic, democratic political values must be considered in antitrust actions.[143] These values include a fear of concentrated economic power, a reduction in the range of private discretion, and an avoidance of state-controlled industries.[144] Antitrust law preserves the competitive economic process, not the individual competitors themselves, and thus promotes a meritorious, democratic system.[145] Concentration of economic power consolidates political power.[146] By outlawing monopolies, monopolistic conduct, and unfair methods of concentration, antitrust laws prevent "industrial monarchs" from amassing concentrated economic power[147] and thus restrict the development of a fascist state.[148] In turn, large corporations are less likely to fall victim to absentee ownership, and local ownership and civic responsibility are continually strengthened.[149]

Much of the legal scholarship surrounding the intertwined nature of antitrust law and democracy can be read as a reaction to the fascist monopolies of 1930s Germany. The presence of monopolies and the lack of antitrust laws contributed to Hitler's rise in the 1930s.[150] During that time, the German economy was dominated by a small number of firms.[151] The absence of competition led to decreased product quality and increased prices throughout markets, which resulted in extreme social inequality.[152] In response, an anti-establishment, populist wave overtook the country and citizens elected an extreme, authoritarian, and autocratic government.[153] Had there been consumer welfare antitrust legal protections, German economy would not have fallen to market concentration and monopolies.[154] As then-Secretary of War Kenneth

141. Daniel A. Crane, *Antitrust as an Instrument of Democracy*, 72 DUKE L.J. ONLINE 21, 23 (2022).
142. *Id.* at 23–24.
143. Robert Pitofsky, *The Political Content of Antitrust*, 127 U. PA. L. REV. 1051, 1051 (1979).
144. *Id.* at 1053.
145. *Id.* at 1063.
146. Khan, *supra* note 131, at 740.
147. *Id.*
148. Pitofsky, *supra* note 143, at 1063.
149. *Id.* at 1064.
150. Chi. Humans. Festival, *Tim Wu: The Curse of Bigness*, YOUTUBE (Jan. 3, 2019), https://youtu.be/_kg41tOGzjg?si=Qlh8rSnXWJQSaDpS.
151. *Id.*
152. *Id.*
153. Crane, *supra* note 141, at 24.
154. Daniel A. Crane, *Fascism and Monopoly*, 118 MICH. L. REV. 1315, 1369 (2020).

Royall bluntly wrote in a report regarding German cartels and industry, "[t]he monopolies . . . got control of Germany, brought Hitler to power and forced virtually the whole world into war."[155]

Following World War II, the United States was very concerned that the country could turn towards fascism or communism if it failed to nurture an economically competitive and diverse society.[156] As a result, strong antitrust enforcement laws were a vital part of post-World War II reconstruction efforts.[157] By targeting monopolistic corporate powers, antitrust laws ensure that no corporation can dominate the market or unilaterally overwhelm the will of the people. Yet we now find ourselves in what Tim Wu calls a "new Gilded Age," where "[m]any fear Google, Amazon, and Facebook, and their power over not just commerce, but over politics, the news, and our private information."[158] With the rise of Big Tech, we "once again . . . face . . . the 'Curse of Bigness,' which . . . represents a profound threat to democracy itself" given . . . industry capacity to exert a "greater influence over elections and lawmaking than [do] mere citizens."[159] Furthermore, democratic erosion is compounded by the fact that individuals experience gross inequality and material suffering in a society characterized by such concentrated monopolistic private power.[160] As the rise of Hitler in Germany illustrates, when individuals are denied choices in all markets, they draw away from democracy and gravitate toward extreme, authoritarian, and autocratic government.[161]

Concerns around the effects of anti-competitive markets on democracy continue to animate the courts today more broadly. The Third Circuit in *LePage's, Inc. v. 3M* reasoned that anti-competitive conduct must be considered not just through individual aspects like price, but holistically to understand the overall combined effect of the conduct.[162] Notably, the court stated that:

