



DATE DOWNLOADED: Thu Jan 18 11:14:04 2024

SOURCE: Content Downloaded from [HeinOnline](#)

Citations:

Please note: citations are provided as a general guideline. Users should consult their preferred citation format's style manual for proper citation formatting.

Bluebook 21st ed.

Mason Marks, Biosupremacy: Big Data, Antitrust, and Monopolistic Power over Human Behavior, 55 UC DAVIS L. REV. 513 (2021).

ALWD 7th ed.

Mason Marks, Biosupremacy: Big Data, Antitrust, and Monopolistic Power over Human Behavior, 55 UC Davis L. Rev. 513 (2021).

APA 7th ed.

Marks, Mason. (2021). Biosupremacy: big data, antitrust, and monopolistic power over human behavior. UC Davis Law Review, 55(1), 513-590.

Chicago 17th ed.

Mason Marks, "Biosupremacy: Big Data, Antitrust, and Monopolistic Power over Human Behavior," UC Davis Law Review 55, no. 1 (November 2021): 513-590

McGill Guide 9th ed.

Mason Marks, "Biosupremacy: Big Data, Antitrust, and Monopolistic Power over Human Behavior" (2021) 55:1 UC Davis L Rev 513.

AGLC 4th ed.

Mason Marks, 'Biosupremacy: Big Data, Antitrust, and Monopolistic Power over Human Behavior' (2021) 55(1) UC Davis Law Review 513

MLA 9th ed.

Marks, Mason. "Biosupremacy: Big Data, Antitrust, and Monopolistic Power over Human Behavior." UC Davis Law Review, vol. 55, no. 1, November 2021, pp. 513-590.
HeinOnline.

OSCOLA 4th ed.

Mason Marks, 'Biosupremacy: Big Data, Antitrust, and Monopolistic Power over Human Behavior' (2021) 55 UC Davis L Rev 513 Please note: citations are provided as a general guideline. Users should consult their preferred citation format's style manual for proper citation formatting.

-- Your use of this HeinOnline PDF indicates your acceptance of HeinOnline's Terms and Conditions of the license agreement available at

<https://heinonline.org/HOL/License>

-- The search text of this PDF is generated from uncorrected OCR text.

-- To obtain permission to use this article beyond the scope of your license, please use:
[Copyright Information](#)

Biosupremacy: Big Data, Antitrust, and Monopolistic Power Over Human Behavior

Mason Marks*

Since 2001, five leading technology companies have acquired more than 600 other firms while avoiding antitrust enforcement. By accumulating technologies in adjacent or unrelated industries, these companies have grown so powerful that their influence over human affairs equals that of many governments. Their power stems from data collected by devices that people welcome into their homes, workplaces, schools, and public spaces. When paired with artificial intelligence, these devices form a vast surveillance network that sorts people into increasingly specific categories related to health, sexuality, religion, and other categories. However, this surveillance network was not created solely to observe human behavior; it was also designed to exert control. Accordingly, it is paired with a second network that leverages intelligence gained through surveillance to manipulate people's behavior, nudging them through personalized newsfeeds, targeted advertisements, dark patterns, and other forms of coercive choice architecture. Together, these dual networks of surveillance and control form a global digital panopticon, a modern analog of Bentham's eighteenth-century building designed for total surveillance. Moreover, they enable a pernicious type of influence that Foucault defined as biopower: the ability to measure and modify the behavior of populations to shift social norms.

* Copyright © 2021 Mason Marks. Assistant Professor, University of New Hampshire Franklin Pierce School of Law; Senior Fellow and Project Lead of POPLAR, Petrie-Flom Center, Harvard Law School; Affiliated Fellow, Information Society Project, Yale Law School. Thanks to Jack Balkin and Fiona Scott Morton for including this article in the Big Tech and Antitrust Conference at Yale Law School. Thanks to Frank Pasquale, Katherine Strandburg, Danielle Allen, Michael Abramowicz, Ari Waldman, James Puckett, and Thomas Kadri for their comments. The article benefited from feedback at NYU Law School's Privacy Research Group, the Northeast Privacy Scholars Workshop at Northeastern University, the Edmond J. Safra Fellow's Workshop at Harvard, and the Rocky Mountain Junior Scholars Workshop at the University of Utah.

This Article is the first to introduce biopower into antitrust doctrine. It contends that a handful of companies are vying for a dominant share of biopower to achieve biosupremacy, monopolistic power over human behavior. The Article analyzes how companies concentrate biopower through unregulated conglomerate and concentric mergers that add software and devices to their surveillance and control networks. Acquiring technologies in new markets establishes cross-market data flows that send information to acquiring firms across market boundaries. Conglomerate and concentric mergers also expand the control network, establishing beachheads from which platforms exert biopower to shift social norms.

Antitrust regulators should expand their conception of consumer welfare to account for the costs imposed by surveillance and coercive choice architecture on product quality. They should revive conglomerate merger control, abandoned in the 1970s, and update it for the Digital Age. Specifically, regulators should halt mergers that concentrate biopower, prohibit the use of dark patterns, and mandate data silos, which contain data within specific markets, to block cross-market data flows.

TABLE OF CONTENTS

INTRODUCTION	515
I. BUILDING THE DIGITAL PANOPTICON	524
A. <i>Omniscience and Obedience: The Inspection House and Disciplinary Power</i>	525
B. <i>From Prisons to Platforms: Panoptic Surveillance in the Digital Age</i>	529
C. <i>Choice Architecture: From Gentle Nudges to Coercive Dark Patterns</i>	532
D. <i>Case Studies of Digital Biopower</i>	537
1. Shaping Online Speech Norms.....	538
2. Shaping Public Health Norms.....	541
3. Shaping Educational Norms.....	543
E. <i>Totalitarian Data Mining</i>	544
1. The Selfish Ledger	544
2. The Threat of Data Fascism	547
II. THE DECLINE OF ANTITRUST AND THE RISE OF DATA CONGLOMERATES	553
A. <i>The Need to Regulate Data Conglomerates</i>	553
B. <i>Antitrust's Original Mandate to Constrain Private Power</i> ..	555
C. <i>The Rise and Fall of Conglomerate Merger Control</i>	558
D. <i>The Emergence of Data Conglomerates and Digital Biopower</i>	561
E. <i>The Role of Neo-Brandeisian Antitrust</i>	568

III.	UPDATING ANTITRUST TO REGULATE DIGITAL BIOPOWER	572
A.	<i>Maximizing Consumer Welfare by Minimizing Surveillance and Behavioral Profiling</i>	575
1.	Data Volume (V)	575
2.	Time Interval (T).....	576
3.	Data Sensitivity (S)	576
4.	Deception During Data Collection (D)	576
5.	Enrichment of Data (E)	577
6.	Refinement of Data (R)	577
B.	<i>Increasing Competition and Product Quality by Restricting Panoptic Surveillance and Coercive Choice Architecture.....</i>	578
C.	<i>Breaching Walled Gardens with Data Portability and Platform Interoperability</i>	579
1.	The Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act.....	582
2.	The Consumer Online Privacy Act (COPRA).....	583
D.	<i>Inhibiting Coercive Choice Architecture.....</i>	584
E.	<i>Revitalizing Merger Control to Block Cross-Market Data Flows, Minimize Coercive Choice Architecture, and Prevent Biosupremacy</i>	586
1.	Structural Remedies	586
2.	Behavioral Remedies.....	587
	CONCLUSION.....	588

INTRODUCTION

On February 28, 2020, Nobel Prize winning economist Paul Romer spoke at an antitrust conference at the NYU School of Law. He asked the audience, “How many think it’s possible for [Mark] Zuckerberg to tip the outcome of the election if he were to decide to do that?” After pausing for a show of hands, Romer continued, “there is nothing that constrains what he can do,” because “this is a level of concentrated power in the hands of one person that I’m not sure we’ve ever seen anywhere in history. And whatever his intentions are, whatever kind of a person he is, we should never have allowed this to happen.”¹

¹ NYU School of Law, *Monopolization and Abuse: Application to Platforms and Digital Markets*, YOUTUBE (May 12, 2020), <https://www.youtube.com/watch?v=XSSGaQ9xwd8&list=PLvLK5ZuczSArx6VwX6a-bKUZsEJEOSilh&tindex=20> [<https://perma.cc/S57N-75L4>].

Nine months later, New York Attorney General Letitia James announced two historic suits against Facebook.² “No company should have this much unchecked power over our personal information and our social interactions,” said James.³ Her declaration followed earlier actions by U.S. and E.U. regulators against Google and Amazon.⁴ These developments were triggered by an alarming trend. Since 2001, five leading technology companies have avoided antitrust enforcement to complete over 600 mergers.⁵ Through uncontested acquisitions, they have dominated markets, eliminated rivals, and grown so powerful that their influence over human affairs equals that of many governments.⁶ Accordingly, lawmakers, scholars, and antitrust regulators increasingly call for restraints on their power.⁷

Despite good intentions and lofty rhetoric, many proposed solutions focus narrowly on tech company behavior within individual markets such as social media and advertising. These market-centric approaches overlook the source of tech firms’ most flexible and dangerous power: the ability to monitor billions of people, nudge their behavior through personalized choice architecture, and shift it toward norms that tech companies establish.⁸ Philosopher Michel Foucault called the ability to manipulate populations *biopower*.⁹ The prefix *bio* refers not only to

² N.Y. Attorney General Asks Courts to Take Action Against Facebook, N.Y. TIMES (Dec. 9, 2020), <https://www.nytimes.com/video/us/politics/100000007495190/new-york-attorney-general-facebook-antitrust.html> [https://perma.cc/CE3D-SBKG].

³ *Id.*

⁴ See John D. McKinnon, *Facebook, Google to Face New Antitrust Suits in U.S.*, WALL ST. J. (Nov. 30, 2020, 10:08 AM ET), <https://www.wsj.com/articles/facebook-google-to-face-new-antitrust-suits-in-u-s-11606742163> [https://perma.cc/RL2S-6HPF].

⁵ See JOHN KWOKA, CONTROLLING MERGERS AND MARKET POWER: A PROGRAM FOR REVIVING ANTITRUST IN AMERICA 109 (2020) (listing acquisitions by Google, Amazon, Facebook, Apple, and Microsoft).

⁶ See Marjorie Heins, *The Brave New World of Social Media Censorship*, 127 HARV. L. REV. F. 325, 325 (2014) (describing how Facebook wields more power over speech than any king or president); see also Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598, 1603 (2018) (describing how internet platforms serve as the new governors of online speech).

⁷ See, e.g., Lina M. Khan, *Amazon’s Antitrust Paradox*, 126 YALE L.J. 710, 802-05 (2017) (arguing for antitrust reform to restrain the powers of dominant internet platforms like Amazon); see also TIM WU, THE CURSE OF BIGNESS: ANTITRUST IN THE NEW GILDED AGE 14-23 (2018).

⁸ See Cass R. Sunstein, *The Ethics of Nudging*, 32 YALE J. ON REGUL. 413, 433 (2015) (describing how nefarious nudges and choice architecture can threaten human welfare, dignity, autonomy, and democracy).

⁹ 1 MICHEL FOUCault, THE HISTORY OF SEXUALITY 130 (1978) (describing biopower as the ability to measure, appraise, and hierarchize populations affecting their distribution around social norms).

biological processes, but to all aspects of life, including its social, occupational, and psychological dimensions.

This Article is the first to introduce the concept of biopower into antitrust policy. It merges the goals and principles of antitrust regulation with concepts and vocabulary from data protection law, behavioral economics, and Foucault's biopolitics to analyze how firms exert power over populations. Though many areas of law would benefit from incorporating biopower into legal doctrine, this Article focuses on antitrust. It contends that Congress, courts, and regulators should incorporate biopower into antitrust regulation for three reasons. First, *digital biopower* is an unprecedented form of concentrated private influence, and restraining private power was the original goal of U.S. antitrust law, as reflected in the legislative history of the Sherman Antitrust Act of 1890.¹⁰ Furthermore, antitrust enforcement was directed toward this goal for over eighty years, during which courts, legislators, and federal agencies accepted that concentrated private power harms individuals, competition, society, and democracy.¹¹

Second, digital biopower can be transformed into other forms of influence including market power and political power making it a source from which other forms of coercive influence spring. Third, analyzing biopower is useful to antitrust scholars and regulators regardless of their theoretical orientation. Disciples of the Neo-Brandeisian School of Antitrust should analyze biopower because its concentration harms competition and product quality, erects barriers to entry, displaces small firms, and threatens social, political, and economic liberty.¹² However, even less progressive antitrust scholars should incorporate biopower into their analyses because its concentration raises costs to consumers, suppresses competition, and restrains innovation.

In 2021, leading technology companies operate vast surveillance networks that collect data on billions of people. These networks are composed of internet-enabled devices containing cameras, microphones, accelerometers, and other sensors that collect data on

¹⁰ See, e.g., Zephyr Teachout & Lina Khan, *Market Structure and Political Law: A Taxonomy of Power*, 9 DUKE J. CONST. L. & PUB. POL'Y 37, 61-62 (2014) (discussing Congressional motivation behind the Sherman Act's passage); see also Carl T. Bogus, *The New Road to Serfdom: The Curse of Bigness and the Failure of Antitrust*, 49 U. MICH. J.L. REFORM 1, 42-51 (2015).

¹¹ See Zephyr Teachout, *Antitrust Law, Freedom, and Human Development*, 41 CARDozo L. REV. 1081, 1089 (2019).

¹² See Khan, *supra* note 7, at 743 (listing Neo-Brandeisian policy goals); see also Wu, *supra* note 7, at 127-39.

people's faces, voices, movements, social behavior, and physiology. Surveillance networks also rely on software that monitors users as they navigate apps and websites, consume news and entertainment, and communicate with other people. Internet-enabled devices and software serve as *sensing units* that collect user data and send it to tech company servers for storage and analysis by artificial intelligence ("AI"). Machine learning, a form of AI that excels at drawing inferences, profiles people to sort them into increasingly specific categories, often related to sensitive topics such as mental health, which form the basis of surveillance-based economies.¹³ Together, platform AI and sensing units form the *sensing net*, one half of an elaborate system that generates biopower.

Because technology companies aim to influence people in addition to observing and analyzing them, the sensing net is paired with a parallel network of influence, the *control net*, which is composed of *motor units*.¹⁴ Instead of monitoring people and transmitting data about them to platform servers, motor units receive information from the sensing net and interact with people to influence their behavior.¹⁵ Motor units include speakers, electric motors that make phones vibrate and robots move, digital human voices that engage people in simulated conversations, and graphical user interfaces that convey messages and images to users. Motor units are often embedded in the same devices that contain sensing units such as smartphones, laptops, wearables, and smart speakers.

The sensing net generates knowledge in the form of behavioral inferences and predictions, which the control net utilizes to manipulate groups and individuals, bending their wills and actions to align with the goals of platform architects.¹⁶ The control net influences behavior

¹³ See JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATION CAPITALISM 57 (2019) (describing the surprisingly varied and granular data collected by mobile devices and their networked sensors); FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 25-32 (2015) (describing the scored society of the United States in which secret algorithms make inferences about people to profile, sort, and penalize them).

¹⁴ See SHOSHANNA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 8 (2019) (describing how competitive pressures motivated platforms to shift from merely observing consumer behavior to controlling it).

¹⁵ See, e.g., Kjerstin Thorson, Kelley Cotter, Mel Medeiros & Chankyoung Pak, *Algorithmic Inference, Political Interest, and Exposure to News and Politics on Facebook*, INFO., COMM&C'N. & SOC'Y 1, 3 (2019) (describing how Facebook delivers customized news and political content to users based on inferences drawn by its algorithms).

¹⁶ See, e.g., Yafit Lev-Aretz, *Facebook and the Perils of a Personalized Choice Architecture*, TECHCRUNCH (Apr. 24, 2018, 3:30 PM PDT), <https://techcrunch.com/>

through nudges administered by manipulative technologies such as customized search results and news feeds, personalized notifications, targeted advertisements, dark patterns, and other forms of coercive choice architecture.¹⁷

The sensing and control nets form a dynamic system that constantly adapts to user behavior.¹⁸ While motor units nudge people's behavior, sensing units monitor their effectiveness and modify the control net's nudges to increase their impact.¹⁹ In this manner, through continuous cycles of sensing and control, tech companies exert biopower, nudging people to conform their behavior to norms that they establish. Unlike norms created by governments of elected representatives, platform norms are often created in secret by unelected corporate leaders.²⁰

When firms acquire a dominant share of biopower, influencing enough traits in sufficiently large populations, they achieve biosupremacy, which this Article defines as monopolistic power over human behavior. Biosupremacy is a Digital Age analog of monopoly power.²¹ While monopoly power gives firms the ability to raise prices and exclude competitors within specific markets, biosupremacy enables firms to exert control, by shifting social norms over large swaths of human behavior, yielding influence that cuts across markets and entire

2018/04/24/facebook-and-the-perils-of-a-personalized-choice-architecture/ [https://perma.cc/FKE2-CYZE] (describing how information from different sources is combined to design personalized choice architecture that subconsciously nudges people to modify their behavior).

¹⁷ See *id.*; Thorson et al., *supra* note 15, at 3; Ari Ezra Waldman, *Cognitive Biases, Dark Patterns, and the Privacy Paradox*, 31 CURRENT OP. PSYCHOLOGY 105, 105 (2020) (describing how internet platforms exploit people's cognitive biases and deploy dark patterns, "design tricks platforms use to manipulate users into taking actions they might otherwise have not" to "weaponize the design of built online environments to harm consumers and their privacy").

¹⁸ See Jonas Kaiser & Adrian Rauchfleisch, *Birds of a Feather Get Recommended Together: Algorithmic Homophily in YouTube's Channel Recommendations in the United States and Germany*, 6 SOC. MEDIA & SOC'Y 1, 10 (2020) (explaining how YouTube's algorithms continuously sense what viewers are watching and provide them with similar content, which can drive users toward extreme or misleading content).

¹⁹ See *id.*

²⁰ See Robert Gorwa, Reuben Binns & Christian Katzenbach, *Algorithmic Content Moderation: Technical and Political Challenges in the Automation of Platform Governance*, 7 BIG DATA & SOC'Y 1, 10 (stating that "content moderation has long been a famously opaque and secretive process").

²¹ See *Monopolization Defined*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/competition-guidance/guide-antitrust-laws/single-firm-conduct/monopolization-defined (last visited Dec. 29, 2020) [https://perma.cc/TYL5-U488] (defining a monopolist as a firm with significant and durable market power characterized by the long-term ability to raise prices or exclude competitors).

industries.²² When a single entity achieves biosupremacy, it becomes a *bio-monopoly*, and when a small number of firms attain it, they constitute a *bio-oligopoly*. Moreover, while monopolies are created through horizontal and vertical mergers, biopower is often cemented through conglomerate or concentric mergers.²³

Conglomerate mergers combine firms in different industries or different geographic regions, and concentric mergers involve firms whose products are related to some extent, for example, with respect to how they are produced, used, or marketed.²⁴ Both types of mergers allow acquiring firms to expand into new sectors, extending their portfolios of sensing and control units, and bolstering their capacity to generate and exert biopower. However, conglomerate and concentric mergers typically fly under the radar of antitrust agencies.²⁵ A timely example is Google's recent acquisition of wearable maker FitBit.²⁶ Through the merger, Google entered the wearables market and gained sensing and motor units embedded in FitBit devices, including its new *Sense* smartwatch, which contains sensors for monitoring skin temperature, heart rate, respiration rate, oxygen saturation, and

²² See *id.*; see also BARRY C. LYNN, LIBERTY FROM ALL MASTERS: THE NEW AMERICAN AUTOCRACY VS. THE WILL OF THE PEOPLE 53 (2020) (describing how dominant technology companies have reorganized entire spheres of human activity and aspire to control additional corners of society).

²³ See Steven C. Salop, *Invigorating Vertical Merger Enforcement*, 127 YALE L.J. 1962, 1971-72 (2018) (arguing for the revival of vertical merger regulation because vertical mergers, like horizontal mergers, intrinsically harm competition and promote monopoly).

²⁴ See Junmao Chiu, Huimin Chung & Yi-Ning Yang, *The Impact of Conglomerate Merger on its Vendors and Rivals – a Case Study of Google's Acquisition of Motorola*, 28 TECH. ANALYSIS & STRATEGIC MANAGEMENT 176, 176 (2015) (defining conglomerate merger); see Samuel R. Reid, *The Conglomerate Merger: A Special Case*, 2 ANTITRUST L. & ECON. REV. 141, 145 (1968) (defining concentric merger).

²⁵ See Robert H. Lande, *The U.S. Needs Conglomerate Merger Legislation*, CLS BLUE SKY BLOG (Jan. 23, 2019), <https://clsbluesky.law.columbia.edu/2019/01/23/the-u-s-needs-conglomerate-merger-legislation/> [https://perma.cc/8FLV-NYX2] (stating that conglomerate mergers are almost always permitted by U.S. antitrust agencies); see also NYU School of Law, *Legislative Reform: What Changes for Antitrust Law and Institutions*, YOUTUBE (Feb. 28, 2020), https://www.youtube.com/watch?v=7Dz9-jOKEPA&ab_channel=NYUSchoolofLaw [https://perma.cc/V7U9-H32F] (Diana Moss, President of the American Antitrust Institute, stating that modern antitrust law does not address concentric mergers).

²⁶ Brian Heater, *Google is Acquiring Fitbit for \$2.1 Billion*, TECHCRUNCH (Nov. 1, 2019, 6:06 AM PDT), <https://techcrunch.com/2019/11/01/google-is-acquiring-fitbit/> [https://perma.cc/EV8G-5CS6].

galvanic skin response.²⁷ These sensing units can send data across market boundaries from FitBit devices to Google's central servers. Once Google's AI has analyzed the information to profile FitBit users, it can send motor impulses back to their devices, nudging them to alter their behavior.²⁸

What makes biopower so versatile is that sensing units in one sector can be paired with motor units in another. For instance, sensing units in FitBit devices can generate intelligence that influences behavior in seemingly unrelated markets in which Google participates such as targeted advertising, video streaming, home automation, and internet search.²⁹ In other words, companies can leverage cross-market data flows to exert biopower in numerous markets, providing unprecedented influence over many spheres of human activity. Some antitrust scholars and regulators seem to comprehend the significance of this power.³⁰ However, they lack the vocabulary to adequately characterize it and the theoretical framework to operationalize it, which is the contribution of this Article.

On December 17, 2020, the European Commission announced its approval of the Google-FitBit merger, subject to behavioral antitrust remedies.³¹ However, because the remedies focus narrowly on the markets for wearables and advertising, they overlook Google's ability to leverage data flows from the wearables market to exert power in sectors other than advertising. Moreover, the remedies ignore Google's ability

²⁷ See John D. Stoll, *Inside Fitbit's Quest to Be Your Health Monitor; Fitbit CEO James Park Discusses the Company's New Products and Competition as It Prepares to Close Its Acquisition by Google*, WALL ST. J. (Oct. 24, 2020), <https://www.wsj.com/articles/inside-fitbits-quest-to-be-your-health-monitor-11603540800> [https://perma.cc/RAX4-33VZ].

²⁸ See Afsaneh Doryab, Daniella K. Villalba, Preerna Chikarsal, Janine M. Dutcher, Michael Tumminia, Xinwen Liu, Sheldon Cohen, Kasey Creswell, Jennifer Mankoff, John D. Creswell & Anind K. Dey, *Identifying Behavioral Phenotypes of Loneliness and Social Isolation with Passive Sensing: Statistical Analysis, Data Mining and Machine Learning of Smartphone and Fitbit Data*, 7 JMIR MHEALTH & UHEALTH 373, 387 (2019) (reporting that data collected from FitBit devices can be analyzed by artificial intelligence to "detect low and high levels of loneliness with high accuracy").

²⁹ See Natasha Lomas, *Europe Clears Google-Fitbit with a Ten-Year Ban on Using Health Data for Ads*, TECHCRUNCH (Dec. 17, 2020), <https://techcrunch.com/2020/12/17/europe-clears-google-fitbit-with-a-ten-year-ban-on-using-health-data-for-ads/> [https://perma.cc/DRK6-PDDB] (describing the potential for Google to user data derived from Fitbit users for purposes other than fitness tracking such as targeted advertising).

³⁰ See, e.g., N.Y. TIMES, *supra* note 2 (featuring statement by N.Y. Attorney General Letitia James regarding Facebook: "No company should have this much unchecked power over our personal information and our social interactions").

³¹ *Mergers: Commission Clears Acquisition of FitBit by Google, Subject to Conditions*, EUROPEAN COMM'N (Dec. 17, 2020), https://ec.europa.eu/competition/presscorner/detail/en/ip_20_2484 [https://perma.cc/HP6B-FLXC] [hereinafter *Mergers*].

to use data and intelligence from markets unrelated to wearables, such as search and home automation, to influence users in the wearables space. Incorporating principles of biopower and data protection into antitrust scholarship will help bridge the gap between regulators' ambitious goals of restraining tech company power and their lackluster record of antitrust enforcement.

Instead of focusing solely on tech firms' absolute size or "bigness," and advocating for their dissolution into smaller firms, this Article emphasizes *data conglomerate-bigness*, reflecting not only a firm's size but its diversification through the acquisition of networked software and devices in disparate markets and industries. Rather than focusing narrowly on individual markets such as advertising or social media, it emphasizes the acquisition of sensing and motor units that enable data and power to flow across market boundaries. It argues that antitrust regulators should expand their view of the digital landscape to visualize cross-market data flows and the anticompetitive behaviors that create and leverage them. This novel approach to antitrust regulation should be a supplement to, instead of a replacement for, other proposed antitrust reforms that revitalize merger control.³² Moreover, though antitrust laws are an important means of regulating Big Tech's power, they are not the only mechanism. Other fields such as data protection regulation and consumer protection law must play supporting roles, and they too will benefit from analyzing cross-market data flows, biopower, and biosupremacy.

Regulating biopower is important because when private companies exert it to shape social norms, some groups will inevitably be considered abnormal and deprived of social, occupational, and political opportunities.³³ Legal safeguards such as the Bill of Rights, which shield people from government abuse of power, do not apply to corporations, creating a need for mechanisms that disperse concentrated private biopower.³⁴ Just as the Constitution and the Bill of Rights restrain public power, antitrust should restrain overconcentrated private influence.³⁵ Failure to use antitrust in this manner, as prescribed by its original mandate, leaves private biopower unopposed.

³² See, e.g., Wu, *supra* note 7, at 127-29 (arguing for a renewed focus on merger review in U.S. antitrust policy).

³³ See, e.g., Mason Marks, *Algorithmic Disability Discrimination*, in *DISABILITY, HEALTH, LAW AND BIOETHICS* 242, 243 (I. Glenn Cohen et al. eds., 2019) (describing how Facebook hid housing-related ads from people its algorithms identified as belonging to certain faiths, races, or groups with disabilities).

³⁴ See Wu, *supra* note 7, at 138.

³⁵ See *id.*

This Article proceeds in three parts. Part I defines biosupremacy and explains how dual networks of sensing and control form a global digital panopticon, a modern analog of Jeremy Bentham's eighteenth-century panoptic edifice. It argues that tech companies expand the digital panopticon through unregulated conglomerate and concentric mergers. Moreover, the Article describes how internet companies use surreptitious surveillance, deceptive dark patterns, and other forms of coercive choice architecture to nudge people to conform their behavior to norms they establish, shifting the behavior of populations, and inching the companies closer to biosupremacy. Part I presents three case studies that illustrate the use of biopower to shape social norms related to online speech, public health, and education. It concludes with a description of how concentrated biopower promotes totalitarianism.

Part II provides a brief history of U.S. antitrust doctrine and how its relationship with private power has evolved. It explains why existing antitrust tools are inadequate to constrain private biopower because they ignore its primary source: the panoptic architecture of internet platforms, the cross-market data flows it creates, and the coercive choice architecture it promotes. It analyzes how the rise of internet-enabled technologies within an antitrust enforcement vacuum created by the Chicago School promoted the consolidation of private biopower, which threatens competition, human autonomy, and democracy.

Part III makes recommendations for updating antitrust law to inhibit the concentration of private biopower and prevent biosupremacy. The proposals fall into two categories. The first set of recommendations should appeal to everyone because it addresses biopower through the lens of consumer welfare. This set of proposals argues that regulators should analyze the costs imposed on people by platform surveillance and maximize consumer welfare by minimizing data collection. Moreover, to promote competition and consumer welfare, regulators should maximize product quality by restricting digital surveillance, deception, and coercion.

The second set of proposals should appeal to proponents of the Neo-Brandeisian School. It argues for revitalizing merger control and incorporating data flows, biopower, and coercive choice architecture into merger review. Specifically, through structural and behavioral remedies, regulators should halt conglomerate and concentric mergers that expand sensing and control networks to concentrate biopower. To promote consumer autonomy, regulators should prohibit the use of dark patterns and implement data silos to block cross-market data flows. Moreover, to prevent platforms from locking consumers into panoptic walled gardens, which further concentrate biopower,

regulators should force tech companies to implement data portability and platform interoperability. Through these proposals, the Article builds on a Neo-Brandeisian foundation to reorient antitrust toward human values such as competition, economic liberty, and personal autonomy. However, it also expands upon the Neo-Brandeisian agenda by providing a novel framework for analyzing data flows and restraining tech company power.

I. BUILDING THE DIGITAL PANOPTICON

This Part frames the system comprising parallel networks of sensing and control as a global digital panopticon, a modern analog of Jeremy Bentham's eighteenth-century structure. Bentham envisioned a building designed for total surveillance that could house prisons, schools, hospitals, factories, and other institutions.³⁶ He believed it was the cure for many social problems.³⁷ Though few examples of the physical panopticon were built, the digital version is used in all the settings Bentham envisioned, and more.³⁸ Instead of occupying a building, it spans the globe.

The digital panopticon is an engine for generating and exerting biopower because it enables platforms to monitor billions of people, calculate statistics on their physical and psychological traits, and nudge them to conform their behavior to norms established by the platforms. In 2021, internet platforms routinely monitor millions of students, employees, patients, criminal suspects, and members of the public. Through nudges administered via the control net, they shift norms in diverse domains including work, hiring, education, healthcare, law enforcement, and communication.³⁹ The resulting influence, which

³⁶ JEREMY BENTHAM, PANOPTICON; OR, THE INSPECTION-HOUSE 2 (T. Payne) (1791).

³⁷ *Id.* at i ("Morals reformed — health preserved — industry invigorated instruction diffused — public burthens lightened — Economy seated, as it were, upon a rock — the gordian knot of the Poor-Laws are not cut, but untied — all by a simple idea in Architecture!" (describing the social benefits of the panopticon)).

³⁸ See, e.g., Sara Gerke, Serena Yeung & I. Glenn Cohen, *Ethical and Legal Aspects of Ambient Intelligence in Hospitals*, 323 JAMA 601 (2020) (describing the use of artificial intelligence to predict health information from people's behavior in hospitals); Todd Feathers, *Schools Spy on Kids to Prevent Shootings, but There's No Evidence It Works*, MOTHERBOARD (Dec. 4, 2019, 6:00 AM), https://www.vice.com/en_ca/article/8xwze4/schools-are-using-spyware-to-prevent-shootingsbut-theres-no-evidence-it-works [https://perma.cc/CCA2-343L] (describing the use of surveillance software and AI to predict school shootings).

³⁹ See, e.g., Ifeoma Ajunwa, *An Auditing Imperative for Automated Hiring Systems*, 34 HARV. J.L. & TECH. 1, 16 (describing the use of platforms such as HireVue, which use cameras, microphones, and AI to monitor and analyze job candidate speech, facial

touches nearly every sphere of human activity, is the type of pervasive power that antitrust law was originally designed to prevent.

The following Sections analyze the digital panopticon and its roots in earlier panoptic systems. They define biopower and biosupremacy, explain how the digital panopticon produces them, and analyze their social and economic harms.

A. *Omniscience and Obedience: The Inspection House and Disciplinary Power*

“It were to be wished that every man’s name were written upon his forehead as well as engraved upon his door. It were to be wished that no such thing as secrecy existed — that every man’s house were made of glass.”⁴⁰

Jeremy Bentham, Deontology

“We don’t need you to type at all. We know where you are. We know where you’ve been. We can more or less know what you’re thinking about.”⁴¹

Former Google CEO Eric Schmidt

In Bentham’s panopticon, a circular wall of cells surrounds a central guard tower called the inspection house. From the tower, guards (inspectors) observe the behavior of the panopticon’s inhabitants (prisoners). However, through the creative use of lighting and architecture, the prisoners cannot see the inspectors. This asymmetrical arrangement leads prisoners to believe that they are constantly being watched even if the tower is empty. As a result, they feel the presence of authority continuously even though they never know if or when they

expressions, and tone of voice); Lois Becket, *Under Digital Surveillance: How American Schools Spy on Millions of Kids*, GUARDIAN (Oct. 22, 2019, 1:00 AM EDT), <https://www.theguardian.com/world/2019/oct/22/school-student-surveillance-bark-gaggle> [https://perma.cc/8BGM-TR9P] (describing how platforms such as Gaggle, Bark, and GoGuardian collect data on millions of American students through internet-enabled software and devices); Adam Satariano, *How My Boss Monitors Me While I Work from Home*, N.Y. TIMES (May 6, 2020), <https://www.nytimes.com/2020/05/06/technology/employee-monitoring-work-from-home-virus.html> [https://perma.cc/WMJ3-YUE8] (describing how platforms such as Hubstaff monitor employees while they work from home).

⁴⁰ 1 JEREMY BENTHAM, DEONTOLOGY; OR, THE SCIENCE OF MORALITY 100 (John Bowring ed., 1834).

⁴¹ Derek Thompson, *Google’s CEO: ‘The Laws Are Written by Lobbyists,’* ATLANTIC (Oct. 1, 2010), <https://www.theatlantic.com/technology/archive/2010/10/googles-ceo-the-laws-are-written-by-lobbyists/63908/> [https://perma.cc/QH65-XY93].

are watched.⁴² Under constant threat of observation, prisoners internalize the inspectors' authority and learn to police themselves.⁴³

Bentham envisioned the panopticon being adapted for use in any setting where behavioral control is desired. He believed it would house schools, hospitals, and factories, and he stressed the importance of uninterrupted surveillance regardless of the application:

It is obvious that, in all these instances, the more constantly the persons to be inspected are under the eyes of the persons who should inspect them, the more perfectly will the purpose of the establishment have been attained. Ideal perfection, if that were the object, would require that each person should actually be in that predicament during every instant of time.⁴⁴

Bentham's panopticon fascinated Foucault, who saw it as a means of disciplining individuals and incorporating them into the machinery of production.⁴⁵ Foucault analyzed how power has evolved during the past five hundred years, and he identified three dominant forms: sovereign or "juridical" power, disciplinary power, and biopower.⁴⁶ Sovereignty bestows the power to kill people or let them live.⁴⁷ It is "the right of the sword" held by absolute monarchs.⁴⁸ Foucault argued that in the eighteenth and nineteenth centuries, a new type of power — biopower — augmented and largely replaced sovereign power.⁴⁹

Whereas sovereign power is the right to kill or let live, biopower is the right to make live and let die.⁵⁰ To illustrate the difference, consider that in pre-modern societies, monarchs routinely executed people. In contrast, modern governments prohibit people from ending their lives

⁴² MICHEL FOUCAULT, *DISCIPLINE AND PUNISH* 201 (1977).

⁴³ *Id.*

⁴⁴ 4 JEREMY BENTHAM, *THE WORKS OF JEREMY BENTHAM* 40 (John Bowring ed., 1843).

⁴⁵ FOUCAULT, *supra* note 42, at 200.

⁴⁶ FOUCAULT, *supra* note 9, at 122-30.

⁴⁷ MICHEL FOUCAULT, *From the Power of Sovereignty to Power Over Life*, in "SOCIETY MUST BE DEFENDED": LECTURES AT THE COLLÈGE DE FRANCE, 1975-76, at 240 (Arnold I. Davidson ed., David Macey trans., 1976).

⁴⁸ *See id.*

⁴⁹ FOUCAULT, *supra* note 9, at 124-25.

⁵⁰ Modern attitudes toward suicide and euthanasia are helpful for differentiating sovereign power from biopower. In times characterized by sovereign power, the state would not stop people from attempting suicide, and the state routinely executed citizens or allowed them to go on living, an exercise of sovereign power. In modern society, sovereign power is less often used, and citizens are rarely sentenced to death. However, most people lack the right to kill themselves or to die by physician assisted suicide. Those with biopower force them to live and hold the power to let them die.

or dying by physician-assisted suicide.⁵¹ The power of the state to take lives has largely been supplanted by its mandate to protect and prolong them.

Biopower emerged in the eighteenth and nineteenth centuries, however, its roots go back farther. In the seventeenth and early eighteenth centuries, humans created devices and technologies to monitor and control human bodies.⁵² Foucault characterizes these inventions as “the disciplinary technology of labor,” which includes social hierarchies and elaborate systems for inspection, bookkeeping, and reporting.⁵³ These inventions controlled individual bodies, incorporating them into the machinery of production to increase output and maximize efficiency. They characterize an anato-politics of the human body, and Bentham’s panopticon is one of its achievements.

In the second half of the eighteenth century, a more subtle form of power emerged that was less overtly disciplinary.⁵⁴ Instead of being applied to individual bodies, biopower was exerted over large populations. With the rise of biopower, the nineteenth century was characterized by the emergence of “power’s hold over life,” the acquisition of power over humans not as individuals but as a biological species.⁵⁵ Thus, seventeenth and eighteenth century anato-politics of the human body gave way to nineteenth century biopolitics of the entire human race.⁵⁶

Early biopolitics was characterized by efforts to shift various statistical means of populations toward values that were considered “normal” or otherwise desirable.⁵⁷ Its targets were statistical reflections of populations such as their rates of birth and death.⁵⁸ Governments used vaccinations, birth control, sanitation, and other public health measures to influence these statistics.⁵⁹ Eventually, in addition to shifting health-related variables, biopower shifted traits that drained the population’s strength, wasted energy or money, and decreased

⁵¹ See, e.g., Alan Meisel, *A History of the Law of Assisted Dying in the United States*, 73 SMU L. REV. 119, 126 (2020) (explaining that except in the few states that have legalized physician-assisted dying, the practice remains a criminal offense in most of the U.S.).

⁵² FOUCAULT, *supra* note 47, at 242.

⁵³ *Id.*

⁵⁴ *Id.*

⁵⁵ *Id.* at 239.

⁵⁶ *Id.*

⁵⁷ FOUCAULT, *supra* note 9, at 129.

⁵⁸ FOUCAULT, *supra* note 47, at 243.

⁵⁹ *Id.*

productivity.⁶⁰ It became directed less toward ends that helped people survive and thrive than ends that promote efficiency and increase output. Modern surveillance and automated decision making are extensions of this trend of promoting efficiency and output above other values.

Eventually biopower influenced interactions between humans and their surroundings, including their built environments.⁶¹ With the emergence of the internet of things, the built environment grew to encompass digital devices, computer screens, web browsers, and other user interfaces. Today it contains social media feeds, smart speakers, augmented reality, and three-dimensional virtual worlds. With its sensing and control networks, the digital panopticon allows platforms to manipulate immersive built environments to nudge the behavior of populations and shift social norms.

The exercise of biopower is neither inherently good nor bad, and many applications benefit society by promoting health and productivity. However, one side effect is that segments of the population falling outside the range of what those who wield biopower define as normal or desirable can be stigmatized and marginalized by systems designed to shift norms and regularize populations. The institutionalization of people with mental and physical disabilities is one striking historical example.⁶² The stigmatization and oppression of people in the LGBTQ community is another.⁶³ Consequently, it is dangerous to concentrate biopower in the hands of corporations whose primary goals are maximizing growth and profit above all else.

Historically, governments, not corporations, wielded the greatest powers. Accordingly, the Constitution limits the influence of government actors through its separation of powers and various checks and balances. Moreover, the Bill of Rights restrains public power by requiring transparency and accountability from government actors. When the Constitution and the Bill of Rights were drafted, governments had little biopower because technological constraints limited their information-producing capacity. In other words, Founding Era

⁶⁰ *Id.* at 244.

⁶¹ *Id.* at 245.

⁶² See Albert R. Roberts & Linda Farms Kurtz, *Historical Perspectives on the Care and Treatment of the Mentally Ill*, 14 J. SOCIO. & SOC. WELFARE 75, 77 (1987).

⁶³ See Christina Morales, *Hundreds of Religious Leaders Call for End to L.G.B.T.Q. Conversion Therapy*, N.Y. TIMES (Dec. 16, 2020), <https://www.nytimes.com/2020/12/16/world/conversion-therapy-pledge.html> [<https://perma.cc/2W3R-68FT>] (describing the discriminatory practice of conversion therapy, which aims to change one's sexual orientation or gender identity).

governments could not gather detailed information on populations. This slack in the system is what made public biopower tolerable. However, in the twenty-first century, the digital panopticon constructed by technology firms enhanced biopower and placed it in the hands of private companies, which exert biopower far greater than any government. Constitutional protections do not apply.

Through the digital panopticon, private actors exert biopower and shift social norms without transparency or accountability. They polarize populations, marginalize vulnerable communities, and promote inequality by creating new means for systemic discrimination and oppression.⁶⁴ The following Section describes the construction of the digital panopticon and its effects on society.

B. From Prisons to Platforms: Panoptic Surveillance in the Digital Age

In 2021, people increasingly welcome internet-enabled devices into their lives.⁶⁵ They carry them in pockets and purses, place them on bedside tables, and wear them in their ears and on their wrists.⁶⁶ Some

⁶⁴ See, e.g., Christopher A. Bail, Lisa P. Argyle, Taylor W. Brown, John P. Bumpus, Haohan Chen, M. B. Fallin Hunzaker, Jaemin Lee, Marcus Mann, Friedolin Merhout & Alexander Volfovsky, *Exposure to Opposing Views on Social Media Can Increase Political Polarization*, 115 PNAS 9216, 9216 (2018) (explaining how social media platforms create echo chambers that prevent people from being exposed to information that challenges their pre-existing beliefs, which promotes political polarization); see also Mason Marks, *Censoring Self-Harm on Facebook Might Do More Harm than Good*, MOTHERBOARD (Mar. 1, 2019, 7:13 AM), <https://www.vice.com/en/article/d3m5vj/censoring-self-harm-on-facebook-might-do-more-harm-than-good> [https://perma.cc/SPF7-2NL6] (describing how social media content moderation marginalizes people with certain mental health conditions).

⁶⁵ See Laura Silver, *Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally*, PEW RSCH. CTR. (Feb. 5, 2019), <https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/> [https://perma.cc/DD4W-M78T] (estimating that in 2019, more than five billion people had mobile devices, over half of which were smartphones); see, e.g., Brian Heater, *The Smart Speaker Market Is Expected to Grow 21% Next Year*, TECHCRUNCH (Oct. 22, 2020, 7:02 AM PDT), <https://techcrunch.com/2020/10/22/the-smart-speaker-market-is-expected-grow-21-next-year/> [https://perma.cc/5GJL-4Y5H] (reporting that an estimated 163 million smart speakers will have been sold worldwide by 2021).

⁶⁶ See, e.g., Geoffrey A. Fowler, *Amazon's Creepy New Health Wearable Analyzes Your Voice and Your Body*, WASH. POST (Aug. 27, 2020, 6:40 PM EDT), <https://www.washingtonpost.com/technology/2020/08/27/amazon-halo-wearable/> [https://perma.cc/8G46-PXUP] (describing the use of artificial intelligence to analyze smartphone and wearable data to infer users' health conditions).

even ingest them or implant them into their bodies.⁶⁷ These networked devices contain sensors including cameras, microphones, accelerometers, thermometers, and other instruments that collect data on people's traits and behaviors. That information is sent to platform servers and databases for algorithmic inspection.

Like Bentham's panoptic building, the digital version contains inspectors (algorithms of the sensing net) that occupy a central inspection house (centralized servers and databases). Like the architecture of Bentham's prison, the structure of the digital panopticon creates asymmetries of power and information flow.⁶⁸ As if positioned behind one-way glass; algorithms monitor user behavior while remaining concealed from view. The increasingly granular information these inspectors produce is shared, sold, and analyzed to sort people into highly specific categories.⁶⁹ By comparing people's actions to vast libraries of behavioral profiles stored in central servers, algorithms infer people's characteristics and predict future behavior.⁷⁰ This network of sensors, servers, and algorithms constitutes the *sensing net*, which was not implemented solely to observe and study human behavior; it was also designed to control it.⁷¹

Platform developers seek not only to understand life, but to manipulate and regulate it.⁷² Accordingly, the sensing net is paired with a *control net*, which receives intelligence from the sensing net and uses it to modify people's behavior. The control net consists of consumer-facing software and hardware that receive information from the sensing net and transform it into actions that influence users' thoughts and

⁶⁷ See Sara Gerke, Timo Minssen, Helen Yu & I. Glenn Cohen, *Ethical and Legal Issues of Ingestible Electronic Sensors*, 2 NATURE ELECS. 329, 329 (2019) (describing ingestible smart pills that upload data to platform servers).