> [T]he provision of the antitrust laws designed to curb the excesses of monopolists and near-monopolists, is the equivalent in our economic sphere of the guarantees of free and unhampered elections in the political sphere. Just as democracy can thrive only in a free political system unhindered by outside forces, so also can market capitalism survive only if those with market power are kept in check. That is the goal of the antitrust laws.163

As recognized in *LePage*, antitrust laws are not solely focused on the price of goods. Instead, the goal of antitrust laws is to facilitate a free economy, and a

155. Pitofsky, *supra* note 143, at 1062.

156. CNBC, *Google, Facebook, Amazon and the Future of Antitrust Laws*, YOUTUBE (Aug. 16, 2019), https://www.youtube.com/watch?v=IcghGCBROR0.

157. Chi. Humans. Festival, *supra* note 150.

158. TIM WU, THE CURSE OF BIGNESS: ANTITRUST IN THE NEW GILDED AGE 15 (2018).

159. *Id.*

160. Crane, *supra* note 141, at 24.

161. *Id.*

162. LePage's Inc. v. 3M, 324 F.3d 141, 162 (3d Cir. 2003).

163. *Id.* at 169.

free economy is a key check to prevent the consolidation of political power by a single entity.

2. *Developments in Privacy and Antitrust Law*

In July of 2022, the House of Representatives Subcommittee on Antitrust, Commercial, and Administrative Law published a report (the "House Report") on competition among the four dominant tech corporations: Amazon, Apple, Facebook, and Google.[164] The House Report detailed how their business practices and market power impact the American economy and democracy.[165] Significantly, the report presented evidence that these firms' dominant practices in digital markets "erode entrepreneurship, degrade Americans' privacy online, and undermine the free and diverse press. The result is less innovation, fewer choices for consumers, and a weakened democracy."[166]

The House Report specifically identified the decline in quality of privacy services over time as evidence of market power, drawing a parallel between a platform's "ability to maintain strong networks while degrading user privacy" and a monopolist's decision to increase prices or reduce product quality.[167] Amazon, Apple, Facebook, and Google lack genuine competitive threats, empowering them to offer fewer privacy protections than they would otherwise have been able to in a more competitive atmosphere, all while extracting even more data and "further entrenching [their] dominance."[168] Consumers have little power to resist because their choices are limited to using a service with intentionally weak, subpar privacy safeguards, or not using the service (or any comparable one, if an alternative even exists) at all.[169] As Subcommittee Chair David Cicilline noted in a hearing, "[b]ecause concentrated economic power also leads to concentrated political power, this investigation also goes to the heart of whether we, as a people, govern ourselves, or whether we let ourselves be governed by private monopolies."[170]

Dina Srinivasan anticipated the findings of the House Report in her article *The Antitrust Case Against Facebook*, in which she argues that "Facebook engaged in a decade-long pattern of false statements and misleading conduct that may have induced users to trust and choose Facebook over [other] market alternatives," even to their own detriment.[171] Instead of focusing on merely the competitive pricing of social media services to consumers (or lack thereof), Srinivasan argues that the success of Facebook's monopolistic practices went

164. H.R. REP. NO. 47-832, at 1 (2022).
165. *Id.*
166. *Id.* at 2.
167. *Id.*
168. *Id.* at 40.
169. *Id.*
170. *Id.* at 61.
171. Dana Srinivasan, *The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy*, 16 BERKELEY BUS. L.J. 39, 45 (2019).

hand in hand with the *quality of its consumer privacy protections*.[172] Specifically, Srinivasan argues that Facebook's overt extraction of consumers' personal data and digital activity in violation of self-promulgated privacy policies was a direct result of its uncontested power.[173]

Facebook gained significant market power in the early 2000s by capitalizing on consumers' privacy concerns.[174] Facebook outwardly signaled that they prioritized consumer privacy by providing a short privacy policy and protective privacy settings.[175] Consumers believed that Facebook had superior privacy quality relative to the other market players at the time, such as MySpace, Friendster, Google, and AOL.[176] Within the decade, 99 percent of adults who used social media used Facebook,[177] and Facebook controlled over 80 percent of consumer time online.[178] These numbers reflect Facebook's monopolistic power in the social media market, against which other social media companies could not compete.[179] Once Facebook massed a significant share of the market, it "leveraged its market power in a consolidated market to successfully degrade privacy to levels unsustainable in the earlier competitive market when market participants were subject to consumer privacy demands."[180]