⁶⁸ See ZUBOFF, *supra* note 14, at 187 (describing power asymmetries created by Google's surveillance and artificial intelligence infrastructure).

⁶⁹ See COHEN, *supra* note 13, at 57 (describing the surprisingly varied and granular data collected by mobile devices and their networked sensors); PASQUALE, *supra* note 13, at 25-32 (describing the secret algorithms that make inferences about people to profile, sort, and penalize them).

⁷⁰ See PASQUALE, *supra* note 13, at 25-32.

⁷¹ ZUBOFF, *supra* note 14, at 8 (describing how competitive pressures motivated platforms to shift from merely observing consumer behavior to controlling it).

⁷² See, e.g., Adam D. I. Kramer, Jamie E. Guillory & Jeffrey T. Hancock, *Experimental Evidence of Massive-Scale Emotional Contagion Through Social Networks*, 111 PNAS 8788 (2014) (describing Facebook's emotional contagion study in which the platform observed and intentionally manipulated the emotions of 689,003 Facebook users by altering the content of their newsfeeds); see also Waldman, *supra* note 17, at 107 (describing dark patterns, user interface features designed to exploit cognitive biases and nudge people to do things they would not otherwise do).

behavior.⁷³ These software and hardware elements include user interfaces that shapeshift to retain user attention, the speakers of smartphones and voice-enabled digital assistants that produce audible notifications and engage people in simulated conversations, and the motors, propellers, and other actuators that animate robots, drones, and smartphones. The goal of activating motor units might be to induce clicking, posting, reading, buying, voting, disclosing more data, or anything else a platform designer desires, and platforms seek to induce these behaviors in billions of users.⁷⁴ Motor units exert influence through technologies of manipulation such as custom search results and news feeds, targeted advertisements, dark patterns, and other forms of personalized choice architecture that leverage intelligence produced by the sensing net to influence individuals and groups.⁷⁵ The ultimate effect is a shift of population level traits in one direction or another.

Critics might argue that corporate manipulation of consumers is nothing new. Entire industries have been based on it for centuries. Advertisers cultivated the art and science of persuasion, alcohol and tobacco companies leverage biological principles to design and sell more addictive cigarettes, and casinos tap into primal drives to attract players to gaming floors and keep them there. However, the digital panopticon is a quantum leap for the technologies and industries of persuasion.

Unlike Bentham's rigid structure of steel and stone, the digital panopticon is agile and dynamic. Compared to traditional theaters of behavior modification, such as prisons and casinos, which are expensive and time consuming to remodel for enhanced effectiveness, developers can improve the digital panopticon instantaneously through software updates and dynamic user interfaces. While physical panopticons take a one-size-fits all approach to influencing human behavior, the dynamic architecture of the digital version can be tailored to individuals and communities in real time for maximum effect.

Targeted advertising, a form of personalized choice architecture, illustrates how developers can update digital environments instantaneously. This dynamic surveillance milieu allows developers to run ad hoc experiments on cross sections of their users, to determine the most effective means of shifting their behavior.⁷⁶ They use dark patterns and other behavioral tricks to maintain people's attention,

⁷³ See Kramer et al., *supra* note 72, at 8788; Waldman, *supra* note 17, at 107.

⁷⁴ See Kramer et al., *supra* note 72, at 8788; Waldman, *supra* note 17, at 107.

⁷⁵ See Lev-Aretz, *supra* note 16 (describing how personalized choice architecture harms democracy and individual autonomy).

⁷⁶ See Kramer et al., *supra* note 72, at 8788.

nudge them to act against their interests, conform their behavior to norms established by platform architects, and keep people from migrating to competing platforms.

Though the purpose of the digital panopticon is to manipulate human behavior, a few caveats are necessary. First, its inferences, predictions, and nudges need not be accurate or effective to shift social norms or cause harm. In fact, the ability of platforms to infer people's traits and behaviors is often exaggerated. In other words, this Article does not suggest that platform algorithms always do what their architects claim they do. They often do not. However, even imperfect inferences and nudges shift social norms, and their ability to do so is largely independent of their accuracy and social value. Facebook's AI-based suicide predictions, which are discussed further below, serve as a useful example. There is no evidence that Facebook's suicide predictions are safe, accurate, or effective. Nevertheless, their implementation has already shifted norms regarding online speech, surveillance, policing, and suicide prevention.

The second caveat is that although the digital panopticon is designed for both sensing and control, sensing alone is sufficient to cause harm and to warrant antitrust enforcement. Platforms use deception to encourage people to provide more information than they realize, or to use the data in ways they do not disclose to users. Even without analyzing that information with AI or using it to manipulate people through the control net, unauthorized surveillance through the sensing net deceives consumers, consolidates power, and suppresses competition. Accordingly, unauthorized surveillance should be regulated.

The following Section describes how platforms utilize networks of sensing and control to nudge users toward norms that they establish.

C. Choice Architecture: From Gentle Nudges to Coercive Dark Patterns

People constantly make choices whether they realize it or not, and the design of their surroundings limits their options. The architecture of buildings, the layout of neighborhoods, and the design of websites influence and constrain one's ability to choose. For instance, the aisles of most supermarkets encourage people to walk up one aisle and down the next. In this respect, physical architecture serves as *choice architecture*, which economist Richard Thaler defines as "the environment in which people choose."⁷⁷ Thaler and law professor Cass

⁷⁷ Richard Thaler, *Nudge, Not Sludge*, 361 Sci. 431, 431 (2018).

Sunstein argue that “the goal of a conscientious choice architect is to help people make better choices ‘as judged by themselves.’”⁷⁸

To help people make better choices, designers build features into human environments that nudge people to choose certain options over others.⁷⁹ Nudges are interventions that steer people along certain paths without forcing them to comply.⁸⁰ Examples include providing people with discounted gym memberships to encourage them to exercise and automatically enrolling employees in retirement accounts to encourage them to save.⁸¹ To be a nudge, an intervention must be relatively easy to avoid.⁸² If the outcome is unavoidable, or a high cost is required to avoid it, then the conditions that produce the outcome are not nudges.

When Thaler and Sunstein first wrote about nudges, they focused on their use by governments.⁸³ However, private companies increasingly use nudges and constantly innovate to make them more effective. Online examples include location and navigation services provided by Google Maps. Though users choose their destination, Google’s mapping software determines the route, calculating the optimal path based on factors such as traffic, weather, construction delays, and accidents, nudging users to maximize efficiency (often at the expense of other factors such as safety, ease of navigation, and satisfaction with the scenery).⁸⁴ Despite these seemingly benign examples of nudging, choice architecture can become deceptive and coercive, limiting people’s autonomy and encouraging them to do things that are harmful or undesirable.

Sunstein and Thaler refer to nudging that is harmful as “sludge” because it “mucks things up and makes wise decision-making and prosocial activity more difficult.”⁸⁵ Sludge comes in two varieties. It can discourage behavior that is in one’s best interest, such as obtaining reimbursement for medical expenses from a health insurance company.

⁷⁸ *Id.*

⁷⁹ As described previously, manipulation of built environments is one means through which biopower is generated and expressed.

⁸⁰ Cass R. Sunstein, *The Ethics of Nudging*, 32 YALE J. ON REGUL. 413, 417 (2015).

⁸¹ *Id.* at 426.

⁸² RICHARD H. THALER & CASS R. SUNSTEIN, *NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS* 6 (2008).

⁸³ *See id.*

⁸⁴ Thaler, *supra* note 77, at 431; Tim Stenovec, *Google Has Gotten Incredibly Good at Predicting Traffic — Here’s How*, BUS. INSIDER (Dec. 18, 2015, 10:41 AM), <https://www.businessinsider.com/how-google-maps-knows-about-traffic-2015-11> [https://perma.cc/5LJX-SEYP] (describing how Google Maps predicts traffic by analyzing a variety of data sources).

⁸⁵ Thaler, *supra* note 77, at 431.

Sludge can also promote self-defeating behavior, such as investing in deals that are too good to be true or providing more personal information to companies than one intends to reveal.⁸⁶ Sludge is “a viscous mixture, in the form of excessive or unjustified frictions that make it difficult for consumers, employees, employers, students, patients, clients, small businesses, and many others to get what they want or to do as they wish.”⁸⁷ Because sludge inhibits consumers from exercising free will, it creates market inefficiencies and negative externalities that are born by consumers and society instead of the businesses that produce it.

Retailers create sludge when they offer rebates to buyers and require them to mail in detailed evidence of the purchase including receipts and pieces of the product packaging within a specified period.⁸⁸ Such companies effectively offer illusory rebates.⁸⁹ They create sludge because their offers entice people to make purchases. However, many are too busy, forgetful, or lazy to complete the steps required to be reimbursed.⁹⁰ In this manner, companies exploit cognitive biases, including people’s tendency to discount the future effects of their behavior, such as having to mail in detailed information to a manufacturer, over the immediate effects of their behavior, receiving a discount from the seller.⁹¹

Panoptic platforms also generate sludge when they attract users by promising “we care about your privacy” before turning around and profiting from that data.⁹² Their promises induce people to trust the platforms and provide them with more personal information. However, their promises are often too good to be true, and users unwittingly disclose more information than they intended to share.⁹³ Platforms also

⁸⁶ *Id.*

⁸⁷ Cass R. Sunstein, *Sludge Audits*, 2020 BEHAV. PUB. POL'Y 1, 3, <https://www.cambridge.org/core/journals/behavioural-public-policy/article/sludge-audits/12A7E338984CE8807CC1E078EC4F13A7> [https://perma.cc/H6D3-R9K9].

⁸⁸ See Thaler, *supra* note 77, at 431.

⁸⁹ *See id.*

⁹⁰ *See id.*

⁹¹ See Waldman, *supra* note 17, at 106 (describing a cognitive bias called hyperbolic discounting, “the tendency to overweight the immediate consequences of a decision and to underweight those that will occur in the future”).

⁹² See, e.g., Seth Colaner, *Facebook Cares About Privacy, for Realsies, Zuckerberg Swears*, VENTURE BEAT (Apr. 30, 2019, 12:05 PM), <https://venturebeat.com/2019/04/30/facebook-cares-about-privacy-for-realsies-zuckerberg-swears/> [https://perma.cc/C4C9-SGAH] (quoting Mark Zuckerberg’s promises to protect user privacy despite his company’s poor track record in this area).

⁹³ See Waldman, *supra* note 17, at 107-08 (describing how people share information with platforms based on trust and how platforms manipulate user trust).

use dark patterns, a more sophisticated form of choice architecture, to create sludge, subtly nudging people to act against their interests.

Dark patterns are user interfaces designed to confuse people, making it difficult for them to express their true preferences, or designed to manipulate them into taking actions they would otherwise not take.⁹⁴ One empirical study concluded that “dark patterns are strikingly effective in getting consumers to do what they would not do when confronted with more neutral user interfaces.”⁹⁵ Essentially, dark patterns exploit cognitive biases, nudging people to buy products and services they would not otherwise buy or to disclose personal information they would rather not reveal.⁹⁶ Professor Ari Waldman describes them as design tricks that “weaponize design of the built environment to harm consumers and their privacy.”⁹⁷

When deployed at scale, dark patterns are an efficient means of exerting biopower, shifting the behavior of populations, often in directions that go against the interests of individuals and communities. One example is making it overly burdensome for people to cancel online subscriptions.⁹⁸ In this context, a common dark pattern involves hiding cancellation buttons behind difficult to find links or forcing people to call a telephone number and endure long wait times before being permitted to cancel a service.

Dark patterns are not limited to the two-dimensional user interfaces of computers and smartphones. They can be incorporated into the design of voice and gesture-based user interfaces for smart speakers, cameras, and three-dimensional augmented reality (“AR”) and virtual reality (“VR”) environments.⁹⁹ Moreover, dark patterns are not always static or uniformly applied. They can be made more powerful through customization that targets the unique susceptibilities of individuals and groups.¹⁰⁰ Through A/B testing involving thousands or millions of

⁹⁴ Jamie Luguri & Lior Jacob Strahilevitz, *Shining a Light on Dark Patterns*, 13 J. LEGAL ETHICS 43, 43 (2021).

⁹⁵ *Id.* at 46.

⁹⁶ See Waldman, *supra* note 17, at 105-06 (describing five major cognitive biases that platforms can exploit through dark patterns).

⁹⁷ See *id.* at 105.

⁹⁸ See Isabella Kwai, *Consumer Groups Target Amazon Prime’s Cancellation Process*, N.Y. TIMES (Jan. 14, 2021), <https://www.nytimes.com/2021/01/14/world/europe/amazon-prime-cancellation-complaint.html> [<https://perma.cc/YYP4-45TK>].

⁹⁹ Because dark patterns are merely user interface design choices intended to confuse or deceive users, they can be implemented in any medium, including voice activated interfaces and immersive virtual environments.

¹⁰⁰ See Arvind Narayanan, Arunesh Mathur, Marshini Chetty & Mihir Kshirsagar, *Dark Patterns: Past, Present, and Future*, 63 COMM’N ACM 42, 45 (2020).

people, platforms can determine which combinations of nudges are most effective in different types of users.¹⁰¹ Then they can deploy targeted nudges at scale to exert biopower, shifting the behavior of each cross-section of the population toward platform-defined norms.

In his book, *Liberty From All Masters*, Barry Lynn describes how Google could use its dominance in the mapping sector to route certain individuals and groups along different paths.¹⁰² The company could link navigation with advertising to route drivers past certain businesses and attractions.¹⁰³ Moreover, Google could prioritize VIP users by nudging them along scenic routes with less traffic while de-prioritizing other users and forcing them to endure sludge in the form of less efficient or scenic routes.¹⁰⁴ This practice would not differ significantly from those already implemented in other sectors such as customer service. Companies use intelligence gathered by the sensing net to determine where to route callers who call customer support. Those perceived as loyal may be routed to agents more quickly and to agents with greater authority to address their concerns.¹⁰⁵ Because Google can calculate personalized travel routes for each user, it could perform similar filtering for navigation, and nobody would know because its algorithms remain a closely guarded secret.

In addition to nudging users to act against their interests, dark patterns inhibit competition in several ways. They can prevent people from downloading and transferring their data to competing platforms or make it difficult for users to delete their data and social media accounts.¹⁰⁶ As a result, consumers are less likely to leave platforms that deploy dark patterns for their competitors.

¹⁰¹ See Luguri & Strahilevitz, *supra* note 94, at 44-45 (describing the experimental use of A/B testing to more than double the percentage of users who respond to a dark pattern).

¹⁰² See LYNN, *supra* note 22, at 65.

¹⁰³ See *id.*

¹⁰⁴ See *id.*

¹⁰⁵ See, e.g., *Intelligent Routing – It's Time to Evolve to Smarter Connections*, NICE, <https://www.nice.com/engage/nexidia-customer-engagement-analytics/predictive-behavioral-routing/intelligent-routing/> (last visited Jan. 16, 2021) [<https://perma.cc/7SS4-Y64U>] (“Predictive Behavioral Routing uses data gathered from previous interactions on the customer’s personality, behavioral characteristics, and communication preferences to intelligently predict the best agent to handle the customer’s call, and then route the call to the best agent for the customer.”).

¹⁰⁶ See *How to Delete Your Facebook, Twitter, Instagram, and TikTok*, WIRED (June 3, 2020, 4:22 PM), <https://www.wired.com/story/how-to-delete-your-facebook-instagram-twitter-snapchat/> [<https://perma.cc/7MJT-GHJG>] (describing how social media networks create obstacles for users who wish to delete their account information because the networks want users to continue using their services).

Dark patterns that manipulate users to provide data they would not otherwise provide can also be anticompetitive. They create competitive advantages for companies that deceive users, providing them with knowledge that is inaccessible to smaller, less deceptive firms, and preventing them from gaining traction in a market.¹⁰⁷ Consequently, antitrust regulators should identify and regulate dark patterns for their anticompetitive effects in addition to their potential to concentrate biopower.

One reason biosupremacy should be prevented is that companies could use it to nudge consumers in certain sectors or geographic areas in one direction while producing sludge in others. During the 2020 general election, Democrats were concerned that Republicans were attempting to discourage people from voting.¹⁰⁸ A social media company could use variable choice architecture to nudge people in historically conservative areas to vote while introducing sludge in historically liberal areas making it more difficult for people to vote. This type of private power is what antitrust law was designed to constrain, and because of the decline of antitrust enforcement since the 1970s, the public lacks protection against it.¹⁰⁹

To prevent abusive nudges, Sunstein calls for routine “sludge audits” in the public and private sectors to decrease the secrecy surrounding harmful nudges and equip regulators with the knowledge to police it.¹¹⁰ In Part III, this Article recommends that antitrust regulators perform sludge audits for merging companies to anticipate how mergers affect their ability to use dark patterns and other forms of coercive choice architecture.

The following Section provides three examples of Digital Age biopower and their impact on social norms.

D. Case Studies of Digital Biopower

This Section describes how tech companies exert biopower to shift norms in three spheres of human behavior: online speech, public health, and education.

¹⁰⁷ See Gregory Day & Abbey Stemler, *Are Dark Patterns Anticompetitive?*, 72 ALA. L. REV. 1, 6 (2020).

¹⁰⁸ See Dana Milbank, *Republicans’ Only Way to Win Is to Stop People from Voting*, WASH. POST (Oct. 29, 2020, 8:41 PM EDT), <https://www.washingtonpost.com/opinions/2020/10/28/republicans-only-way-win-is-stop-you-voting/> [https://perma.cc/RA8S-VJ6F].

¹⁰⁹ See Ariel Katz, *The Chicago School and the Forgotten Political Dimension of Antitrust Law*, 87 U. CHI. L. REV. 413, 457 (2020).

¹¹⁰ See Sunstein, *supra* note 87, at 3.

1. Shaping Online Speech Norms

In a 2020 Senate hearing, lawmakers questioned Mark Zuckerberg and Jack Dorsey on the content moderation practices of Facebook and Twitter.¹¹¹ Ted Cruz and other republicans alleged that the platforms systematically censor conservative voices.¹¹² Whether or not that is true, platforms shape speech norms regarding a variety of topics including politics, science, healthcare, substance use, violence, and terrorism.¹¹³ Sometimes, platforms coordinate their efforts, forming what Evelyn Douek calls content cartels: “arrangements between platforms to work together to remove content or actors from their services without adequate oversight.”¹¹⁴ In 2020, Senator Josh Hawley questioned Zuckerberg about these collaborations in a hearing before the Senate Judiciary Committee.¹¹⁵

Hawley argued that Facebook uses a platform called Tasks to coordinate the activities of its internal units and determine which individuals, hashtags, and websites Facebook should censor.¹¹⁶ According to Hawley, Facebook also uses Tasks to coordinate its content moderation efforts with Google and Twitter. In the hearing, Zuckerberg acknowledged that the companies share intelligence or “signals” regarding security related topics such as terrorism, child

¹¹¹ Mike Issac & Kellen Browning, *Zuckerberg and Dorsey Face Harsh Questioning from Lawmakers*, N.Y. TIMES (Nov. 17, 2020), <https://www.nytimes.com/live/2020/11/17/technology/twitter-facebook-hearings> [https://perma.cc/7LQY-X2CR].

¹¹² *Id.*

¹¹³ See, e.g., Maia Szalavitz, *Facebook Is Censoring Posts that Could Save Opioid Users’ Lives*, VICE (July 2, 2019, 8:15 AM), <https://www.vice.com/en/article/qv75ap/facebook-is-censoring-harm-reduction-posts-that-could-save-opioid-users-lives> [https://perma.cc/8AX2-QYRK]; see also John Koetsier, *Facebook Deleting Coronavirus Posts, Leading to Charges of Censorship*, FORBES (Mar. 17, 2020, 8:39 PM EDT), <https://www.forbes.com/sites/johnkoetsier/2020/03/17/facebook-deleting-coronavirus-posts-leading-to-charges-of-censorship/?sh=7bf2b0875962> [https://perma.cc/8H86-HDMU]; Mason Marks, *Online Content Moderation as Public Health Regulation*, BILL HEALTH (July 22, 2019), <https://blog.petrieflom.law.harvard.edu/2019/07/22/online-content-moderation-as-public-health-regulation/> [https://perma.cc/EAP3-F7UB].

¹¹⁴ Evelyn Douek, *The Rise of Content Cartels*, KNIGHT FIRST AMEND. INST. COLUM. UNIV., Feb. 11, 2020, at 1, 6, <https://knightcolumbia.org/content/the-rise-of-content-cartels> [https://perma.cc/9R55-YEJY].

¹¹⁵ CNET Highlights, *Republican Senator Grills Zuckerberg on Facebook, Google, and Twitter Collaboration*, YOUTUBE (Nov. 17, 2020), <https://www.youtube.com/watch?v=pOdrPruSnrw> [https://perma.cc/HQ56-A8Q5] (drawing analogies between price fixing by Gilded Age robber barons and coordinated moderation of online speech by content cartels).

¹¹⁶ *Id.*

exploitation, and foreign influence campaigns.¹¹⁷ These signals are collected by each platforms' sensing units, and sharing them between companies mingles their data streams, linking their sensing networks and the segments of the digital panopticon under their control. If Facebook, Google, and Twitter coordinate efforts to moderate content, they may constitute a bio-oligopoly that controls online speech norms for most of the world's population.¹¹⁸

In 2021, after supporters of President Trump stormed the U.S. capitol, Google and Apple removed the social networking app Parler from their app stores, and Amazon removed the app from its web servers.¹¹⁹ Though action was warranted, this example illustrates the power of platforms to coordinate and shape the voice of populations.

Even without coordinating with its peers, Facebook constitutes a bio-monopoly with respect to online speech, and its many of its content moderation activities violate democratic values of free expression and non-discrimination.¹²⁰ In 2019, it started censoring content uploaded by people with a stigmatized mental health condition called borderline personality disorder ("BPD"). Facebook and its photo sharing subsidiary Instagram blur images of people with BPD and hide their content from other users by excluding it from search results and other platform features that allow users to discover it organically.¹²¹ The platforms also censor content with hashtags related to BPD by suppressing it or concealing it behind content warnings.¹²² This systematic censorship is an expression of biopower. It nudges people to stop discussing certain topics and flagging their content with certain hashtags, shifting norms regarding online speech.