"Multiple independent investigations" revealed that Facebook was simply not concerned with user privacy.[181] Facebook itself conceded that the privacy protection claims made through its privacy policies and public comments were false.[182] Yet Facebook's disingenuous marketed commitment to user privacy nonetheless succeeded in engendered trust in consumers and succeeded in pushing out rivals. This subsequently led to a degradation of privacy below what is required in a competitive market "in contravention to consumer welfare" while Facebook continued to rake in astronomical profits—precisely the type of harm that antitrust law is meant to prevent. [183]

As *Klein v. Facebook*,[184] *Brown v. Google LLC*,[185] *Brooks v. Thomson Reuters Corporation*,[186] and *Federal Trade Commission v. Facebook*[187] demonstrate, courts recognize that privacy harms are not price-barred under

172. *Id.* at 46.
173. *Id.* at 44.
174. *Id.* at 53–54.
175. *Id.* at 51.
176. *Id.* at 53–54.
177. *Id.* at 54.
178. *Id.* at 88.
179. *Id.*
180. *Id.* at 55.
181. *Id.* at 92.
182. *Id.*
183. *Id.* at 90.
184. Klein v. Facebook, Inc., 580 F. Supp. 3d 743, 763 (N.D. Cal. 2022).
185. Brown v. Google LLC, No. 4:20-CV-3664-YGR, 2023 WL 5029899, at *21 (N.D. Cal. Aug. 7, 2023).
186. Brooks v. Thomson Reuters Corp., No. 21-CV-01418-EMC, 2021 WL 3621837, at *11 (N.D. Cal. Aug. 16, 2021).
187. Fed. Trade Comm'n v. Facebook, Inc., 581 F. Supp. 3d 34, 55–56 (D.D.C. 2022).

antitrust laws. Instead, a corporation's misrepresentation of privacy protections and failure to provide adequate privacy guardrails are sufficient claims that warrant remedy.

a. Klein v. Facebook

In *Klein v. Facebook*, a consumer-class action lawsuit tested Srinivasan's legal argument that a tech company's data collection practices could be remedied through an antitrust framework. The claim survived a motion to dismiss, alleging that (i) "Facebook acquired and maintained monopoly power in the Social Network and Social Media Markets by making false representations to users about [its] data privacy practices" and that (ii) Facebook's "Copy, Acquire, Kill" strategy allowed it to maintain monopoly power in the social network and social media markets in violation of section 2 of the Sherman Act.[188] The plaintiffs claimed that Facebook's false misrepresentations to users about its data privacy practices "were 'instrumental to Facebook gaining and maintaining market share at the expense of its rivals.'"[189] For more than a decade, the plaintiffs alleged, Facebook deceived consumers about the data privacy protections it provided to users in exchange for access and retention of personal data. Facebook then sold the data to third parties while representing to users that it was keeping such data private, and this enabled Facebook to increase its reach in both user base and profits.[190]

The court held that the plaintiffs "alleged with significant particularity that Facebook made numerous 'clearly false' representations about Facebook's data privacy practices."[191] Namely, the court sustained the plaintiffs' claims that Facebook falsely represented that: (i) it was not sharing users' private information with third parties; (ii) users could prevent the "Beacon" tool and "Like" button from collecting personal data; and (iii) it was not using cookies to collect personal data for commercial purposes.[192] By drawing on recent privacy claims that recognized that plaintiffs who lose personal information suffer an economic injury, the court also sustained plaintiffs' allegation that information and attention has monetary value.[193] The plaintiffs plausibly alleged that they lost money or property when they provided Facebook with their attention and personal information.[194] In surviving the motion to dismiss, the plaintiffs demonstrated that antitrust privacy claims based on false representations of privacy protections are a viable strategy to remedy privacy harms.

188. *Klein*, 580 F. Supp. at 763.

189. *Id.* at 785 (quoting the Complaint, ¶¶ 108, 217).

190. *Id.* at 788.

191. *Id.* at 795.

192. *Id.*

193. *Id.* at 803–04; *see also* Calhoun, *supra* note 114; In re Marriott Int'l, Inc. Consumer Data Sec. Breach Litig., 440 F. Supp. 3d 447, 461 (D. Md. 2020); In re Yahoo! Inc. Consumer Data Sec. Breach Litig., No. 16-MD-02752-LHK, 2017 WL 3727318, at *19–20 (N.D. Cal. Aug. 30, 2017).

194. *Klein*, 580 F. Supp. at 803.

b. Brown v. Google

In *Brown v. Google*, the court held that plaintiffs suffered an injury under California's Unfair Competition Law (UCL) when Google collected and sold their private browsing data.[195] The plaintiffs alleged that Google represented it would not collect their information when the plaintiffs used the private browsing mode.[196] Google allegedly collected a user's private browsing history and connected it to a preexisting user profile, which allowed Google to "offer better, more targeted, advertisements to users."[197] Furthermore, by selling the plaintiffs' private browsing data, Google prevented plaintiffs from monetizing their data on their own.[198]

On summary judgement, Google argued that the plaintiffs' UCL claim failed because they did not lose money or property, so they did not suffer an economic injury.[199] The court disagreed, and found that there was a market for the plaintiffs' private browsing data and that "Google's alleged surreptitious collection of the data inhibited plaintiffs' ability to participate in that market."[200] Importantly, the court found that money damages alone was not a sufficient remedy; Google could be subject to an injunction that would address the "ongoing collection of users' private browsing data."[201]

c. Brooks v. Thomson Reuters Corp.

In *Brooks v. Thomson Reuters Corp.*, the court sustained the plaintiffs' claim for injunctive relief for violations of California's UCL.[202] The plaintiffs, on behalf of all California residents whose personal data was included in a third-party database during the limitations period, alleged the following: Thomson Reuters aggregated public and nonpublic information about millions of people from sources such as social networks and law enforcement agencies to create "detailed cradle-to-grave dossiers."[203] These dossiers contained an individual's name, photograph, criminal history, financial records, employment information, relatives, and associates.[204] Thomson Reuters subsequently sold these dossiers through an online platform named CLEAR "without the knowledge or consent of the persons to whom the information concern[ed]" and profited significantly.[205]

195. Brown v. Google LLC, No. 4:20-CV-3664-YGR, 2023 WL 5029899, at *1 (N.D. Cal. Aug. 7, 2023).
196. *Id.*
197. *Id.* at *2.
198. *Id.*
199. *Id.* at *21.
200. *Id.*
201. *Id.*
202. Brooks v. Thomson Reuters Corp., No. 21-CV-01418-EMC, 2021 WL 3621837, at *11 (N.D. Cal. Aug. 16, 2021).
203. *Id.* at *1.
204. *Id.*
205. *Id.*

The court sustained the unfair prong of the plaintiff's unfair competition claim because: (i) "the unauthorized dissemination of virtually every piece of Plaintiffs' personal information on the CLEAR platform may constitute a severe invasion of privacy"[206] and (ii) the California legislature intended to protect the personal information and consumer data of the Plaintiffs from unauthorized online dissemination.[207] Although the court denied the plaintiffs' claim for monetary relief for their unfair competition claim, the court granted an injunction to ensure that Thomson Reuters stopped their practice of selling the plaintiffs' personal information without their consent.[208] Importantly, the court recognized the ultimate futility of damages claims: damages would not incentivize Thomson Reuters to change their behavior, nor could damages fully remedy the plaintiffs' invasion of privacy injury.[209]

d. Federal Trade Commission v. Facebook, Inc.