¹¹⁷ *Id.*

¹¹⁸ See, e.g., Chinmay Arun, *Making Choices: Social Media Platforms and Freedom of Expression Norms*, in *Regardless of Frontiers: Global Freedom of Expression in a Troubled World*, in 275-76 REGARDLESS OF FRONTIERS: GLOBAL FREEDOM OF EXPRESSION IN A TROUBLED WORLD (Agnes Collamard & Lee C. Bollinger eds., 2021) (describing how online platforms create their own speech norms that can "reflect, modify, shape and even override existing speech norms").

¹¹⁹ See Jack Nicas & Alba Davey, *Amazon, Apple and Google Cut Off Parler, an App that Drew Trump Supporters*, N.Y. TIMES (Jan. 9, 2021), <https://www.nytimes.com/2021/01/09/technology/apple-google-parler.html> [https://perma.cc/W2MQ-KQ87].

¹²⁰ See Heins, *supra* note 6, at 325 (describing Facebook's unparalleled power over speech).

¹²¹ See Marks, *supra* note 64.

¹²² *Id.*; Harriet Williamson, *Instagram Is Censoring a Hashtag for Borderline Personality Disorder*, VICE (Dec. 8, 2020, 4:03 AM), <https://www.vice.com/en/article/xgzg7q/instagram-censors-bpd-hashtag> [https://perma.cc/3HFC-ZZ4S].

Experts on BPD warn that Facebook's policies could further stigmatize and marginalize people with BPD, harm their self-image, impede their ability to form communities, and potentially worsen their mental and physical health.¹²³ Nevertheless, Facebook's decision instantly shifted speech norms regarding BPD, and billions of people who use Facebook and Instagram were forced to abide by the changes. This example illustrates how bio-monopolies can rapidly shift norms to deprive people of opportunities to communicate and coordinate, erasing their images and removing their voices from public discourse.

Through its role as an information gatekeeper, Facebook also shifts norms regarding the production, sharing, and consumption of news.¹²⁴ In 2018, editors of Wired Magazine described the power Facebook holds over journalists and publishers. The editors claimed, “[e]very publisher knows that, at best, they are sharecroppers on Facebook's massive industrial farm. The social network is roughly 200 times more valuable than the *Times*.” Moreover, “journalists know that the man who owns the farm has the leverage. If Facebook wanted to, it could quietly turn any number of dials that would harm a publisher—by manipulating its traffic, its ad network, or its readers.”¹²⁵

Like all expressions of biopower, content moderation is not inherently good nor bad. However, it is harmful when concentrated in the hands of a single company or group of companies. The Constitution provides no protection, and there is little transparency and accountability for the expression of private biopower. In addition to censoring freedom of expression and shifting speech norms, platforms alter digital environments to manipulate people's emotions, potentially shifting political opinion and influencing elections.¹²⁶ They exert biopower by altering the information people receive through customized search results, newsfeeds, and social media timelines, excluding groups and topics from public discourse or sending them to the fore by actively promoting them.¹²⁷ Because there is no meaningful

¹²³ Marks, *supra* note 64.

¹²⁴ SUBCOMM. ON ANTITRUST, COM. & ADMIN. L. OF THE COMM. ON THE JUDICIARY, 116TH CONG., INVESTIGATION OF COMPETITION IN DIGITAL MARKETS 62-63 (Comm. Print 2020) [hereinafter SUBCOMM. ON ANTITRUST].

¹²⁵ Nicholas Thompson & Fred Vogelstein, *Inside the Two Years that Shook Facebook — and the World*, WIRED (Feb. 12, 2018, 7:00 AM), <https://www.wired.com/story/inside-facebook-mark-zuckerberg-2-years-of-hell/> [<https://perma.cc/MC65-XMWY>].

¹²⁶ See, e.g., Kramer, *supra* note 72, at 8788 (describing Facebook's emotional contagion experiment in which the company altered users' newsfeeds to manipulate their emotions and influence their behavior).

¹²⁷ See Eric Goldman, *Content Moderation Remedies*, MICH. TECH. L. REV. 1, 40-47 (Mar. 24, 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3810580 [<https://perma.cc/>]

oversight and little transparency, those who are silenced or otherwise harmed have little recourse.

2. Shaping Public Health Norms

Internet companies increasingly shape norms regarding public health surveillance and intervention. This Section provides two examples: COVID-19 exposure notification apps (often erroneously called “contact tracing apps”) and AI-based violence and suicide prevention software.

During the COVID-19 pandemic, Google and Apple partnered to produce COVID-19 exposure notification software for smartphones.¹²⁸ Despite a lack of evidence for their effectiveness, the companies convinced people and governments around the world to adopt their software.¹²⁹ In this example, the companies use Bluetooth modules in smartphones as sensing units to detect when users come into proximity with people who claim to have tested positive for COVID-19. The app interfaces serve as sensing units because people input their test results. The interfaces also serve as motor units by notifying people when they have been in close contact with someone who reported a positive test, nudging users to alter their behavior.

Through their unusual partnership, Google and Apple may constitute a bio-oligopoly with respect to automated exposure notification. Professor Tamar Sharon argues that even if their software protects user privacy as well as the companies claim, its adoption represents the expansion of their influence over the fields of health and medicine.¹³⁰ Ultimately, that influence could reorganize those sectors to align with

FH8D-P69J] (describing 11 restrictions that social media platforms impose on user content to reduce its visibility).

¹²⁸ Kif Leswing, *Apple and Google Will Build Their Coronavirus Contract Tracing Software Right into Your Phone*, CNBC (Sept. 1, 2020, 1:50 PM EDT), <https://www.cnbc.com/2020/09/01/apple-google-will-build-coronavirus-contact-tracing-software-right-into-your-phone.html> [https://perma.cc/KX9L-H8A7].

¹²⁹ See Kif Leswing, *States Are Finally Starting to Use the COVID-19 Tracking Tech Apple and Google Built – Here’s Why*, CNBC (Oct. 4, 2020, 3:24 PM EDT), <https://www.cnbc.com/2020/10/03/covid-app-exposure-notification-apple-google.html> [https://perma.cc/RG4F-ZK27]; see also Ashkan Soltani, Ryan Calo & Carl Bergstrom, *Contact-Tracing Apps Are Not a Solution to the COVID-19 Crisis*, BROOKINGS (Apr. 27, 2020), <https://www.brookings.edu/techstream/inaccurate-and-insecure-why-contact-tracing-apps-could-be-a-disaster/> [https://perma.cc/U9FQ-8RRQ].

¹³⁰ TAMAR SHARON, *BLIND-SIDED BY PRIVACY? DIGITAL CONTACT TRACING, THE APPLE/GOOGLE API AND BIG TECH’S NEWFOUNDED ROLE AS GLOBAL HEALTH POLICY MAKERS* 1, 2 (2020), <https://link.springer.com/article/10.1007%2Fs10676-020-09547-x> [https://perma.cc/YQ27-LBGN].

corporate values and interests instead of the public interest.¹³¹ Moreover, widespread adoption of exposure notification apps represents the shaping of public policy by unelected officials and the expression of corporate power across diverse spheres of human activity.¹³²

The second public health example involves Facebook's use of AI to predict suicide.¹³³ When a user interacts with Facebook and Instagram, their AI assigns a suicide risk score to the user, which is continuously updated.¹³⁴ In this case, Facebook's social media interface serves as a suite of sensing units, collecting digital traces, and sending them back to central servers for algorithmic analysis. If the resulting suicide risk score is high enough, Facebook's Community Operations Team seem may send police to the user's home to perform what it calls a wellness check.¹³⁵ Though Facebook's system predicts suicide risk in billions of people daily, and the company has sent police to the homes of thousands of users, the system lacks transparency.¹³⁶ Moreover, it is unscientific, untested, and it exposes vulnerable individuals to potentially violent confrontations with law enforcement.¹³⁷ In this case, armed police officers serve as motor units of the system. For those in certain marginalized communities, such as people with disabilities and racial minorities, Facebook's wellness checks can amount to a death sentence.¹³⁸ In this respect, they represent a potential point of confluence of biopower and sovereign power, where the power to preserve life transforms into the power to kill.

By implementing AI-based suicide prediction worldwide in at least four languages, Facebook has shifted global norms for monitoring private communications for public health surveillance and intervention.¹³⁹ In many respects, it has made panoptic surveillance

¹³¹ See *id.*

¹³² *Id.*

¹³³ Mason Marks, *Artificial Intelligence Based Suicide Prediction*, 21 YALE J.L. & TECH 98, 108 (2019).

¹³⁴ *Id.*

¹³⁵ *Id.* at 110.

¹³⁶ *Id.* at 109 (stating that in late 2017, Facebook claimed it had conducted over 3,500 wellness checks internationally).

¹³⁷ *Id.* at 111-16.

¹³⁸ See Mason Marks, *Emergent Medical Data: Health Information Inferred by Artificial Intelligence*, 11 U.C. IRVINE L. REV. 995, 1035-36 (2021).

¹³⁹ See, e.g., Natasha Singer, *In Screening for Suicide Risk, Facebook Takes On Tricky Public Health Role*, N.Y. TIMES (Dec. 31, 2018), <https://www.nytimes.com/2018/12/31/technology/facebook-suicide-screening-algorithm.html> [https://perma.cc/GQ74-UYYP]

socially acceptable for this purpose, which enhances Facebook's biopower.

3. Shaping Educational Norms

Facebook is not the only company using AI to predict suicide. A handful of companies operate comparable systems to predict suicide, substance use, violence, and other behaviors in the context of K-12 education.¹⁴⁰ For instance, Gaggle, Bark, and GoGuardian monitor millions of school age children in the U.S. and United Kingdom, analyzing nearly everything students do online.¹⁴¹

Schools and technology companies provide children with laptops, tablets, and software with sensing units that continuously scan students' homework and personal communications for what developers define as abnormal behavior.¹⁴² Like Facebook, these systems may trigger police intervention, and there is little or no transparency or accountability.¹⁴³ Moreover, there is no data on the safety and effectiveness of these interventions. Nevertheless, a small group of companies have convinced thousands of U.S. schools to adopt their software, shifting norms regarding the surveillance of American students and how schools address mental health-related issues.¹⁴⁴ Meanwhile, during the COVID-19 pandemic, millions of students left classrooms to study and learn at home. This development led to the widespread adoption of surveillance

(reporting that as of late 2018, Facebook made automated suicide predictions in English, Spanish, Portuguese, and Arabic).

¹⁴⁰ See Becket, *supra* note 39.

¹⁴¹ See *id.*

¹⁴² See, e.g., *GoGuardian Beacon: The Student Safety Solution for K-12*, GOGUARDIAN, <https://www.goguardian.com/beacon/> (last visited June 12, 2021) [<https://perma.cc/89RV-KM8S>] (describing how GoGuardian Beacon software monitors students across multiple search engines, e-mail clients, social media platforms, web apps, and more to detect content that GoGuardian believes is predictive of behaviors such as suicide, violence, and bullying); see also *How It Works*, BARK, <https://www.bark.us/#how> (last visited June 12, 2021) [<https://perma.cc/W3AG-J7SP>] (describing how Bark software monitors children's behavior on over thirty software applications on smartphones, laptops, and e-book readers); *Monitor School-Issued Accounts for Free*, BARK, <https://www.bark.us/schools> (last visited June 12, 2021) [<https://perma.cc/3ZWFR-CRNN>] (describing how Bark software notifies school administrators when it detects content that Bark believes is indicative of concerning student behavior).

¹⁴³ See Becket, *supra* note 39 (describing instances in which software from GoGuardian and Gaggle flagged students as high risk, resulting in welfare checks at their homes).

¹⁴⁴ See *id.*

technologies that monitor students in their homes to detect cheating at the expense of their privacy.¹⁴⁵

If Facebook or Google acquired one of these companies, the merger would extend their portfolios of sensing and motor units into the education sector. It would establish cross-market data flows through which they could transfer information from the education industry into other sectors in which they operate. Simultaneously, they could shift biopower from those sectors into the education industry.

The following Section describes what could go wrong if the concentration of private biopower remains unopposed.

E. Totalitarian Data Mining

1. The Selfish Ledger

In 2018, online tech magazine The Verge obtained a mysterious film titled *The Selfish Ledger*, which was leaked from a division of Google called “X.”¹⁴⁶ This research and development unit is Google’s “moonshot factory” that creates “radical new technologies to solve some of the world’s hardest problems.”¹⁴⁷ The film opens with a wide shot of stars moving across the night sky. Chirping crickets lull viewers into a relaxed, dream like state, while the imagery evokes themes of creation, the divine, and the infinite.

The scene shifts to a workbench and a photo of French naturalist Jean Baptiste Lamarck. A predecessor of Charles Darwin, Lamarck believed that living beings possessed an internal code that is modified by their experiences (giraffes stretching their necks to reach the tops of trees is one example) and passed to successive generations through reproduction. Lamarck’s theory of evolution was supplanted by Darwin’s, but Google invokes Lamarck’s work to describe its vision for the future of data analytics: Lamarckian user data.

The scene shifts again to a person staring down at a smartphone. The narrator explains: “When we use contemporary technology, a trail of information is created in the form of data. When analyzed, it describes

¹⁴⁵ See Sara Morrison & Rebecca Heilweil, *How Teachers Are Sacrificing Student Privacy to Stop Cheating*, VOX (Dec. 18, 2020, 9:30 AM EST), <https://www.vox.com/recode/22175021/school-cheating-student-privacy-remote-learning> [https://perma.cc/TU2C-3PLQ].

¹⁴⁶ Vlad Savov, *Google’s Selfish Ledger is an Unsettling Vision of Silicon Valley Social Engineering*, VERGE (May 17, 2018, 8:00 AM EDT), <https://www.theverge.com/2018/5/17/17344250/google-x-selfish-ledger-video-data-privacy> [https://perma.cc/F2N7-98QC].

¹⁴⁷ GOOGLE X, <https://x.company/> (last visited Sept. 3, 2020) [https://perma.cc/7PVM-ME5S].

our actions, decisions, preferences, movement, and relationships. This codified version of who we are becomes ever more complex, developing, changing, and deforming based on our actions.” The narrator continues, “In this regard, this ledger of our data may be considered a Lamarckian epigenome, a constantly evolving representation of who we are.” In this scene, Google is describing the sensing net and how data is continuously collected to update digital profiles of individuals.

Scholars have given many names to this digital reflection of the self. Some call it a data double, a shadow profile, or a digital phenotype. The last term is derived from the word phenotype, which refers to an organism’s observable traits such as height and eye color.¹⁴⁸ The process of assembling and analyzing one’s digital phenotype is called digital phenotyping.¹⁴⁹ It is an emerging field of medicine and an example of how tech companies are influencing fields as diverse as healthcare, education, and policing. Though these fields are currently adopting digital phenotyping, tech companies have used it for years, building psychographic profiles that drive targeted advertising and exert political influence.¹⁵⁰

The film’s narrator explains: “As new users enter an ecosystem, they begin to create their own trail of data. By comparing this emergent ledger with the mass of historical user data, it becomes possible to make increasingly accurate predictions about decisions and future behaviors.”¹⁵¹ In other words, once a digital phenotype is created for an individual, it can be compared to the digital phenotypes of the entire population to infer characteristics of the individual and predict future actions. Essentially, the population-level knowledge contained in the ledger serves as a behavioral Rosetta Stone to interpret and predict the behavior of individuals when they join the system.

¹⁴⁸ In contrast to an organism’s phenotype, its genotype comprises its genetic material. In conjunction with environmental factors, the genotype contributes to an organism’s phenotype.

¹⁴⁹ See, e.g., Kit Huckvale, Svetha Venkatesh & Helen Christensen, *Toward Clinical Digital Phenotyping: A Timely Opportunity to Consider Purpose, Quality, and Safety*, 2 NPJ DIGIT. MED., Sept. 6, 2019, at 1, 1 <https://www.nature.com/articles/s41746-019-0166-1> [<https://perma.cc/4EH2-Q3B5>] (discussing four opportunities for digital phenotyping directed towards clinical improvement).

¹⁵⁰ See Matthew Rosenberg, Nicholas Confessore & Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. TIMES (Mar. 17, 2018), <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html> [<https://perma.cc/NHV9-WCPJ>] (describing Cambridge Analytica’s use of psychographic profiling to predict traits such as openness, neuroticism, and life satisfaction in American voters during the 2016 presidential election).

¹⁵¹ Savov, *supra* note 146.

In what seems ripped from the pages of Foucault's work on biopower, and Bentham's work on social control, the narrator concludes: "As cycles of collection and comparison extend, it may be possible to develop a species level understanding of complex issues such as depression, health, and poverty." However, the organizations poised to develop this species level understanding of humanity are private companies that have completed uncontested mergers over the past twenty years and become the most influential and profitable corporations in history. As private entities, they are under no legal obligation to share their insights publicly or use them for social good. Instead, they can hoard their behavioral intelligence and use it to coerce users, shift social norms, and maximize profit.

The narrator poses the following questions: "What if the ledger could be given a volitional purpose, rather than simply acting as a historical reference . . . [i]nitially the notion of a goal-oriented ledger may be user driven. As an organization, Google would be responsible for offering suitable targets for a user's ledger." The user interface of a fictional Google app suddenly comes into frame. Called Google Resolutions, it allows users to select from a series of pre-set goals such as eating healthier or protecting the environment. "Once the user selects a volition for their ledger, every interaction may be compared to a series of parallel options. If one of these options allows the ledger to move closer to its goal, it will be offered up to the user. Over time, by selecting these options, the user's behavior may be modified, and the ledger moves closer to its target."¹⁵²

The narrator is describing an elaborate system that uses nudges and choice architecture for behavior modification. Would you like to protect the environment? The ledger can nudge you to carpool by defaulting to Uber Pool instead of Uber Black or putting locally grown produce in your online shopping cart instead of imported products that burn more fossil fuels in transit. Users might select a broad goal, and Google's ledger will present them with a series of options that propel them toward achieving it. Essentially, the ledger nudges people to achieve their goals by manipulating the choice architecture of the Google Resolutions interface.

On the surface, this hypothetical app and behavior modification system appears utopian, a benevolent use of biopower. However, the narrator continues: "As this line of thinking accelerates, and the notion of a goal driven ledger becomes more palatable, suggestions may be

¹⁵² *Id.*

converted not by the user, but by the ledger itself.”¹⁵³ In other words, as people become accustomed to surrendering agency to Google, its AI could set goals on behalf of users and modify their behavior to achieve them.

The Verge called *The Selfish Ledger* “an unsettling vision of Silicon Valley social engineering.”¹⁵⁴ When asked for comment, Google said: “We understand if this is disturbing — it is designed to be. This is a thought-experiment by the Design team from years ago that uses a technique known as ‘speculative design’ to explore uncomfortable ideas and concepts in order to provoke discussion and debate.” Google claimed, “[i]t’s not related to any current or future products.” However, the ideas expressed in the film reflect Google’s current practices.

Google’s AI already makes decisions on behalf of users. It decides which ads people read, the news they consume, the videos they watch, and the routes they take to work. Google and other leading tech companies influence a wide range of behaviors associated with employment, education, speech, healthcare, and law enforcement. They nudge people to conform their behavior to norms determined by platforms, policed by the sensing net and its AI. These companies express biopower on a scale that would have been unimaginable to Bentham and Foucault.

2. The Threat of Data Fascism

There is a fine line between the influence of leading tech platforms and the power of totalitarian rulers. In her recent book on surveillance capitalism, Shoshana Zuboff labels the influence of panoptic platforms *instrumentarianism*, power that shapes human behavior toward others’ ends.¹⁵⁵ She compares this power to totalitarianism because both brands of coercive influence arose unexpectedly.¹⁵⁶

When totalitarianism emerged in the twentieth century, many observers struggled to comprehend its significance as an existential threat.¹⁵⁷ Similarly, the twenty-first century rise of panoptic surveillance caught the world off guard, and many still fail to appreciate its scale and importance.¹⁵⁸ However, Zuboff claims the similarities end there. She provides an overview of totalitarianism, exemplified by the regimes of

¹⁵³ *Id.*

¹⁵⁴ Savov, *supra* note 146.

¹⁵⁵ ZUBOFF, *supra* note 14, at 8.

¹⁵⁶ *Id.* at 352-53.

¹⁵⁷ *Id.* at 357.

¹⁵⁸ See *id.* at 352.

Mussolini and Stalin, and contrasts it with instrumentarian power, like that of Facebook and Amazon, which she claims cannot be totalitarian.¹⁵⁹

Zuboff traces the roots of totalitarianism to the writing of Italian philosopher Giovanni Gentile.¹⁶⁰ His political theory is defined by the concept of the “total,” which requires citizens to surrender their independence and uniqueness to the state.¹⁶¹ Gentile wrote the introduction to Mussolini’s book *The Doctrine of Fascism*, which defines fascism as “a spiritual attitude” best viewed in relation to one’s general outlook on life.¹⁶² According to Gentile, fascism is “an inwardly accepted standard and rule of conduct, a discipline of the whole person; it permeates the will no less than the intellect . . . sinking deep down into his personality . . . entering into the soul and ruling with undisputed sway.”¹⁶³

According to Zuboff, “[t]otalitarianism was bent on the reconstruction of the human species through the dual mechanisms of genocide and the ‘engineering of the soul.’”¹⁶⁴ In contrast, “[i]nstrumentarian power . . . takes us in a sharply different direction. Surveillance capitalists have no interest in murder or the reformation of our souls.”¹⁶⁵ According to Zuboff, they care only that human behavior remains accessible, measurable, and controllable, so that they can observe and profit from it.¹⁶⁶ She says “[t]otalitarian power cannot succeed by remote control.”¹⁶⁷ However, in a time when centrally controlled technologies reach out and touch people in their homes, and even within their bodies, totalitarianism can take many forms, including data fascism that operates at a distance.

When tech companies propose implanting internet-enabled devices into people’s bodies and brains to infer and manipulate their thoughts and behaviors, perhaps they are attempting to capture and refashion people’s souls.¹⁶⁸ One might argue they have already succeeded by

¹⁵⁹ See *id.* at 353-60.

¹⁶⁰ *Id.* at 354.

¹⁶¹ *Id.*

¹⁶² BENITO MUSSOLINI, THE DOCTRINE OF FASCISM 6 (1938).

¹⁶³ *Id.* at 6-7.

¹⁶⁴ ZUBOFF, *supra* note 14, at 353.

¹⁶⁵ *Id.*

¹⁶⁶ *Id.* at 360.

¹⁶⁷ *Id.* at 359.

¹⁶⁸ See generally Lauren Golembiewski, *Are You Ready for Tech that Connects to Your Brain?*, HARV. BUS. REV. (Sept. 28, 2020), <https://hbr.org/2020/09/are-you-ready-for-tech-that-connects-to-your-brain> [<https://perma.cc/KT4H-9YMN>] (describing the rise of brain-computer interfaces).

changing the way people think and relate to each other since the advent of smart phones and other internet enabled devices.¹⁶⁹ In this respect, *The Selfish Ledger* and the digital panopticon are modern extensions of Gentile's fascism. They require people to surrender their autonomy and uniqueness. However, instead of surrendering to totalitarian governments, people surrender their autonomy to internet platforms whose singular devotion to data collection and analytics is total, perhaps even spiritual.¹⁷⁰

Digital Age totalitarians need not resort to murder and genocide because they have more subtle means of control. Instead of deploying spies to do their bidding, they rely on sensing and motor units. Their algorithms infer one's thoughts and predict one's behaviors. Their choice architecture shapes people's perceptions of the world while nudging them to conform. In 2021, whistleblower Frances Haugen leaked internal documents indicating that Facebook knew its products were negatively impacting the health of teenage users.¹⁷¹ According to the documents, "thirty-two percent of teen girls said that when they felt bad about their bodies, Instagram made them feel worse."¹⁷² Moreover, Facebook researchers warned the company that Instagram's Explore feature, which serves users customized content, can push them toward harmful information.¹⁷³

Hundreds of years ago, Hume observed that a government's control of subjects depends on swaying their opinions because brute force alone

¹⁶⁹ See, e.g., Dan Milmo, *How Losing a Friend to Misinformation Drove Facebook Whistleblower*, GUARDIAN (Oct. 4, 2021, 9:13 AM EDT), <https://www.theguardian.com/technology/2021/oct/04/how-friend-lost-to-misinformation-drove-facebook-whistleblower-frances-haugen> [https://perma.cc/3SYH-3DPB] (describing how Facebook's power to spread misinformation drove whistleblower Frances Haugen to reveal that the company knew it was harming the public).

¹⁷⁰ Nick Saint, Google CEO: "We Know Where You Are. We Know Where You've Been. We Can More Or Less Know What You're Thinking About," BUS. INSIDER (Oct. 4, 2010), <https://www.businessinsider.com/eric-schmidt-we-know-where-you-are-we-know-where-youve-been-we-can-more-or-less-know-what-youre-thinking-about-2010-10> [https://perma.cc/9N73-BJ8D].

¹⁷¹ Georgia Wells, Jeff Horwitz & Deepa Seetharaman, *Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show*, WALL ST. J. (Sept. 14, 2021, 7:59 AM EST), <https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739> [https://perma.cc/W85P-TJNQ].

¹⁷² *Id.*

¹⁷³ Jessica Bursztynsky & Lauren Feiner, *Facebook Documents Show How Toxic Instagram is for Teens*, Wall Street Journal Reports, CNBC (Sept. 14, 2021, 9:01 AM ET), <https://www.cnbc.com/2021/09/14/facebook-documents-show-how-toxic-instagram-is-for-teens-wsj.html> [https://perma.cc/TQZ9-QSLV].

is insufficient.¹⁷⁴ Accordingly, totalitarians combine force with propaganda. Today, the digital panopticon is the ultimate tool for influencing public opinion. Tech companies rely on its nudges and sludges instead of resorting to physical force. Though they use different tools than twentieth century fascists, and lack their overt bloodlust, platforms can still have blood on their hands. Systematic discrimination, violence, and even genocide, are not outside the scope of their powers.¹⁷⁵ “The version of Facebook that exists today is tearing our societies apart and causing ethnics violence around the word,” said Haugen.¹⁷⁶

In addition to endangering human lives, data fascists are killing the technological future envisioned by early internet pioneers.¹⁷⁷ In this respect, digital biopower resembles the brand of totalitarianism described by Herbert Marcuse in his 1965 book *One Dimensional Man: Studies in the Ideology of Advanced Industrial Society*.¹⁷⁸ Marcuse believed technology could create utopian societies where humans are liberated from unpleasant work, freeing them to exercise autonomy and craft the lives they want to live.¹⁷⁹ However, technology has instead been used to suppress individuality and concentrate human efforts into increasingly efficient and productive arrangements. Marcuse describes this social structure as totalitarian, “[f]or ‘totalitarian’ is not only a terroristic political coordination of society, but also a nonterroristic economic

¹⁷⁴ See DAVID HUME, *Of the First Principles of Government*, in ESSAYS: MORAL, POLITICAL AND LITERARY 32, 32-34 (Eugene F. Miller ed., Liberty Fund 2012) (1742) (stating that effective government depends on opinion).

¹⁷⁵ See Tom Miles, *U.N. Investigators Cite Facebook Role in Myanmar Crisis*, REUTERS (Mar. 12, 2018, 2:40 PM), <https://www.reuters.com/article/us-myanmar-rohingya-facebook/u-n-investigators-cite-facebook-role-in-myanmar-crisis-idUSKCN1GO2PN> [<https://perma.cc/C4NK-C9ED>]; see also Tony Room, *Facebook, Twitter Could Face Punishing Regulation for Their Role in U.S. Capitol Riot, Democrats Say*, WASH. POST (Jan. 8, 2021, 12:51 PM ET), <https://www.washingtonpost.com/technology/2021/01/08/facebook-twitter-congress-trump-riot/> [<https://perma.cc/H8MB-3UC7>].

¹⁷⁶ Kari Paul & Dan Milmo, *Facebook Putting Profit Before Public Good, Says Whistleblower Frances Haugen*, GUARDIAN (Oct. 4, 2021, 4:35 PM), <https://www.theguardian.com/technology/2021/oct/03/former-facebook-employee-frances-haugen-identifies-herself-as-whistleblower> [<https://perma.cc/MCJ4-LPGP>].

¹⁷⁷ See, e.g., Katrina Brooker, “I Was Devastated”: Tim Berners-Lee, the Man Who Created the World Wide Web, Has Some Regrets, VANITY FAIR (July 1, 2018), <https://www.vanityfair.com/news/2018/07/the-man-who-created-the-world-wide-web-has-some-regrets> [<https://perma.cc/B2ZT-V7VC>] (describing Tim Berners-Lee’s concerns that instead of improving society, the internet could destroy it).

¹⁷⁸ See HERBERT MARCUSE, ONE-DIMENSIONAL MAN: STUDIES IN THE IDEOLOGY OF ADVANCED INDUSTRIAL SOCIETY 18-19 (1964).

¹⁷⁹ Id. at 18 (describing a possible future where the automation of tasks necessary for survival reduces the need for labor and enables individual autonomy).

technical coordination which operates through the manipulation of needs by vested interests.”¹⁸⁰ His analysis foreshadowed the twenty-first century construction of the digital panopticon and *The Selfish Ledger*. Marcuse predicted that the physical and psychological powers of machines would surpass those of humans, making machines “the most effective political instrument[s]” of technologically focused societies.¹⁸¹ Over half a century later, panoptic platforms are proving him right.

In the digital panopticon, machines observe all spheres of behavior and AI supplants human agency as the architect of the future. Algorithmic nudges represent the “manipulation of needs by vested interests” described by Marcuse and the shaping of the soul described by Mussolini and Gentile. The goose-stepping of technology firms toward biosupremacy represents the kind of unrestrained private power that antitrust was designed to prevent.¹⁸²

Overconcentrated private power undermines personal autonomy and political liberty.¹⁸³ In the extreme, it threatens republican ideals and democracy itself.¹⁸⁴ The German Republic’s support of monopolies helped Hitler rise to power.¹⁸⁵ After the Second World War, fears that concentrated private power might undermine American democracy prompted Congress to strengthen antitrust laws.¹⁸⁶ In 1979, law professor Robert Pitofsky argued that those laws “exhibited a clear concern that an economic order dominated by a few corporate giants could, during a time of domestic stress or disorder, facilitate the overthrow of democratic institutions and the installation of a totalitarian regime.”¹⁸⁷

During the COVID-19 pandemic, Americans spent most of their lives online. They relied on tech companies for work, education, healthcare, food, entertainment, and communication. Meanwhile, amid widespread

¹⁸⁰ *Id.* at 19.

¹⁸¹ *Id.*

¹⁸² See Khan, *supra* note 7, at 740.

¹⁸³ See Lina M. Khan, *The End of Antitrust History Revisited*, 133 HARV. L. REV. 1655, 1660 (2020) (reviewing Tim Wu, *THE CURSE OF BIGNESS: ANTITRUST IN THE NEW GILDED AGE* (2018)).

¹⁸⁴ See Wu, *supra* note 7, at 139.

¹⁸⁵ *Id.* at 79-80; see also Tim Wu, *Be Afraid of Economic ‘Bigness.’ Be Very Afraid*, N.Y. TIMES (Nov. 10, 2018), <https://www.nytimes.com/2018/11/10/opinion/sunday/fascism-economy-monopoly.html> [<https://perma.cc/2DZ9-56LA>].

¹⁸⁶ Wu, *supra* note 7, at 80-81.

¹⁸⁷ Robert Pitofsky, *The Political Content of Antitrust*, 127 U. PA. L. REV. 1051, 1054 (1979).

death and despair, ten billionaires, including founders of Facebook, Amazon, and Google, increased their net worth by \$400 billion.¹⁸⁸

Some leading tech companies completed additional mergers during the pandemic. Alphabet quietly acquired smart glasses maker North, cloud services provider StratoZone, data analytics company Dataform, and operating system developer Neverware.¹⁸⁹ Two of these acquisitions occurred after U.S. states and the Department of Justice (“DOJ”) filed antitrust lawsuits against Google, reflecting the current lack of scrutiny for conglomerate and concentric mergers. Similarly, after the DOJ and forty-eight states filed suits against Facebook for abusing its market power, the company expanded its surveillance of consumers by requiring them to sign-in with active Facebook accounts before using its messaging service WhatsApp and its VR platform Oculus.¹⁹⁰ The fact that these anticompetitive behaviors occurred after high profile antitrust complaints were filed illustrates how current antitrust regulation is incapable of restraining private biopower.

Part II explains how antitrust enforcement has declined since the late 1970s, allowing data conglomerates to prosper while engaging in hundreds of unregulated mergers. It describes the original mandate of

¹⁸⁸ See Rupert Neate, *Ten Billionaires Reap \$400bn Boost to Wealth During Pandemic*, GUARDIAN (Dec. 19, 2020, 11:00 AM EST), <https://www.theguardian.com/technology/2020/dec/19/ten-billionaires-reap-400bn-boost-to-wealth-during-pandemic> [https://perma.cc/T24Z-VS7Z].

¹⁸⁹ Monica Chin, *Google Acquires Neverware, A Company that Turns Old PCs into Chromebooks*, VERGE (Dec. 16, 2020, 5:15 PM), <https://www.theverge.com/2020/12/16/22179242/google-neverware-chromebook-laptops-chrome-os-software> [https://perma.cc/DU9V-KWFA]; Souvik Choudhury & Erwan Menard, *Ramping Up Cloud Migration Discovery and Assessment*, GOOGLE CLOUD (Aug. 24, 2020), <https://cloud.google.com/blog/products/cloud-migration/google-cloud-has-acquired-stratozone> [https://perma.cc/7JCH-MXKF]; Steve O’Hear, *Google Quietly Acquires Dataform, the UK Startup Helping Businesses Manage Data Warehouses*, TECHCRUNCH (Dec. 9, 2020, 4:27 AM PST), <https://techcrunch.com/2020/12/09/google-quietly-acquires-dataform/> [https://perma.cc/J3KM-9X9M]; see Hirsh Chitkara, *Google’s Possible North Acquisition Could Help Revive Its AR Glasses Ambitions*, BUS. INSIDER (June 29, 2020, 6:57 AM), <https://www.businessinsider.com/alphabet-may-acquire-north-to-help-google-launch-ar-glasses-2020-6> [https://perma.cc/4VPN-6SXT].

¹⁹⁰ See Carly Page, *WhatsApp Tells Users: Share Your Data with Facebook or We’ll Delete Your Account*, FORBES (Jan. 8, 2021, 7:02 AM EST), <https://www.forbes.com/sites/carlypage/2021/01/08/whatsapp-tells-users-share-your-data-with-facebook-or-well-deactivate-your-account/?sh=754685c32d46> [https://perma.cc/W39M-TA66]; Adi Robertson, *Facebook is Making Oculus’ Worst Feature Unavoidable*, VERGE (Aug. 19, 2020, 7:04 PM EDT), <https://www.theverge.com/2020/8/19/21375118/oculus-facebook-account-login-data-privacy-controversy-developers-competition> [https://perma.cc/C8F4-USNN] (discussing Facebook’s move to require users of its VR headsets to log in with active Facebook accounts and describing users’ and critics’ reactions to the announcement).

antitrust law and why antitrust regulation is an appropriate means of constraining digital biopower.

II. THE DECLINE OF ANTITRUST AND THE RISE OF DATA CONGLOMERATES

This Part provides an overview of antitrust history, how neoliberal economics shaped modern antitrust policy, and why antitrust law must be updated for the Digital Age. It describes the field's original mandate to constrain private power, the rise and fall of conglomerate merger control in the 1960s and 70s, and the emergence of data conglomerates in the 2000s within the vacuum of antitrust enforcement left in the Chicago School's wake. This Part also describes the rise of Neo-Brandeisian Antitrust and its influence on current state and federal lawsuits against Google and Facebook. It concludes that antitrust must revive conglomerate merger control and incorporate biopower, cross-market data flows, and coercive choice architecture into antitrust jurisprudence and enforcement.

A. *The Need to Regulate Data Conglomerates*

Since 2000, Google, Amazon, Facebook, Apple, and Microsoft have completed a total of over 600 acquisitions.¹⁹¹ Google and Microsoft lead the pack with over 200 mergers each.¹⁹² Economist John Kwoka reports that between 2005 and 2009, the leading five firms collectively completed about twenty-five acquisitions per year, which rose to nearly fifty acquisitions per year since 2009.¹⁹³ Despite these striking statistics, antitrust agencies have challenged Big Tech-related mergers far less often than acquisitions in other sectors.¹⁹⁴

Many antitrust scholars agree that this trend of underenforcement is concerning.¹⁹⁵ Part of the problem is that courts and regulators take an increasingly narrow view of the goals of antitrust law. The entrenched

¹⁹¹ KWOKA, *supra* note 5, at 109-10.

¹⁹² *Id.*

¹⁹³ *Id.*

¹⁹⁴ *Id.*

¹⁹⁵ See Stigler Committee on Digital Platforms, in STIGLER CENTER FOR THE STUDY OF THE ECONOMY AND THE STATE 31 (2019) [hereinafter *Stigler Report*]; see also WU, *supra* note 7, at 121-23 (describing the rise of tech monopolies in the 2000s and the failure of U.S. antitrust regulators to respond, allowing dominant firms to buy up hundreds of competitors without fear of antitrust scrutiny and enforcement).

view promotes the aging “consumer welfare standard” above all else.¹⁹⁶ This approach originated with the Chicago School of Antitrust and its neoliberal ideology, conceived by Aaron Director in the 1970s and popularized by Robert Bork and Richard Posner in the 70s and 80s.¹⁹⁷ Proponents of the consumer welfare standard say it brought clarity, predictability, and ease of administration to antitrust after decades of confusion and overenforcement.¹⁹⁸ They argue that until antitrust adopted consumer welfare as its north star, U.S. antitrust regulation was a tangle of perplexing and inconsistently applied theories that were unwieldy and counterproductive.¹⁹⁹ They claim the standard made antitrust regulation more manageable, coherent, and predictable.²⁰⁰ However, despite proponents’ devotion to the consumer welfare standard, few can agree on its definition.

Some economists support Richard Posner’s view that low prices are the most important indicator of consumer welfare.²⁰¹ In contrast, Herbert Hovenkamp argues that maximizing output rather than minimizing price should be paramount.²⁰² Others claim there is room in the standard for non-price related factors such as product quality and innovation.²⁰³ With so many views on the meaning of consumer welfare, it is difficult to see how its adoption has simplified antitrust law or made it more manageable.

Regardless of how one defines it, consumer welfare is a misnomer. To those outside the field of antitrust, it conjures a broad conception of wellbeing that includes non-economic factors such as fairness, product

¹⁹⁶ See Elyse Dorsey, *Antitrust in Retrograde: The Consumer Welfare Standard, Socio-Political Goals, and the Future of Enforcement*, in THE GLOBAL ANTITRUST INSTITUTE REPORT ON THE DIGITAL ECONOMY 109, 109 (Joshua D. Wright & Douglas H. Ginsburg eds., 2020).

¹⁹⁷ See WU, *supra* note 7, at 83-87.

¹⁹⁸ See Joshua D. Wright, Elyse Dorsey, Johnathan Klick & Jan M. Rybnicek, *Requiem for a Paradox: The Dubious Rise and Inevitable Fall of Hipster Antitrust*, 51 ARIZ. ST. L.J. 293, 298-99 (2019).

¹⁹⁹ See Elyse Dorsey, Geoffrey A. Manne, Jan M. Rybnicek, Kristian Stout & Joshua D. Wright, *Consumer Welfare & the Rule of Law: The Case Against the Populist Antitrust Movement*, 47 PEPPERDINE L. REV. 861, 873-74 (2020) (describing U.S. antitrust regulation before the consumer welfare standard as unprincipled and rudderless).

²⁰⁰ See *id.* at 880-84 (“[the consumer welfare standard is] a predictable methodology that leads to more consistency across different antitrust cases and . . . treat[s] similarly situated parties equally under the law.”).

²⁰¹ See Khan, *supra* note 7, at 717, 723.

²⁰² See Herbert J. Hovenkamp, *Antitrust: What Counts as Consumer Welfare?*, PENN L., July 20, 2020, at 1, 3-4, https://scholarship.law.upenn.edu/faculty_scholarship/2194/ [<https://perma.cc/5NP8-QC7U>].

²⁰³ See Dorsey, *supra* note 196, at 133-34.

quality and variety, autonomy, and economic liberty. However, most economists agree that consumer welfare does not address those factors.²⁰⁴ In this respect, the term's adoption reflects how the Chicago School used language to subvert the purpose of antitrust and to shape it so that only trained specialists could understand it.²⁰⁵

Economist Mark Glick argues that U.S. antitrust should abandon the consumer welfare standard because "it is based on unsound economics and is in conflict with modern welfare economics."²⁰⁶ Moreover, "there is no evidence that Chicago School assumptions and policies about efficiency have benefitted the macroeconomy."²⁰⁷ Even if proponents of the consumer welfare standard are correct that it makes antitrust more predictable, if it produces results that are consistently harmful or unhelpful, then its continued use cannot be justified.

Despite varying interpretations of antitrust's scope and purpose, ample evidence suggests that when Congress established the field, it had one overarching goal: constraining private power.²⁰⁸ That goal is more important than ever — The unbridled expansion of large technology firms, and their concentration of biopower through unregulated conglomerate and concentric mergers, reflects the need for new approaches to antitrust law that acknowledge its original mandate. To understand where antitrust should go next, the following Section briefly discusses its origins.

B. Antitrust's Original Mandate to Constrain Private Power

During the Gilded Age of the late nineteenth century, America witnessed the rise of trusts composed of powerful corporations that bought up competitors or pushed them to extinction. Examples include the New Haven Railroad and John D. Rockefeller's Standard Oil. Early monopolists believed large trusts could save the country from financial

²⁰⁴ See, e.g., Hovenkamp, *supra* note 202, at 4-8 (discussing what is not included in the definition of consumer welfare).

²⁰⁵ See Stigler Center, *Should Antitrust Promote Economic Liberty?: Caffara, Kovacic, Lynn, & Schlesinger*, YOUTUBE (Oct. 20, 2020), <https://www.youtube.com/watch?v=2oakHVSnYhU&list=PLvLk5ZuczSArx6VwX6a-bKUZsEJEOSilh&index=60> [<https://perma.cc/B256-PX5Y>] (featuring Barry Lynn commenting on the use of language to subvert the purpose of U.S. antitrust).

²⁰⁶ University of Utah, *Economic Challenges to Traditional Antitrust Economics – A New Future for Antitrust*, YOUTUBE (Nov. 4, 2019), <https://www.youtube.com/watch?v=oX2zVHeXksw&feature=youtu.be>. [<https://perma.cc/4WSC-LRYX>].

²⁰⁷ *Id.*

²⁰⁸ See, e.g., Teachout & Khan, *supra* note 10, at 61-62; see also Bogus, *supra* note 10, at 42-43.

ruin.²⁰⁹ They embraced a survival-of-the-fittest mentality and insisted that breaking up trusts would inhibit innovation and human progress.²¹⁰ Some claimed a small number of highly capable men who had fought their way to success, eliminating rivals along the way, made the best economic leaders.²¹¹ Railroad magnate Cornelius Vanderbilt boasted that he earned one million dollars every year and generated three times that much value for the American public.²¹²

As monopolies and oligopolies dominated markets, their political influence grew. To achieve and maintain their positions, they engaged in bribery, deception, and other unfair practices.²¹³ Monopolists acquired private power so great that it could not have been anticipated by America's Founders a century earlier when governments and monarchs wielded the greatest powers. Accordingly, the Constitution offers little protection from corporate consolidation because it was drafted with public power in mind. Nevertheless, amid the abuses of the Gilded Age, people noticed the unchecked social and political influence of monopolies, and legislators resolved to do something about it. They created antitrust laws to constrain private economic and political power.²¹⁴ Throughout antitrust's history, one finds statements from courts, legislators, and regulators confirming its constitutional role.²¹⁵

According to Senator John Sherman, his 1890 act was "a bill of rights, a charter of liberty."²¹⁶ Speaking on the Senate floor 100 years before the ascension of Zuckerberg and Bezos, Sherman compared the powers of monopolists to those of absolute monarchs: "If the concentrated powers of this combination are [e]ntrusted to a single man, it is a kingly prerogative, inconsistent with our form of government, and should be subject to the strong resistance of the state and national authorities. If anything is wrong this is wrong."²¹⁷ Sherman emphasized antitrust's role in restraining private power, "If we will not endure a king as a political power, we should not endure a king over the production,

²⁰⁹ See WU, *supra* note 7, at 26 (arguing that some Americans blamed low prices and competition for the country's economic decline in the 1890s and that monopolies overcame these issues).