In *Federal Trade Commission v. Facebook, Inc.*, the court held that the FTC sufficiently alleged a claim that Facebook maintained a monopoly in social networking services in violation of section 2 of the Sherman Act by acquiring competitors and potential competitors.[210] The FTC sued for injunctive relief aimed at preventing the alleged unlawful conduct in the future as well as divestment of assets to restore the competition that would have existed absent the alleged unlawful conduct.[211] Although the complaint did not focus on Facebook's data collection and data use practices, the FTC identified that Facebook's acquisitions of applications like Instagram and WhatsApp had an anticompetitive effect, leading to "poorer services and less choice for consumers."[212] The consumer harms included, but were not limited to, "decreased privacy and data protection, excessive advertisements and decreased choice and control with regard to ads, and a general lack of consumer choice in the market for such services."[213]

Klein, *Brown*, *Brooks*, and *FTC v. Facebook* demonstrate that courts will readily hear privacy harm claims framed as antitrust cases. However, since the litigation is still working through the courts, a more powerful tool is needed to protect consumers now.

III. THE FTC SHOULD ENFORCE LARGE-SCALE PRIVACY VIOLATIONS

Due to the sheer scale and ubiquitous nature of the privacy violations and the resulting harms, the Federal Trade Commission must aggressively enforce

206. *Id.* at *8.
207. *Id.* at *9.
208. *Id.* at *11.
209. *Id.*
210. Fed. Trade Comm'n v. Facebook, Inc., 581 F. Supp. 3d 34, 65 (D.D.C. 2022).
211. *Id.* at 42.
212. *Id.* at 55.
213. *Id.*

anticompetitive and unfair competition laws tech companies that engage in harmful data collection practices. Private litigation, with its narrow set of claims, is simply not a powerful enough tool to prevent future harms. If the FTC does not label corporate data collection practices as inherently deceptive, then consumers will unwittingly consent to them. Successful, aggressive FTC enforcement will both increase injunctions to prevent future privacy harms and rebuild trust in government institutions.[214]

The FTC has an explicit Congressional mandate to protect the public from deceptive or unfair business practices and from unfair methods of competition.[215] This is a broad delegation of authority. The legislative history of the Federal Trade Commission Act demonstrates that the FTC's authority is "evolutionary and wide-reaching" such that the agency has extensive data protection enforcement authority.[216] The FTC has consumer protection jurisdiction over deceptive and unfair practices, which include (but are not limited to) "broken promises of privacy and data security, deceptive action to induce the disclosure of information, and failure to give sufficient notice of privacy invasive practices."[217] Congress has already recognized that "[f]orceful agency action is critical" to ensure that digital markets remain open and fair.[218] The FTC not only has the authority to adjudicate whether data security practices are unfair through the Federal Trade Commission Act, but also to successfully change privacy practices.[219] This includes a data minimization component, which would limit a tech company's ability to collect and retain data only for a necessary purpose, and reinforce the right to be forgotten or avoid being profiled.[220] Ultimately, this would allow individuals greater control and leverage over their personal information.

Moreover, the FTC can bolster antitrust enforcement through participatory rulemaking. Rohit Chopra and Lina Kahn argue that rulemaking is especially apt in two specific scenarios: in situations where there exists an extensive

214. The scope of the FTC's authority may not be affected should the Supreme Court overturn the *Chevron* doctrine of agency deference. In Chevron U.S.A., Inc. v. Nat. Res. Def. Council, Inc., 467 U.S. 837, 843 (1984), the Supreme Court held that when a statute is "silent or ambiguous with respect to the specific issue, the question for the court is whether the agency's answer is based on a permissible construction of the statute." *See* Gus Hurwitz, Chevron *and Administrative Antitrust, Redux*, 30 GEO. MASON. L. REV. 972, 997 (2023). Hurwitz analyzes that the Court may accept administrative antitrust by the FTC if the FTC will "lend greater stability to industry understanding of antitrust norms and incorporate advances in economic knowledge into the law more smoothly than the judiciary can." *Id.* On the other hand, if the FTC aggressively disrupts "long-standing antitrust principles," the Court may limit FTC authority. *Id.* at 999.