²¹⁰ *Id.* at 28.

²¹¹ See *id.* at 27-28.

²¹² SEAN DENNIS CASHMAN, AMERICA IN THE GILDED AGE 41 (N.Y. Univ. Press ed., 3d ed. 1993).

²¹³ See WU, *supra* note 7, at 29.

²¹⁴ See *id.* at 19.

²¹⁵ See *id.* at 53 ("[antitrust law served as a limit on private power by] teach[ing] the masters of the biggest corporations in the land that they were not . . . above the law.").

²¹⁶ Khan, *supra* note 7, at 740.

²¹⁷ Katz, *supra* note 109, at 424.

transportation, and sale of any of the necessities of life.”²¹⁸ His view persisted well into the twentieth century.

In 1914, during passage of the Federal Trade Commission Act, Senator Cummins explained, “we must do something to preserve the independence of the man as distinguished from the power of the corporation . . .”²¹⁹ As if he foresaw the eventual rise of data conglomerates and their defenders, Cummins advocated for rigorous antitrust enforcement even though some economists argued that big companies were good for consumers. He acknowledged that low prices often come at a high cost to society. As if describing Zuckerberg’s power and Facebook’s model of providing “free” services in exchange for people’s secrets and autonomy, Cummins argued “we can purchase cheapness at altogether too high a price, if it involves the surrender of the individual, the subjugation of a great mass of people to a single master mind.”²²⁰

In 1945, Judge Learned Hand acknowledged that when Congress passed the Sherman Antitrust Act, it had social and political goals in mind and was unlikely motivated “by economic motives alone.”²²¹ Over a decade later, President Kennedy’s chief antitrust advisor Lee Loevinger viewed consolidated private power as an existential threat.²²² In 1958, he told Congress: “The problems with which the antitrust laws are concerned—the problems of distribution of power within society—are second only to the questions of survival in the face of threats of nuclear weapons.”²²³

In his dissenting opinion in *United States v. Columbia Steel, Co.*, Justice Douglas expressed concern over the impact of big business on society, politics, and the economy.²²⁴ According to Douglas, “[p]ower that controls the economy should be in the hands of elected representatives of the people, not in the hands of an industrial oligarchy.” He argued that industrial power “should be scattered into many hands, so that the fortunes of the people will not be dependent on the whim or caprice, the political prejudices, the emotional stability of a few self-appointed men . . . That is the philosophy and the

²¹⁸ Khan, *supra* note 7, at 740.

²¹⁹ Teachout & Khan, *supra* note 10, at 62 (quoting Senator Cummins).

²²⁰ *Id.*

²²¹ *United States v. Aluminum Co. of Am.*, 148 F.2d 416, 427 (2d Cir. 1945).

²²² See WU, *supra* note 7, at 78.

²²³ *Id.*

²²⁴ *United States v. Columbia Steel Co.*, 334 U.S. 495, 535-36 (1948) (Douglas, J., dissenting).

command of the Sherman Act.”²²⁵ Douglas claimed private companies could not be trusted with “power so great that only a government of the people should have it.”²²⁶

These statements reflect the longstanding view of courts, legislators, and federal agencies that U.S. antitrust laws were created to disrupt concentrated private power because it harms individuals, society, and democracy. In the mid-twentieth century, Congress, courts, and the antitrust agencies held this view, and they aggressively used antitrust enforcement to halt mergers between large, powerful firms, and to break them up when necessary.²²⁷

C. The Rise and Fall of Conglomerate Merger Control

In 1950, following a burst of corporate mergers, Congress strengthened U.S. antitrust law with the Celler-Kefauver Act (the “Anti-Merger Act”).²²⁸ Passed partly out of fears that consolidated private power could undermine democracy in America after World War II, the Act closed loopholes in the Clayton Act of 1914, which applied only to certain horizontal mergers.²²⁹ As amended by the Anti-Merger Act, Section 7 of the Clayton Act addressed any merger that substantially lessens competition whether horizontal, vertical, or conglomerate.²³⁰

When courts and antitrust agencies interpreted the Anti-Merger Act, they produced aggressive structural remedies to curb consolidated private power.²³¹ Economic structuralists believe that when markets are dominated by a few large firms, there will be less competition, in part because large firms are incentivized to engage in collusion, price fixing, and other anticompetitive behaviors like their Gilded Age

²²⁵ *Id.* at 536.

²²⁶ *Id.*

²²⁷ See *United States v. E.I. du Pont de Nemours & Co.*, 353 U.S. 586, 607 (1957) (blocking du Pont’s acquisition of a twenty-three percent stock interest in General Motors, finding it certain that the acquisition was likely to lessen competition); Wu, *supra* note 7, at 78-82 (describing the period of peak antitrust in the mid-twentieth century); see, e.g., Charles J. Steele, *A Decade of the Celler-Kefauver Anti-Merger Act*, 14 VAND. L. REV. 1049, 1062 (1961) (describing judicial interpretation of the Celler-Kefauver Act of 1950, which allowed courts to halt a merger if there was a reasonable probability that it would lessen competition).

²²⁸ Teachout & Khan, *supra* note 10, at 65.

²²⁹ See Noah Naparst, *The Spirit of Antitrust: How Antitrust Lost Its Way, and How It Can Be Revived*, 18 STAN. UNDERGRADUATE RSCH. J. 21, 24-25 (2019).

²³⁰ See Celler-Kefauver Antimerger Act, ch. 1184, 64 Stat. 1125-26 (1950); see also Richard E. Day, *Conglomerate Mergers and the Curse of Bigness*, 42 N.C. L. REV. 511, 517 (1964).

²³¹ See Teachout & Khan, *supra* note 10, at 65-66.

predecessors.²³² However, regulators' intense focus on the size of firms (their "bigness") created blind spots that would soon be exploited.

Between 1965 and 1970, there was a wave of conglomerate mergers.²³³ Antitrust scholars believe it resulted from the Federal Trade Commission's ("FTC") intense scrutiny of horizontal and vertical mergers.²³⁴ To avoid antitrust enforcement, firms expanded through conglomerate mergers, acquiring companies that produced unrelated goods and services, because it was the path of least resistance. In response, the FTC launched an assault on what law professor Richard E. Day calls "conglomerate bigness," a term that reflects both a firm's size and its degree of diversification through participation in different markets.²³⁵

In 1963, the FTC noted Congress's intent to regulate conglomerate mergers, and articulated the need for innovative approaches to analyze and stop them:

Congress' clearly expressed concern with the conglomerate merger is in striking contrast to the preoccupation of lawyers and economists with tests that look only to the number and size distribution of firms in a single market, and is a challenge to this Commission and to the courts to devise tests more precisely adjusted to the special dangers to a competitive economy posed by the conglomerate merger.²³⁶

The FTC's frustration with economists is notable because in the decade that followed, economists would capture the entire field of antitrust, realigning it with neoliberal theories and values. In the meantime, to meet the challenge of regulating conglomerate mergers, U.S. courts and antitrust agencies adopted new theories of economic harm with names like entrenchment, deep pockets, and reciprocal dealing.²³⁷ They reasoned that conglomerate mergers restrained competition through "conglomerate leverage."²³⁸ Under this theory, a firm could leverage its dominance in one market to foreclose competition in another.²³⁹ In the

²³² See Wu, *supra* note 7, at 29.

²³³ See Joel Dean, *Causes and Consequences of Growth by Conglomerate Merger: An Introduction*, 44 ST. JOHN'S L. REV. 15, 15 (1970).

²³⁴ See *id.* at 15-16.

²³⁵ See Day, *supra* note 230, at 525.

²³⁶ Procter & Gamble Co., 63 F.T.C. 1465, 1546-47 (1963).

²³⁷ William J. Kolasky, *Conglomerate Mergers and Range Effects: It's a Long Way from Chicago to Brussels*, 10 GEO. MASON L. REV. 533, 533 (2002).

²³⁸ Day, *supra* note 230, at 525.

²³⁹ *Id.* at 526.

1960s, regulators believed firms exerted leverage primarily through product tie-ins and various forms of reciprocity.²⁴⁰

By 1970, scrutiny of conglomerate mergers was so common that the St. John's Law Review held a symposium on the topic and published a special issue containing over sixty related essays.²⁴¹ However, the trend of regulating conglomerate mergers slowed in the late 1970s with the rise of the Chicago School. Since then, conglomerate mergers have flown under the radar of antitrust enforcement, and antitrust's mandate to restrain private power has been obscured by a preoccupation with consumer welfare. Descendants of the Chicago School reject structuralism and the scrutiny of non-economic factors in favor of a streamlined approach focused on price theory, which according to Richard Posner, is "the proper lens for viewing antitrust problems."²⁴² Thus, the scope of antitrust policy narrowed, and antitrust remedies became increasingly anemic and infrequently used.

In 2001, William J. Kolasky proudly recounted the decline of conglomerate merger enforcement. "As the Chicago School taught us the central importance of consumer welfare and efficiency in antitrust analysis, these [conglomerate merger] theories faded away," said Kolasky.²⁴³ "After fifteen years of painful experience with these now long-abandoned theories, the U.S. antitrust agencies concluded that antitrust should rarely, if ever, interfere with any conglomerate merger."²⁴⁴ However, Kolasky made these observations before the meteoric rise of leading technology companies.

In 2001, Google and Amazon were young companies focused narrowly on internet search and bookselling. Google had not discovered surveillance capitalism, Amazon had not dominated logistics, and neither firm had become the diversified AI and cloud computing powerhouses they are today. For the past twenty years, amid an enforcement vacuum created by the Chicago School, the leading tech companies acquired hundreds of other firms producing sprawling *data*

²⁴⁰ *Id.*; see *Tying the Sale of Two Products*, FED. TRADE COMM'N, <https://www.ftc.gov/tips-advice/competition-guidance/guide-antitrust-laws/single-firm-conduct/tying-sale-two-products> (last visited July 20, 2021) [<https://perma.cc/9MZ3-8HXW>] (Tying occurs when a seller conditions the sale of one product on a buyer's agreement to take a second product. According to the FTC, "a monopolist may use forced buying, or 'tie-in' sales, to gain sales in other markets where it is not dominant and to make it more difficult for rivals in those markets to obtain sales").

²⁴¹ See Symposium, *Conglomerate Mergers and Acquisitions: Opinion and Analysis*, 44 ST. JOHN'S L. REV. 9 (1970).

²⁴² Khan, *supra* note 7, at 718-19.

²⁴³ Kolasky, *supra* note 237, at 533.

²⁴⁴ *Id.*

conglomerates. These mergers differ from those Congress and the FTC feared in the 1950s and 60s; they are far more dangerous.

Instead of leveraging their dominance in one market through tie-ins and reciprocity, data conglomerates leverage cross-market data flows springing from software and devices in the new markets they enter. Data conglomerates analyze data streams using proprietary AI and leverage the resulting intelligence to exert biopower, shifting behavioral norms in numerous sectors. Part III of this Article argues that antitrust regulators should renew their focus on conglomerate mergers and incorporate the concepts of biopower, data flows, and coercive choice architecture into antitrust enforcement. The following Section describes how data conglomerates leverage data flows to generate biopower.

D. *The Emergence of Data Conglomerates and Digital Biopower*

In the past twenty years, tech firms have consolidated biopower through hundreds of unregulated conglomerate mergers.²⁴⁵ Examples include Facebook's acquisitions of Instagram and Oculus, Amazon's purchases of Ring and Audible, and Google's acquisitions of FitBit and Double Click.²⁴⁶ By acquiring companies that sell products and services outside their existing product lines, or in adjacent categories, companies add sensing and motor units to their portfolios, extending the reach of their corners of the digital panopticon. Acquiring sensing units in new sectors creates cross-market data flows that send user information back to acquiring firms from markets where they previously lacked insight. Similarly, acquiring motor units establishes beachheads from which platforms deploy coercive choice architecture to shift norms in sectors where they previously lacked influence.

When Google Street View launched in 2007, people objected to Google's use of car mounted cameras to photograph neighborhoods across America.²⁴⁷ Since then, the sensing net has become broader and

²⁴⁵ See KWOKA, *supra* note 5, at 109-10.

²⁴⁶ See, e.g., Brad Stone, *Amazon to Buy Audiobook Seller for \$300 Million*, N.Y. TIMES (Feb. 1, 2008), <https://www.nytimes.com/2008/02/01/technology/01amazon.html> [<https://perma.cc/WR8G-L7SR>] (reporting that Amazon would purchase Audible, an online audiobook service).

²⁴⁷ See, e.g., Jamie Doward, *Google Street View Does Not Breach Privacy Laws*, GUARDIAN (Apr. 11, 2009, 7:01 PM EDT), <https://www.theguardian.com/technology/2009/apr/12/google-street-view-privacy> [<https://perma.cc/F3QG-CX2H>] (reporting that hundreds of people complained about Google Street View within one month of its launch); David Streitfeld, *Google Concedes that Drive-By Prying Violated Privacy*, N.Y. TIMES (Mar. 12, 2013), <https://www.nytimes.com/2013/03/13/technology/google-pays-fine-over-street-view-privacy-breach.html> [<https://perma.cc/YRT9-3TTS>] (reporting that in addition to taking photos for Street View, Google's vehicles collected people's

more sophisticated. Through its 2018 acquisition of Ring, Amazon added sensing units in the form of internet-enabled doorbell cameras.²⁴⁸ When individual doorbells are linked together by Amazon's network, they blanket neighborhoods with surveillance.²⁴⁹

In 2019, Amazon revealed it had quietly acquired a robotics company called Dispatch to build a sidewalk robot called "Scout."²⁵⁰ Ostensibly built for last-mile delivery, Scout has another purpose: It continuously patrols neighborhoods and creates detailed three-dimensional models of the world and the objects in it.²⁵¹ Equipped with GPS, radar, and an array of cameras and other sensors, sidewalk robots gather far richer streams of data than Google Street View, and they can explore places larger vehicles cannot reach including sidewalks, office parks, and college campuses.²⁵² While Amazon's Ring doorbells gaze outward toward the street, Amazon's Scout robots look inward at people's homes. Together, they create a 360-degree view of neighborhoods. Meanwhile, Amazon's PrimeAir drones are poised to fill the skies, and its Ring home surveillance drone and Astro home robot will map people's home interiors.²⁵³

passwords, e-mail correspondence, medical and financial records, and other personal information without their knowledge).

²⁴⁸ See Samuel Gibbs, *Amazon Buys Video Doorbell Firm Ring for Over \$1bn*, GUARDIAN (Feb. 28, 2018, 6:43 AM EST), <https://www.theguardian.com/technology/2018/feb/28/amazon-buys-video-doorbell-ring-smart-home-delivery> [https://perma.cc/XB7V-5WNU].

²⁴⁹ See Drew Harwell, *Doorbell-Camera Firm Ring Has Partnered with 400 Police Forces, Extending Surveillance Concerns*, WASH. POST (Aug. 28, 2019), <https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach/> [https://perma.cc/NK9U-PACK].

²⁵⁰ Mark Harris, *Amazon Quietly Acquired Robotics Company Dispatch to Build Scout*, TECHCRUNCH (Feb. 7, 2019, 5:45 AM PST), <https://techcrunch.com/2019/02/07/meet-the-tiny-startup-that-helped-build-amazons-scout-robot/> [https://perma.cc/HDH8-96G5].

²⁵¹ See Tom Simonite, *How Amazon Cloned a Neighborhood to Test Its Delivery Robots*, WIRED (June 14, 2019, 7:00 AM), <https://www.wired.com/story/how-amazon-cloned-neighborhood-test-delivery-robots/> [https://perma.cc/44PC-QBTU].

²⁵² See, e.g., Jenni Fink, *Delivery Robots Headed to 100 College Campuses: Entire Generation Expects Robot Service, Company Says*, NEWSWEEK (Aug. 20, 2019, 4:29 PM EDT), <https://www.newsweek.com/starship-technologies-delivery-robots-college-1455348> [https://perma.cc/758Z-TS45] ("[Robots] can tackle sidewalks, crossing streets and even going over curbs.").

²⁵³ See Alan Levin, *Amazon's Drone Delivery Fleet Hits Milestone with FAA Clearance*, BLOOMBERG (Aug. 31, 2020, 6:00 AM PDT), <https://www.bloomberg.com/news/articles/2020-08-31/amazon-s-drone-delivery-fleet-hits-milestone-with-faa-clearance> [https://perma.cc/25EU-7V2U]; see also Dieter Bohn, *The Ring Drone Is Just the Latest Amazon Privacy Puzzle Box*, VERGE (Sept. 25, 2020, 10:30 AM EDT), <https://www.theverge.com/2020/9/25/21455197/amazon-ring-drone-home-security-surveillance-sidewalk-halo-privacy> [https://perma.cc/G2YM-DNZE]; see also James

Amazon's world-mapping capability reflects expansion of the digital panopticon from two dimensional spaces, such as laptop and smartphone screens, into three dimensional environments including homes, neighborhoods, cities, workplaces, and immersive virtual worlds. In 2021, a Bloomberg Opinion article claimed that Amazon was building factory towns to support the working class.²⁵⁴ However, this development has concerning parallels with the company towns of America's Gilded Age, which oppressed workers and represented an expansion of corporate biopower. One notable example is Pullman, Illinois on the outskirts of Chicago. In 1884, George Pullman built a new factory, and a town to house its workforce, to support his thriving business manufacturing luxury railcars for wealthy patrons.²⁵⁵ Like modern panoptic platforms, Pullman exerted significant control over the people who inhabited his town, and what he conceived as a utopia quickly became dystopian.

Pullman stratified the population, housing different categories of workers in different sections of the town; executives lived in larger homes close to the factory, and line workers lived farther away in more modest apartments.²⁵⁶ Employees were forced to rent from Pullman and faced unannounced home inspections by his staff.²⁵⁷ He determined what they wore, where they worshipped, and how they behaved.²⁵⁸ When he cut workers' wages without reducing their rent, the town erupted in protest, which ended in a violent clash with federal troops.²⁵⁹

Many parallels can be drawn between Pullman's surveillance and control of employees, his attempt to shape norms by exerting biopower, and Amazon's surveillance and control of factory workers, delivery

Vincent, *Don't Be Fooled — Amazon's Astro Isn't a Home Robot, it's a Camera on Wheels*, VERGE (Sept. 29, 2021, 9:44 AM EDT), <https://www.theverge.com/22699916/amazon-astro-home-robot-camera-surveillance-device> [https://perma.cc/GG62-XGWE] (describing the Astro robot as "part of a dangerous trend of ubiquitous and unthinking surveillance").

²⁵⁴ Conor Sen, *Amazon's New 'Factory Towns' Will Lift the Working Class*, BLOOMBERG (Sept. 16, 2021), <https://www.bloomberg.com/opinion/articles/2021-09-16/amazon-s-new-factory-towns-will-lift-the-working-class> [https://perma.cc/U4X3-QBW4].

²⁵⁵ Elizabeth Nix, *Five Famous Company Towns*, HIST. (Aug. 22, 2018), <https://www.history.com/news/5-famous-company-towns> [https://perma.cc/53AS-H8CK].

²⁵⁶ Ron Grossman, *Pullman's Folly*, CHI. TRIBUNE (Aug. 1, 1994), <https://www.chicagotribune.com/news/ct-xpm-1994-08-01-9408010189-story.html> [https://perma.cc/T59V-529C].

²⁵⁷ *Id.*

²⁵⁸ *Id.*

²⁵⁹ *Id.*

drivers, customer service representatives, and other employees.²⁶⁰ However, the digital panopticon, which its ubiquitous network of sensors and motor units, allows Amazon to monitor and influence the behavior of employees and consumers regardless of where they reside. According to Zuboff, Amazon's achievements have outgrown the outdated concept of the company town.²⁶¹ By expanding the digital panopticon into three-dimensional space, Amazon has built a company world.²⁶²

Facebook is also leading the digital panopticon's transition from two to three-dimensional space by investing heavily in augmented reality and virtual reality.²⁶³ In 2014, Facebook acquired VR company Oculus for \$2 billion.²⁶⁴ Through the Oculus merger, Facebook acquired sensing and motor units that track and influence behavior in both real and virtual three-dimensional environments. The investment is paying dividends. In 2020, Facebook announced Project Aria, an initiative that uses AR glasses to map the world and the objects in it.²⁶⁵ In 2021, the company's Oculus Quest 2 headset was a best-selling and top-ranked VR unit.²⁶⁶ Facebook also announced a partnership with Ray-Ban to offer AR glasses some call "smart glasses that actually look cool."²⁶⁷ These developments are part of Zuckerberg's plan to create the

²⁶⁰ See Joseph Cox, *Amazon to Monitor Customer Service Worker's Keyboard and Mouse Strokes*, VICE (Aug. 12, 2021, 7:18 AM), <https://www.vice.com/en/article/dyvejq/amazon-monitor-employees-keyboard-mouse> [https://perma.cc/YXC3-8TG9].

²⁶¹ See Shira Ovide, *A City with Amazon at the Center*, N.Y. TIMES (Feb. 22, 2021), <https://www.nytimes.com/2021/02/22/technology/amazon-california-inland-empire.html> [https://perma.cc/CB7P-P2AE].

²⁶² See *id.* (reporting Zuboff's view that Amazon's scale and ubiquity have created a company world).

²⁶³ Zuckerberg Wants Facebook to Become Online 'Metaverse,' BBC NEWS (July 23, 2021), <https://www.bbc.com/news/technology-57942909> [https://perma.cc/2QPP-G8ZH] (reporting Zuckerberg's goal to transform Facebook into a 'metaverse company' in five years, creating an online world where people work, play, and communicate in immersive virtual environments).

²⁶⁴ Josh Constine, *Facebook's \$2 Billion Acquisition of Oculus Closes, Now Official*, TECHCRUNCH (July 21, 2014, 1:04 PM PDT), <https://techcrunch.com/2014/07/21/facebook-s-acquisition-of-oculus-closes-now-official/> [https://perma.cc/7QU5-YA2T].

²⁶⁵ See S.A. Applin, *Why Facebook is Using Ray-Ban to Stake a Claim to our Faces*, MIT TECH. REV. (Sept. 15, 2021), <https://www.technologyreview.com/2021/09/15/1035785/why-facebook-ray-ban-stories-metaverse/> [https://perma.cc/KE8E-HDM3].

²⁶⁶ Will Greenwald, *The Best VR Headsets for 2021*, PC MAG. (Oct. 21, 2021), <https://www.pc当地/2021/10/21/the-best-vr-headsets/> [https://perma.cc/CF3P-BKC3].

²⁶⁷ Rachel Metz, *Facebook and Ray-Ban are Rolling out Smart Glasses That Actually Look Cool. Will Anyone Buy Them?*, CNN (Sept. 9, 2021, 1:28 PM EST), <https://www.cnn.com/2021/09/09/tech/facebook-smart-glasses-rayban-stories/index.html> [https://perma.cc/37YA-9PUY].

metaverse, an immersive virtual environment in which people work, play, and communicate.²⁶⁸ The metaverse is “an embodied Internet that you’re inside of rather than looking at,” said Zuckerberg.²⁶⁹

Facebook’s dominant position in the VR market puts it in a strong position to lead the future of immersive computing. Building the metaverse will provide the company with unparalleled opportunities to monitor and control users while concentrating and exerting biopower. Some regulators have taken notice. In 2020, Facebook rebranded Oculus “Facebook Reality Labs” and changed its policies by requiring VR users to sign-in with active Facebook accounts.²⁷⁰ Linking data from its VR devices to its social media platform caught the eye of Germany’s Federal Cartel Office, the Bundeskartellamt.²⁷¹ According office president Andreas Mundt, “Linking virtual reality products and the group’s social network in this way could constitute a prohibited abuse of dominance by Facebook.”²⁷²

One year earlier, the Bundeskartellamt alleged that Facebook had exploited its dominance in social media by forcing users to share data collected from other sources such as Instagram, WhatsApp, and the “Like” and “Share” buttons that Facebook scatters across the internet.²⁷³ The Bundeskartellamt ordered Facebook to stop secretly combining data from outside sources without people’s knowledge or consent.²⁷⁴ When Facebook appealed the order, a court in Dusseldorf ruled the company need not comply.²⁷⁵ However, on June 23, 2020, the German Federal Court of Justice overturned the lower court’s decision and ordered Facebook to comply with the Bundeskartellamt’s order.²⁷⁶

²⁶⁸ See Mike Isaac, *Facebook Renames Itself Meta*, NY TIMES (Oct. 28, 2021), <https://www.nytimes.com/2021/10/28/technology/facebook-meta-name-change.html> (reporting Zuckerberg’s intent to focus on building the metaverse and his rebranding of Facebook as Meta to represent its shifting priorities).

²⁶⁹ Kyle Chyka, *Facebook Wants Us to Live in the Metaverse*, NEW YORKER (Aug. 5, 2021), <https://www.newyorker.com/culture/infinite-scroll/facebook-wants-us-to-live-in-the-metaverse> [<https://perma.cc/YF7D-FYVS>].

²⁷⁰ See Robertson, *supra* note 190.

²⁷¹ David Rising, *German Regulators Launch New Facebook Investigation over VR*, ABC NEWS (Dec. 10, 2020, 6:36 AM), <https://abcnews.go.com/Business/wireStory/german-regulators-launch-facebook-investigation-vr-74646836> [<https://perma.cc/W35Y-XLXZ>].

²⁷² *Id.*

²⁷³ *Id.*

²⁷⁴ See *id.*

²⁷⁵ *Id.*

²⁷⁶ See Adam Satariano, *Facebook Loses Antitrust Decision in Germany over Data Collection*, N.Y. TIMES (June 23, 2020), <https://www.nytimes.com/2020/06/23/technology/facebook-antitrust-germany.html> [<https://perma.cc/8V4X-CJSR>].

These examples illustrate the versatility of biopower. Sensing units in one industry can be paired with motor units in another. For instance, Facebook's sensing units embedded in websites across the internet convey information to the company's central servers, and the resulting intelligence is used to influence users of its social media platform. Meanwhile, sensing units in Facebook's AR glasses and VR headsets can generate data and intelligence that is used to influence behavior on any of Facebook's platforms. Similarly, sensing units in Amazon's drones and security products can generate data and intelligence that influences behavior in Amazon's other markets such as online retail, video streaming, e-books, and healthcare. In other words, unlike twentieth century conglomerates that tied products to leverage market dominance, twenty-first century data conglomerates leverage cross-market data flows to exert biopower in numerous markets, providing unprecedented influence over diverse spheres of human life. If they can influence behavior in a sufficient number of domains, data conglomerates can achieve biosupremacy and nudge humanity along a path of their choosing.

In contrast to the Bundeskartellamt's orders against Facebook, the European Commission's approval of the Google-FitBit merger represents a missed opportunity and a lack of appreciation for how companies exert biopower. When Google completed the merger, it entered the wearables market and acquire sensing units embedded in FitBit devices. Google can now access data generated by those sensing units as it flows across market boundaries to its servers and databases. It can share the data with other Alphabet subsidiaries including its industry-leading AI firm DeepMind.

Cross-market data flows between Alphabet acquisitions and DeepMind are concerning because new data streams can be incorporated into behavioral models produced by DeepMind's AI.²⁷⁷ Those models and their predictions can then be disseminated to

²⁷⁷ See James Vincent, *How Google Maps Uses DeepMind's AI Tools to Predict Your Arrival Time*, VERGE (Sept. 3, 2020, 10:00 AM EDT), <https://www.theverge.com/2020/9/3/21419632/how-google-maps-predicts-traffic-eta-ai-machine-learning-deepmind> [<https://perma.cc/8V4X-CJSR>] (describing how DeepMind researchers analyze data from a variety of sources to predict traffic patterns and the arrival times of people using Google Maps); see also Jordan Novet, *Google Is Finding Ways to Make Money from Alphabet's DeepMind A.I. Technology*, CNBC (Mar. 31, 2018, 9:20 AM EDT), <https://www.cnbc.com/2018/03/31/how-google-makes-money-from-alphabets-deepmind-ai-research-group.html> [<https://perma.cc/E2YT-W96Z>] (describing how Alphabet commercializes technology developed by DeepMind such as artificial human voices, digital personal assistants, and methods of personalizing recommendations made by Google's Play Store).

companies and divisions throughout Alphabet's corporate family tree — such as YouTube, Android, Google search, Gmail, Nest, Verily, and Waymo — leveraging data streams established through the FitBit acquisition to profile consumers, manipulate them, and inhibit competition in the diverse markets in which Google and Alphabet operate. However, the European Commission's conditions for approving the deal (its behavioral remedies) focus narrowly on the advertising market.²⁷⁸ They require Google to contain FitBit user information within a data silo to prevent it from being used in Google's advertising business.²⁷⁹ However, the silo is less like an impervious container than a semipermeable membrane that allows health data to flow out for any purpose other than advertising.²⁸⁰ The Commission ignored Google's ability to leverage data from the wearables market to exert influence in sectors other than advertising, and conversely, its ability to utilize data and intelligence from those sectors to influence FitBit users in the wearables space.

Google described the practice of leveraging cross-market data flows to exert biopower and influence user behavior in *The Selfish Ledger*. In the film, Google collected data from sensing units in people's smartphones, sent it back to central servers where it was incorporated into behavioral models, compared users' digital phenotypes to those models, and sent data to the Google Resolutions app to shift their behavior. Though Google claimed this scenario was hypothetical, the film reflects the company's current practices and its aspirations to assume decision making capacity on behalf of individuals and populations, nudging (and sludging) their behavior toward goals defined by its AI.

By acquiring new sensing and control units through conglomerate and concentric mergers, firms expand their corners of the digital panopticon to manipulate populations and march closer to biosupremacy. Consequently, antitrust regulators must develop tools to identify and constrain private biopower. They must revive and update the FTC's long-forgotten tools for scrutinizing conglomerate mergers, updating them to account for the addition of sensing and motor units.²⁸¹ Regulators should develop methods for identifying cross-market data

²⁷⁸ See *Mergers*, *supra* note 31.

²⁷⁹ *Id.*

²⁸⁰ See *id.*

²⁸¹ See KWOKA, *supra* note 5, at 110 (displaying a table of major acquisitions by the leading five U.S. tech companies, reflecting a diversity of markets and industries); see also Robert H. Lande & Sandeep Vaheesan, *Preventing the Curse of Bigness Through Conglomerate Merger Legislation*, 52 ARIZ. ST. L.J. 75, 79 (2020).

flows and dark patterns that concentrate biopower and generate harmful sludge. Because this approach renews antitrust's focus on merger control and revives its mandate to restrain non-economic power, the Neo-Brandeisian antitrust movement serves as an appropriate foundation.

E. The Role of Neo-Brandeisian Antitrust

Tim Wu and Lina Khan lead a vanguard of scholars called the Neo-Brandeisians who reject modern antitrust's obsession with price and consumer welfare. They are named for Justice Louis D. Brandeis who framed antitrust in terms of human values instead of purely economic terms.²⁸² The Neo-Brandeisians argue that antitrust should both return to its nineteenth and twentieth century roots, when it focused on constraining private power, and be updated for the twenty-first century by becoming more democratic and attuned to the demands of digital markets. In 2019, several Neo-Brandeisians outlined their shared beliefs in a document called The Utah Statement.²⁸³ This document describes their beliefs that private power must be subjected to democratic checks, that protection of fair competition promotes democracy and creates economic opportunity, and that overconcentration of private power is antidemocratic. The Utah Statement contends that antitrust, though not suitable for every situation, is a democratically enacted tool for achieving these aims.²⁸⁴

Despite general agreement among the Neo-Brandeisians regarding their overall goals, they differ in their approaches to achieving them. Wu argues for shifting the focus of U.S. antitrust policy from the consumer welfare standard back to the "protection of competition standard," that guided it from the 1890s through the 1970s.²⁸⁵ He calls for refocusing merger control on structural remedies by pursuing high-profile cases against large firms, implementing tougher enforcement standards, renewing presumptions against incipient monopolies, and democratizing merger review, which occurs largely in secret, by opening it up for public scrutiny.²⁸⁶

²⁸² See Greg Ip, *Antitrust's New Mission: Preserving Democracy, Not Efficiency*, WALL ST. J. (July 7, 2021), <https://www.wsj.com/articles/antitrusts-new-mission-preserving-democracy-not-efficiency-11625670424> [<https://perma.cc/Z99Q-NLKS>].

²⁸³ Teachout, *supra* note 11, at 1104.

²⁸⁴ *Id.* at 1105.

²⁸⁵ Wu, *supra* note 7, at 136.

²⁸⁶ *Id.* at 128-29 (quoting Louis D. Brandeis).

While Wu focuses on absolute bigness, structural relief, transparency, and public accountability, Khan takes a broader view that emphasizes conglomerate bigness and the private power it yields. She analyzes the structure of markets and their underlying dynamics, including how firms engage with different sectors.²⁸⁷ According to Khan: Seeking to gauge the firm's market role by isolating a particular line of business and assessing prices in that segment fails to capture either the true nature of a firm's dominance or the ways it leverages dominance in one market to gain influence in another.²⁸⁸ In this respect, she calls for reincorporating leverage theory into modern antitrust. In her article *Amazon's Antitrust Paradox*, Khan explains how Amazon leveraged its dominance in online retail to gain bargaining power and set favorable terms in the delivery sector.²⁸⁹

In an earlier article, Khan and co-author Zephyr Teachout argue that antitrust should regulate firms that abuse their dominance to impose "a form of private governance on the public," exerting power that constrains people's actions while being unaccountable to them.²⁹⁰ In this respect, they support reintegrating antitrust's original mandate to restrain private power into twenty-first century antitrust policy.

Critics of the Neo-Brandeisians argue that focusing antitrust on non-economic goals will undermine economic growth by discouraging vigorous competition.²⁹¹ Ariel Katz summarizes the critics' position as follows: "considering anything other than a narrow set of purely economic variables such as prices and output would 'politicize' antitrust law, thereby undermining its efficacy and legitimacy."²⁹² Konstantin Medvedovsky claims that abandoning the consumer welfare standard "would risk turning what is presently a data-driven, law enforcement exercise into something that is beholden to the political issues of the day."²⁹³ However, aligning antitrust with one school of thought over another is inherently political.²⁹⁴ It invariably promotes certain legal outcomes that determine how resources are distributed among different

²⁸⁷ See Khan, *supra* note 7, at 717.

²⁸⁸ *Id.* at 747.

²⁸⁹ *Id.* at 774.

²⁹⁰ See Teachout & Khan, *supra* note 10, at 58.

²⁹¹ See Carl Shapiro, *Antitrust in a Time of Populism*, 61 INT'L J. INDUS. ORG. 714, 745-46 (2018) (arguing that firms will be discouraged from competing vigorously out of fear that their success will trigger scrutiny from antitrust regulators).

²⁹² Katz, *supra* note 109, at 414.

²⁹³ KONSTANTIN MEDVEDOVSKY, HIPSTER ANTITRUST – A BRIEF FLING OR SOMETHING MORE? 6 (2018), <https://dev.competitionpolicyinternational.com/wp-content/uploads/2018/04/CPI-Medvedovsky.pdf> [<https://perma.cc/3GRY-GY9H>].

²⁹⁴ Katz, *supra* note 109, at 416.

actors within society, such as consumers and corporations.²⁹⁵ Politics cannot be removed from antitrust because antitrust policies govern how society manages the distribution of power between groups and individuals and determines how they compete with one another.²⁹⁶

The Critics of Neo-Brandeisian Antitrust also argue that it will render the antitrust enforcement incomprehensible. Medvedovsky claims that “[w]ithout the ‘true north’ of consumer welfare, enforcers would be left to balance multiple, often competing policy goals, as well as to weigh the evidence with respect to each one of those goals.”²⁹⁷ He and other critics contend that antitrust would become less predictable and more difficult to administer. However, Tim Wu claims such fears are exaggerated.²⁹⁸ He believes that whatever replaces the consumer welfare standard can be equally predictable.²⁹⁹ Besides “[d]ecades of practice have shown that the promised certainty of the Chicago method has not materialized.”³⁰⁰

Despite their critics, the Neo-Brandeisians are making an impact. Scholars, legislators, and regulators have come to see the Chicago School as a partisan reframing of antitrust policies that consolidated private power in the hands of a privileged few. Nobel Prize winning economist Joseph Stiglitz describes it as “a pure power grab” designed “to give free rein to corporate and business interests.”³⁰¹ Neoliberals achieved this goal by replacing antitrust’s original mandate with a new philosophy that changed how society perceives the purpose of antitrust law.³⁰² Rather than ensuring liberty and democracy for all, Neoliberals decided antitrust should promote efficiency as measured by the consumer welfare standard.³⁰³

Chicago School co-founder Richard Posner believed “the true meaning of justice is efficiency.”³⁰⁴ This Neoliberal perspective suffers from the same shortsightedness as Silicon Valley CEOs who believe

²⁹⁵ *Id.*

²⁹⁶ See, e.g., Sandeep Vaheesan, *The Twilight of the Technocrats’ Monopoly on Antitrust*, YALE L. REV. F. 980, 985 (2018) (arguing that antitrust is unavoidably political because it regulates markets and determines “whom the law benefits and to what ends,” which inevitably requires making moral and political judgements).

²⁹⁷ MEDVEDOVSKY, *supra* note 293, at 6.

²⁹⁸ WU, *supra* note 7, at 134.

²⁹⁹ *Id.*

³⁰⁰ WU, *supra* note 7, at 134.

³⁰¹ See JOSEPH E. STIGLITZ, PEOPLE, POWER, AND PROFITS: PROGRESSIVE CAPITALISM FOR AN AGE OF DISCONTENT (2019).

³⁰² *Id.*

³⁰³ *Id.*

³⁰⁴ *Id.*

surveillance and AI can solve every social problem. The Neo-Brandeisians are pushing back against this legacy, and their influence can be seen in antitrust reports from Congress and leading economic think tanks.³⁰⁵ Their philosophy is also evident in ongoing lawsuits filed by states and federal agencies against Facebook and Google.³⁰⁶ However, though these lawsuits reflect renewed interest in regulating Big Tech mergers, they are not groundbreaking.

According to law professor Doug Melamed, the “U.S. v. Google complaint is a very conservative complaint; [it] doesn’t break any new legal ground of any consequence.”³⁰⁷ He and other antitrust scholars see it as a relatively traditional lawsuit comparable to the government’s historic 2001 case against Microsoft.³⁰⁸

Like U.S. v. Google, suits filed by U.S. attorneys generally focus narrowly on the markets for search and advertising. Though this approach is not wrong from the perspective of prevailing legal doctrine, it is unlikely to significantly disrupt Google’s power over society.³⁰⁹ As mentioned previously, the European Commission’s approval of the Google-FitBit merger illustrates how focusing on individual markets does not address the biopower generated through conglomerate and concentric mergers.

In 2021, President Biden appointed Wu to the National Economic Council to develop U.S. technology and competition policy.³¹⁰ A few months later, Biden named Khan chairwoman of the FTC.³¹¹ Khan’s appointment triggered intense reactions from Facebook and Amazon.³¹²

³⁰⁵ See, e.g., SUBCOMM. ON ANTITRUST, *supra* note 124, at 19-20 (recommending a renewed emphasis on structural remedies, presumptions against future mergers, and the role of antitrust enforcement in promoting democracy).

³⁰⁶ See McKinnon, *supra* note 4.

³⁰⁷ The Federalist Society, United States v. Google: Examining the Historic Antitrust Case Against Big Tech, YOUTUBE (Nov. 6, 2020), <https://www.youtube.com/watch?v=Dgih1jM05mA&list=PLvLK5ZuczSArx6VwX6a-bKUZsEJEOSilh&index=40> [<https://perma.cc/7WED-BW5F>].

³⁰⁸ *Id.*

³⁰⁹ *Id.*

³¹⁰ Lauren Feiner, *Big Tech Critic Tim Wu Joins Biden Administration to Work on Competition Policy*, CNBC (Mar. 5, 2021, 8:41 AM EST), <https://www.cnbc.com/2021/03/05/big-tech-critic-tim-wu-joins-biden-administration-to-work-on-competition-policy.html> [<https://perma.cc/32GF-R3WK>].

³¹¹ David McCabe & Cecilia Kang, *Biden Names Lina Khan, a Big-Tech Critic, as F.T.C. Chair*, N.Y. TIMES (June 15, 2021), <https://www.nytimes.com/2021/06/15/technology/lina-khan-ftc.html> [<https://perma.cc/EUY6-YUB8>].

³¹² Lauren Feiner, *Facebook Asks for FTC Chair Lina Khan to be Recused From its Antitrust Case*, CNBC (July 14, 2021), <https://www.cnbc.com/2021/07/14/facebook-asks-for-ftc-chair-lina-khan-to-be-recused-from-its-antitrust-case.html>.

Claiming that her past criticisms of each company made her biased, Amazon sought Khan's recusal from an ongoing probe into its business practices, and Facebook sought her recusal from the FTC's ongoing lawsuit against it.³¹³ After a judge dismissed the FTC's original complaint against Facebook, Khan revised and refiled it, and the company again moved to have the case dismissed because the FTC had failed to recuse her.³¹⁴

Though Wu and Khan's appointments may be watershed moments, U.S. antitrust enforcement remains rooted in the Chicago School tradition. While regulators' eyes are fixed on Google and Facebook's search and advertising business, and government resources are tied up battling their armies of corporate lawyers, Google and Facebook will continue to invest in other markets. They will expand their biopower, and move closer to biosupremacy, while the ongoing lawsuits create a distraction for Congress, regulators, and the public. After Haugen's revelations sparked a new round of Congressional hearings on Facebook's conduct, Zuckerberg announced the company would change its name to reflect its role in crafting the metaverse.³¹⁵ While Congress and the FTC sink resources into scrutinizing Facebook's existing technologies and business models, Zuckerberg looks to the future. If U.S. antitrust retains its focus on consumer welfare, the government will be unprepared. Part III of this Article makes recommendations to bridge the gap between existing antitrust doctrine and the needs created by the emerging data economy that will drive the metaverse and further consolidate biopower.

III. UPDATING ANTITRUST TO REGULATE DIGITAL BIOPOWER

This Part makes recommendations to update antitrust law for the Digital Age by incorporating concepts from data protection, behavioral economics, and Foucault's biopolitics. The first set of proposals focuses on the costs imposed on consumers by panoptic surveillance. It urges

asks-for-ftc-chair-lina-khan-to-be-recused-from-its-antitrust-case.html [https://perma.cc/4XVG-Y4MK].

³¹³ *Id.*

³¹⁴ Rishi Iyengar, *Facebook Asks Court to Dismiss FTC Antitrust Complaint*, CNN (Oct. 4, 2021, 4:32 PM EST), <https://www.cnn.com/2021/10/04/tech/facebook-ftc-antitrust-dismiss/index.html> [https://perma.cc/5KLQ-ZTXB].

³¹⁵ Shirin Ghaffary, *Facebook's Name Change Plan Reflects its Real Priorities*, Vox (Oct. 20, 2021, 4:45 PM EDT), <https://www.vox.com/recode/2021/10/20/22737168/facebook-name-change-metaverse-zuckerberg-frances-haugen-whistleblower> [https://perma.cc/7UKY-DZXX]; see also Isaac, *supra* note 268 (reporting that Facebook had changed its name to Meta).

courts and antitrust regulators to acknowledge that when people access “free” online services, they usually pay with their data instead of currency. Consequently, at the very least, antitrust regulators should expand the concept of consumer welfare to accommodate the cost of deceptive data collection. To that end, this Part introduces a novel framework for calculating the costs imposed on consumers by panoptic surveillance. The first Section also urges courts and regulators to analyze the impact of deceptive and coercive data collection on competition and product quality, variables that many antitrust scholars agree should fall within the scope of consumer welfare.

The second set of recommendations focuses on non-price effects such as quality, lock-in effects, and barriers to entry. When platforms surreptitiously surveil people and coerce them to act against their interests, they reduce the quality of their products and services. Moreover, because dark patterns constrain user behavior and unfairly confer competitive advantages on platforms that deceive users, they are often anticompetitive. Consequently, regulators should develop tools to evaluate dark patterns and incorporate them into merger review. To further promote competition and improve quality, they should force platforms to be interoperable with their competitors while providing users with straightforward ways to access and download their data. Forced interoperability and data portability prevent panoptic platforms from becoming walled gardens that restrict user migration contributing to user lock-in, which further concentrates biopower.