215. Rohit Chopra & Lina M. Khan, *The Case for "Unfair Methods of Competition" Rulemaking*, 87 U. CHI. L. REV. 357, 363–64 (2020); *Mission*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/mission (last visited June 20, 2024).

216. Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2246 (2015).

217. *Id.* at 2247.

218. H.R. REP. NO. 47-832, at 2 (2022).

219. *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 585 (2014).

220. Stucke, *supra* note 12, at 762.

enforcement record and in situations where private litigation is unlikely to deter anticompetitive conduct.[221] The litigation impacting syndicate tech corporations fits precisely into the second category.

In a press conference in August of 2022, FTC Chair Lina Khan affirmatively addressed the minimal deterrence of case-by-case enforcement actions, recognizing that "the growing and continuing digitization of our economy means that [privacy violations and data security breaches] may be prevalent and that case-by-case enforcement may fail to adequately deter law breaking or remedy the resulting harms."[222] In 2019, the Department of Justice and Federal Trade Commission settled a case with Facebook for an unprecedented $5 billion civil penalty and promises to implement privacy compliance measures.[223] However, privacy litigation is unlikely to deter the anticompetitive conduct of tech companies because of the privacy self-management regime. Companies only need to change a clause in their privacy policy to ameliorate plaintiffs.

Critics of FTC enforcement state that tech companies should be regulated through private actions and market economics,[224] worrying that increased FTC enforcement will impede industry and innovation.[225] Furthermore, it was the FTC's acquiescence of the industry-led notice and choice framework that (at least in part) led to the society-wide privacy harms.[226]

Yet "humility" and acquiescence to the "active steps" taken by social media companies is not the answer to the total degradation of online individual autonomy, as Ashutosh Bhagwat suggests.[227] Nor will FTC enforcement impede industry and innovation; Google's and Meta's anticompetitive practices are capable of slowing down the development of new technologies all on their own.[228] Aggressive FTC enforcement is vital because companies cannot be trusted to self-govern to protect consumers' privacy interests. For advertising-based companies such as Google and Meta, their business model *relies* on the

221. Chopra & Khan, *supra* note 215, at 371–72; *Mission*, *supra* note 215.

222. WSJ News, *FTC Boosts Digital Privacy Protection Efforts | WSJ Tech News Briefing*, YOUTUBE, at 00:47 (Aug. 12, 2022), https://www.youtube.com/watch?v=TEVvFX_ESbM.

223. *Facebook Agrees to Pay $5 Billion and Implement Robust New Protections of User Information in Settlement of Data Privacy Claims*, OFF. OF PUB. AFFS., U.S. DEP'T OF JUST. (July 24, 2019), https://www.justice.gov/opa/pr/facebook-agrees-pay-5-billion-and-implement-robust-new-protections-user-information; Lesley Fair, *FTC's $5 Billion Facebook Settlement: Record-Breaking and History-Making*, FED. TRADE COMM'N (July 24, 2019), https://www.ftc.gov/business-guidance/blog/2019/07/ftcs-5-billion-facebook-settlement-record-breaking-and-history-making.

224. Hartzog & Solove, *supra* note 216, at 2276.

225. James C. Cooper, *Privacy and Antitrust: Underpants Gnomes, the First Amendment, and Subjectivity*, 20 GEO. MASON L. REV. 1129, 1129 (2013).

226. Richards & Hartzog, *supra* note 20, at 1–2.

227. Bhagwat, *supra* note 101, at 2402.

228. *See* Hard Fork, *BONUS: Hard Fork Live! Big Tech's Arch Nemesis + Bot or Not?*, N.Y. TIMES (Mar. 20, 2023), https://www.nytimes.com/2023/03/20/podcasts/hard-fork-live-from-sxsw.html?showTranscript=1 (arguing that successful federal antitrust actions precede technological innovations).

sale of personal data for microtargeting purposes.[229] With a market cap of $1.353 trillion[230] and $534.10 billion[231] for Google and Meta, respectively, it is unlikely that digital advertising based companies will voluntarily change their data collection practices.[232] Critically, "security and privacy directly contradict Meta's business model."[233] Together, Meta and Google had a 90 percent growth in the digital advertising space from 2017 to 2018[234]—so much so that Google's digital advertising practices could plausibly be monopolistic.[235] Their pervasive user tracking practices across digital infrastructure gives them a "360-degree view of use activity."[236] Tech companies are not stupid. They can see the writing on the wall and know that increased enforcement through either litigation or otherwise is a ticking time bomb aimed at their pervasive data tracking practices. They are unlikely to preemptively blow up their business model before being compelled to do so by court injunction.

Private and federal litigation are complementary. Aggressive FTC enforcement will not subsume private litigation because "[p]rivate litigation is a democratizing force in antitrust."[237] Spencer Weber Waller argues that private litigation gives individuals the agency to pursue their own remedies when they have been wronged in a court of law, regardless of whether the government pursues such an action.[238] Private litigation also advances the jurisprudence of an issue because multiple parties are able to advance different theories of liability, causes of action, defenses, and immunities.[239] Most importantly for democratic institutions, private litigation can bring stability to the judicial system because tribunals can apply the appropriate law without even the appearance of political coercion.[240] As Waller acutely observes, "private rights of action are an additional venue to maintain democracy in competition law."[241] Parallel litigation provides individuals an opportunity to be compensated for privacy harms, may force corporate syndicates like Meta to adapt their business model, and can help rebuild trust in our democratic institutions.[242]

229. Bhagwat, *supra* note 101, at 2359.

230. *Market Capitalization of Alphabet (Google) from 2014–2024*, COMPANIESMARKETCAP, https://companiesmarketcap.com/alphabet-google/marketcap (last visited June 20, 2024).

231. *Market Capitalization of Meta Platforms (Facebook) from 2012–2024*, COMPANIESMARKETCAP, https://companiesmarketcap.com/meta-platforms/marketcap (last visited June 20, 2024).

232. Bhagwat, *supra* note 101, at 2359.

233. Sean Illing, *Why We Can't Trust Facebook to Police Itself*, VOX (Apr. 11, 2018, 6:52 AM PDT), https://www.vox.com/2018/3/21/17146674/zuckerberg-hearing-facebook-cambridge-analytica.

234. *Id.*

235. *See* In re Google Digit. Advert. Antitrust Litig., 627 F. Supp. 3d 346, 361 (S.D.N.Y. 2022).

236. Illing, *supra* note 233.

237. Harry First & Spencer Weber Waller, *Antitrust's Democracy Deficit*, 81 FORDHAM L. REV. 2543, 2545 (2013).

238. Waller, *supra* note 140, at 844.

239. *Id.*

240. *Id.*

241. *Id.*

242. Illing, *supra* note 233.

CONCLUSION

Consumers cannot maintain informational autonomy online because tech companies like Meta and Google have denigrated privacy protections, enabled by their consolidation of significant power in digital markets. Under the privacy self-management regime, individuals are left without agency to control their own personal data. It denies individuals the opportunity to protect their personal autonomy online. The mass collection of personal information by a limited number of tech companies creates a digital gerrymander, amplifies social inequality, and erodes trust in democratic institutions, and the overwhelming market share that tech companies hold jeopardizes the free flow of information online. Given the societal level ramifications of consolidated digital markets on consumers, antitrust laws are the appropriate mechanism to remedy privacy harms and rebuild the guardrails of privacy protections. Aggressive federal enforcement of current unfair competition and antitrust laws by the Federal Trade Commission is the most successful path forward for consumers who have had their personal information misappropriated and will rebuild trust in democratic institutions.

Every election cycle, American voters are told that it is the most important election of their lifetime because their personal autonomy is at stake. Rather than wait for legislators to enact privacy protection statutes, both private plaintiffs and federal regulators should bring antitrust actions against large tech companies based on privacy misrepresentations and allow consumers the opportunity to demand privacy protections from digital markets.