The third set of recommendations focuses on revitalizing merger control by reviving tools for scrutinizing conglomerate mergers and updating them for the Digital Age. Though regulating conglomerate bigness fell out of favor with the rise of the Chicago School, it is now necessary for limiting the concentration of sensing and control units to constrain private biopower. Due to the specialized nature of data, AI, and the internet of things, Congress should form a data competition agency to advise U.S. antitrust regulators on these matters.

Critics might argue that surveillance, data flows, and AI-based inferences are better handled by data protection regulation than by antitrust law. However, this criticism misinterprets the current role of data protection law and ignores antitrust’s original mandate to constrain private power. Data protection laws, such as the European Union’s General Data Protection Regulation (“GDPR”), promote the flow of user data and give data subjects limited control over where the information

flows, how it is processed, and how it is used.³¹⁶ However, data protection law has not been concerned with power, which was historically the domain of antitrust. Moreover, modern antitrust law is obsessed with price, and when consumers access “free” internet products and services, they pay with their data, a cost that should be acknowledged and accounted for by economists and antitrust regulators, making antitrust an appropriate means for regulating surveillance, data flows, and AI-based inferences.

Many antitrust scholars agree that data protection law can inform antitrust regulation in areas where they overlap.³¹⁷ Lina Khan recommends strengthening merger control by analyzing how firms use information. “One way to address the concern about a firm’s capacity to cross-leverage data is to expressly include it in merger review,” says Khan.³¹⁸ “It could make sense for agencies to automatically review any deals that involve exchange of certain forms (or certain quantities) of data.”³¹⁹ The European Commission took this approach while analyzing the Google-FitBit merger. However, as discussed above, its narrow remedies overlooked how Google can leverage its dominance in other markets to influence FitBit users and vice versa.

Though innovative and important, Khan’s analysis of how data flows affect private power is limited. Moreover, the Neo-Brandeisians have not addressed ubiquitous surveillance or the manipulation of consumers through coercive choice architecture in their analyses or proposals. Consequently, this Part builds on their foundation by incorporating biopolitics and data flows into antitrust policy. It argues that regulators must analyze how mergers affect a firm’s ability to secretly monitor people and influence their behavior. In other words, U.S. antitrust agencies should analyze how firms acquire sensing and

³¹⁶ See, e.g., Stephanie Hare, *These New Rules Were Meant to Protect Our Privacy. They Don’t Work*, GUARDIAN (Nov. 10, 2019, 3:30 AM EST), <https://www.theguardian.com/commentisfree/2019/nov/10/these-new-rules-were-meant-to-protect-our-privacy-they-dont-work> [https://perma.cc/2FQG-R5QV] (stating that the GDPR gives people limited knowledge of, and control over, where their data flows, yet it does little to stop personal data from being used to monitor, manipulate, and exploit people). The GDPR could have better protected personal data by making privacy its default. However, that would impede the ability of companies and governments to monitor, predict, and influence people’s behavior. *Id.*

³¹⁷ See OECD Competition Division, *How Can Privacy and Data Protection Be Integrated into Competition Law?*, YOUTUBE (Oct. 29, 2018), <https://www.youtube.com/watch?v=bN3m7YBtRJE&list=PLvLK5ZuczSArx6VwX6a-bKUZsEJEOSilh&index=15> [https://perma.cc/9SMF-HBAP].

³¹⁸ Khan, *supra* note 7, at 792.

³¹⁹ *Id.* at 793.

control units through conglomerate and concentric mergers to acquire biopower and how they use coercive choice architecture to exert it.

A. *Maximizing Consumer Welfare by Minimizing Surveillance and Behavioral Profiling*

This Section argues that minimizing panoptic surveillance and unauthorized behavioral profiling increases consumer welfare, even as measured under the prevailing consumer welfare standard. In the surveillance-based economy, people often access platforms without paying a fee. Instead, they pay with their data, which is collected by a platform's sensing units. This Section presents a framework for analyzing the cost to consumers of collecting and processing data in exchange for access to products and services. It argues that like a one-time payment or ongoing subscription fee, the collection and processing of user data imposes costs on consumers (the *data cost*). However, unlike the costs associated with payments or subscription fees, which usually remain constant, the data cost often increases over time and in response to changes in other variables. Specifically, the data cost increases under the following conditions: 1) when more data is collected, 2) when data is collected over longer periods of time, 3) when data is harvested deceptively, 4) when the data collected or the inferences drawn from it are sensitive, 5) when data is enriched with information from other sources, and 6) when artificial intelligence is used to refine the data.

These six variables associated with data collection and processing (volume, duration, deception, sensitivity, enrichment, and AI refinement) contribute to the data cost imposed on consumers for accessing a product or service. Moreover, when they are minimized, the data cost is minimized.

1. Data Volume (V)

There is a positive correlation between the volume of data collected and the cost to consumers. This relationship follows from the fact that since data is valuable, collecting more of it increases the overall value of the information harvested and the harm done to consumers when it is used against their interests. Additionally, the larger the volume of data collected, the greater the number of inferences that can be drawn from the information further increasing its value and associated risk.

2. Time Interval (T)

Because the value of data is cumulative, the data cost to consumers increases with time, as the duration of surveillance is extended. Consumers who use platforms such as Facebook, Gmail, or Amazon for years have contributed large volumes of data, which allows platforms to make more detailed inferences and predictions about them. Consequently, their data cost per unit time may be higher than that of a new user who lacks an established history with the platform. For new users, platforms have a smaller cross-section of their behavior for analysis by behavioral algorithms.

3. Data Sensitivity (S)

Sensitive data, such as health information and financial data, is arguably more valuable than mundane information such as the breakfast cereals consumers prefer. People tend to guard sensitive data more closely because it is intimate, it might be embarrassing, and it provides insights into other areas of their lives such as their sexual, employment, and substance use histories. As a result, collecting sensitive data, or inferring it from relatively mundane data, imposes higher data costs on consumers.

4. Deception During Data Collection (D)

Platforms use deceptive dark patterns and other coercive choice architecture to collect more data from consumers than they would otherwise provide. Oftentimes, deception yields sensitive information about people's health, finances, sexuality, and spiritual practices. Therefore, when platforms use deceit to collect data from people, they increase the data cost by increasing the volume and sensitivity of data collected, because consumers would otherwise prefer to maintain its confidentiality. Minimizing the use of dark patterns and limiting expansion of control networks that enable them are two means of restricting deceptive data collection and reducing data costs to consumers. Limiting expansion of control networks by scrutinizing mergers that consolidate motor units will be discussed further in the Section on conglomerate merger control.

5. Enrichment of Data (E)

Platforms increase the value data collected by enriching it with information from other sources.³²⁰ Enriching data can increase the volume and sensitivity of the information while providing a wider snapshot of behavior for analysis by artificial intelligence, allowing platforms to draw broader, more accurate, and more sensitive inferences. Consequently, enriching data with information from other sources increases the data cost. Minimizing the expansion of sensing networks through conglomerate mergers is one means through which antitrust can limit the enrichment of data with information from other sectors.

6. Refinement of Data (R)

Platforms use artificial intelligence, such as machine learning and natural language processing, to draw inferences from the data collected from consumers, often without their knowledge or consent.³²¹ Refining data to produce inferences increases its value to tech companies and increases the data cost to consumers. Like enrichment and deceptive data collection, the refinement of user data can be limited through conglomerate merger control by scrutinizing mergers that consolidate a firm's ability to concentrate the AI-related components of its sensing networks.

One might argue that when the data cost to consumers is minimized, they benefit from a *privacy surplus* that is analogous to consumer surplus. While consumer surplus equals the difference between the price paid by a consumer and the price the consumer was willing to pay, privacy surplus is defined as the difference between the data cost paid by a consumer and the data cost the consumer was willing to pay. Consumers do not necessarily spend their privacy surplus on goods and services the way they might spend a financial surplus. Instead, they may use their privacy surplus to access opportunities that might otherwise be foreclosed if the information that contributed to their data surplus

³²⁰ See Chris Jay Hoofnagle & Jan Whittington, *Free: Accounting for the Costs of the Internet's Most Popular Price*, 61 UCLA L. REV. 606, 610 (2014); Sam Schechner & Mark Secada, *You Give Apps Sensitive Personal Information. Then They Tell Facebook*, WALL ST. J. (Feb. 22, 2019, 11:07 AM ET), <https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636> [https://perma.cc/EUP4-3GUN] (describing how Facebook accesses the personal information of consumers using third party smart phone apps, including the Flo Period & Ovulation Tracker and the Realtor.com app).

³²¹ See Marks, *supra* note 138, at 1000.

was acquired or inferred by panoptic platforms. Technology companies increasingly use data for reputational scoring and automated processing that constrains the options available to consumers.

B. Increasing Competition and Product Quality by Restricting Panoptic Surveillance and Coercive Choice Architecture

This Section argues that internet-enabled products that deceive and exploit users are inherently of lower quality than comparable products that do not deceive or exploit consumers. For instance, internet-enabled smart refrigerators are designed to provide value to users by keeping food cold, monitoring their contents, and ordering products such as milk and eggs when supplies run low. A smart refrigerator that does these tasks well is a high-quality smart refrigerator. However, smart refrigerators can also secretly monitor the frequency of users' late-night snacking and junk food consumption and share that information with potential employers, lenders, and insurance companies. In that case, a smart fridge deceives users by collecting and inferring more information than they agreed to provide, and it exploits people by using their data against them. Consequently, it is a lower quality product than a smart fridge that does not deceive users, protects their privacy, and does not exploit them by misusing their data.

Similarly, a social media platform that allows users to communicate securely with friends and family members, safeguards their information, and allows them to easily access their data and transfer it to competing services is a high-quality platform. However, a social media platform that continuously monitors users, harvests their data, profiles them, and exploits their information is a low-quality service regardless of how well it allows users to connect and communicate. To ensure that consumers have a variety of high-quality products from which to choose, regulators should inhibit the use of dark patterns and the consolidation of sensing and motor units that surveil and coerce consumers.

Regulators are starting to acknowledge the impact of deceptive surveillance on product quality and consumer welfare. In their 2020 complaint against Facebook, forty-eight state attorneys general argue that Facebook "diminished consumer welfare through reduced quality, degraded privacy protections, reduced choice, and suppressed innovation."³²² However, critics of this view argue that quality is too

³²² Complaint at 73, *New York v. Facebook, Inc.*, No. 1:20-cv-03589-JEB (D.C. Cir. Dec. 9, 2020), ECF No. 4; see Press Release, Letitia James, N.Y. Atty Gen., Attorney General James Leads Multistate Lawsuit Seeking to End Facebook's Illegal Monopoly

difficult to define, and consumers are capable of determining how much data they are willing to sacrifice to access free products and services.³²³

Those who argue that surveillance does not affect quality, and that quality is too nebulous to define, are either being disingenuous, or they lack an understanding of how modern platforms collect and use consumer information. Platforms routinely make detailed inferences about users without their knowledge and use dark patterns to coerce them into doing things they would rather not do. It strains credulity to categorize deceptive platforms that limit user autonomy as high-quality products, regardless of whether some of their practices improve efficiency, unless one supports the dystopian vision of data analytics depicted in Google's *The Selfish Ledger*.

Advertising networks and data brokers also deploy nudges and dark patterns, discouraging users from opting out of data collection, by requiring them to mail physical letters or making opt-out instructions difficult to find and follow. In other words, when consumers attempt to opt-out of panoptic surveillance, they encounter a thick stream of sludge. Even worse, opting out requires users to contact hundreds of firms individually and to continuously update their opt-out requests. Not all companies provide opportunities for people to opt-out, and there is no guarantee that companies will honor opt-out requests because there is so little oversight.

C. Breaching Walled Gardens with Data Portability and Platform Interoperability

Many internet platforms operate as walled gardens. Facebook, Instagram, YouTube, and Twitter are popular examples that nudge or require users to sign-in to proprietary, closed ecosystems that function as small-scale versions of the global digital panopticon. For as long as users remain confined within walled gardens, they are watched, analyzed, and influenced to generate biopower. If users or their data are permitted to leave platforms too easily, then the platforms influence over people and populations is diminished. Consequently, platforms are incentivized to raise barriers to easy migration of users and their data.

Data portability is the ability of users to download their information from a platform and transport it elsewhere, for instance, to a hard drive for storage, or to a competing platform when they wish to switch

(Dec. 9, 2020), <https://ag.ny.gov/press-release/2020/attorney-general-james-leads-multistate-lawsuit-seeking-end-facebooks-illegal> [https://perma.cc/GN5X-B5LC].

³²³ See Geoffrey A. Manne & R. Ben Sperry, *The Problems and Perils of Bootstrapping Privacy and Data into an Antitrust Framework*, 2015 CPI ANTITRUST CHRON. 1, 3.

services. In practice, panoptic platforms make it difficult, if not impossible, to achieve data portability. Common excuses include the technical complexity of implementation, risks to user privacy, and claims that platforms already offer data portability.

Though some platforms offer limited data portability, they often use sludge to prevent users from migrating elsewhere. They make download links difficult to find, require users to wait days before their data becomes available, force them to download information in several batches, output the data in difficult to read formats, nudge users to change their minds, and provide incomplete data sets.³²⁴ Generating sludge in this manner generates biopower and is a form of exclusionary conduct that should be regulated by antitrust law. Competitors who are honest with users and do not deploy dark patterns are placed at an unfair disadvantage because they choose not to manipulate people, and they cannot retain users as effectively.

Facebook, Apple, Google, Microsoft, and Twitter are collaborating through a program called the Data Transfer Project (“DTP”) to build a framework that “can connect any two online service providers.”³²⁵ Like the content cartel composed of leading social media platforms, the DTP constitutes a data transfer cartel and bio-oligopoly because through this collaboration, platforms are fixing a portion of the data cost imposed on users. By restricting the quantity and quality of data that can be transferred, they increase the data costs imposed on consumers. This activity should be viewed in the same light as price-fixing, which carries harsh penalties under antitrust laws. Moreover, by collaborating to shape norms surrounding how data transfers occur, the DTP exerts biopower over billions of internet users. For that reason, data transfer standards should be determined democratically by public institutions instead of data transfer cartels composed of for-profit corporations with a vested interest in shaping standards for their benefit.

Interoperability refers to the ability of users to communicate with people who use competing platforms. For example, a Facebook user might wish to communicate with friends on LinkedIn who lack Facebook accounts. However, because the platforms are not interoperable, this kind of cross-platform communication is not possible. Common excuses for a lack of interoperability include

³²⁴ See Nitasha Tiku, *What’s Not Included in Facebook’s ‘Download Your Data,’* WIRED (Apr. 23, 2018, 7:00 AM), <https://www.wired.com/story/whats-not-included-in-facesbooks-download-your-data/> [<https://perma.cc/JAT3-V5EZ>] (describing the limited data sets Facebook makes available to users through its data portability tool).

³²⁵ *About Us,* DATA TRANSFER PROJECT, <https://datatransferproject.dev/> (last visited Jan. 1, 2021) [<https://perma.cc/GB93-7RAC>].

technical complexity, risks to user privacy, and an alleged lack of consumer demand. However, interoperability is already offered in other sectors demonstrating that technical challenges can be overcome.

In 2002, CEO Jeff Bezos sent a memo to his employees mandating that Amazon's many departments be made interoperable. It seemed like an impossible task. However, instead of telling employees how to do it, Bezos made only the desired outcome clear.³²⁶ He declared that there would be no exceptions, and “[a]nyone who doesn't do this will be fired. Thank you; have a nice day!” It worked, and similar approaches must be taken with panoptic platforms because they are incentivized to resist interoperability and data portability.

Interoperability could promote competition because startups could more easily compete with large platforms for a share of their users. Moreover, interoperability disrupts panoptic architecture and opens markets to competitors that respect and protect user privacy. It could even force dominant platforms to take privacy more seriously to remain competitive.

There are existing blueprints for interoperable services that protect user privacy. One ecosystem uses an open-source protocol called Activity Pub that supports a variety of decentralized social media platforms.³²⁷ Together, they form a constellation of services called the Fediverse. Within this ecosystem, there are open-source analogs of Twitter, Facebook, and Instagram, which are called Mastodon, Friendica, and PixelFed.³²⁸ However, due to a lack of interoperability between panoptic platforms and these open-source alternatives, and a functional lack of data portability, users are discouraged from migrating from panoptic platforms to non-panoptic alternatives. Nevertheless, the growing user base of the Fediverse reflects demand for alternatives that do not spy on users or subject them to targeted advertisements and other forms of manipulative choice architecture.

An accessible means of transitioning from panoptic platforms to less harmful alternatives is essential to democracy, competition, human autonomy, and consumer welfare. It would dilute concentrated

³²⁶ Grace F. Schroeder, *What Year Did Bezos Issue the API Mandate at Amazon?*, MEDIUM: SLINGR (July 7, 2016), <https://medium.com/slingr/what-year-did-bezos-issue-the-api-mandate-at-amazon-57f546994ca2> [https://perma.cc/DJ3L-HZDC].

³²⁷ See Darius Kazemi, *Decentralizing Social Interactions with ActivityPub*, MOZILLA HACKS (Nov. 20, 2018), <https://hacks.mozilla.org/2018/11/decentralizing-social-interactions-with-activitypub/> [https://perma.cc/V5F7-Z3CQ].

³²⁸ Simply Explained, *Distributed Social Media – Mastodon & Fediverse Explained*, YOUTUBE (Mar. 5, 2019), <https://www.youtube.com/watch?v=S57uhCQBEk0&list=PLvLK5ZuczSArx6VwX6a-bKUZsEJEOSilh&index=7&t=0s> [https://perma.cc/W92D-NAQH].

biopower by distributing it among numerous competitors. This Section discusses two proposed approaches to implementing data portability and platform interoperability: The Augmenting Compatibility and Competition by Enabling Service Switching (“ACCESS”) Act and the Consumer Online Privacy Rights Act (“COPRA”).³²⁹

1. The Augmenting Compatibility and Competition by Enabling Service Switching (“ACCESS”) Act

The ACCESS Act was introduced in 2019 by Josh Hawley and Democratic Senators Mark Warner and Richard Blumenthal.³³⁰ According to Blumenthal, the Act “would empower consumers to finally stand up to Big Tech and move their data to services that respect their rights.”³³¹ According to Warner, “As a former cell phone guy, I saw what a game-changer number portability was for that industry.” Warner claims that “[b]y making it easier for social media users to easily move their data or to continue to communicate with their friends after switching platforms, startups will be able to compete on equal terms with the biggest social media companies.”³³²

By mandating data portability and platform interoperability, the ACCESS Act would increase competition between digital platforms. However, there are several problems with the Act that would reduce its effectiveness at dispersing digital biopower. The Act would create a new class of intermediaries called custodial third-party agents who facilitate data transfers. According to Blumenthal, “empowering trusted custodial companies to step in on behalf of users to better manage their accounts across different platforms will help balance the playing field between consumers and companies.” In other words, “by enabling portability, interoperability, and delegatability, this bill will help put consumers in the driver’s seat when it comes to how and where they use social

³²⁹ Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act, S. 2658, 116th Cong. (2019); Consumer Online Privacy Rights Act, S. 2968, 116th Cong. (2019).

³³⁰ Tobias Hoonhout, *Hawley Introduces Bipartisan Bill Empowering Users to Withdraw Their Data from Social Media Giants*, NAT'L REV. (Oct. 22, 2019, 11:26 AM), <https://www.nationalreview.com/news/hawley-introduces-bipartisan-bill-empowering-users-to-withdraw-their-data-from-social-media-giants/> [https://perma.cc/6STL-Y8SE].

³³¹ Press Release, Mark R. Warner, U.S. Sen. from Va., Senators Introduce Bipartisan Bill to Encourage Competition in Social Media (Oct. 22, 2019), <https://www.warner.senate.gov/public/index.cfm/2019/10/senators-introduce-bipartisan-bill-to-encourage-competition-in-social-media> [https://perma.cc/XD3X-HJRD].

³³² Hoonhout, *supra* note 330.

media.³³³ However, in addition to decreasing barriers to migration, creating a new class of internet intermediaries would expand the digital panopticon, which could negate any benefits gained through increased data portability and interoperability.

The ACCESS Act defines a custodial third-party agent as an “entity that is duly authorized by a user to interact with a large communications platform provider on that user’s behalf to manage the user’s online interactions, content, and account settings.”³³⁴ Custodial third-party agents would have access to the entirety of a user’s data, and likely the data of users across multiple platforms, potentially making them more powerful than many third parties with whom platforms currently share user information, perhaps even more powerful than some existing platforms.

2. The Consumer Online Privacy Act (“COPRA”)

The Consumer Online Privacy Act (“COPRA”) was introduced in 2019 by Senator Maria Cantwell. It is an ambitious bill that attempts to achieve many privacy-related goals. Data portability is covered only briefly, and the Act lacks provisions for interoperability.

Section 105 of the Act creates a right to data portability that would require covered entities to export user data after receiving a verified request from a user.³³⁵ The right excludes the export of “derived data,” which the Act defines as “data that is created by the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information . . .”³³⁶ Consequently, AI-mediated inferences would likely fall within this exception, which demonstrates that the Act’s drafters intend for inferences to remain under control of the platforms that derive them rather than the users about which inferences are drawn. This drafting decision concentrates biopower and is anticompetitive because it allows companies that draw inferences to retain exclusive control over the information.

Though critics complain that data portability and platform interoperability are burdensome to achieve, they are necessary features of modern internet platforms. Platforms should make data portability easy and promote interoperability with their competitors, or they should be unable to operate in the United States. Moreover, the obstruction of data portability and interoperability should be framed in

³³³ Warner, *supra* note 331.

³³⁴ ACCESS Act, S. 2658, 116th Cong. § 2 (2019).

³³⁵ *Id.* § 105.

³³⁶ *Id.* § 2.

terms of their effects on biopower and competition. Antitrust regulators should analyze those effects during merger review and require merging firms to implement data portability and interoperability. However, care must be taken to ensure that their implementation disperses digital biopower instead of concentrating it.

D. Inhibiting Coercive Choice Architecture

Congress and antitrust regulators must acknowledge that coercive choice architecture concentrates private power and prevents consumers from exercising autonomy. Dark patterns and other forms of sludge increase switching costs for users by discouraging them from downloading their data, migrating to competing platforms, and deleting their accounts. Through digital nudges, platforms coerce people to reveal personal information, increasing the volume of data that flows to tech company servers. By generating sludge, platforms prevent people from exercising their true preferences and coerce them to act against their interests. These practices inhibit competition by raising entry barriers for companies that choose not to deceive and manipulate consumers. Accordingly, Congress should task regulators with developing tools to identify and quantify dark patterns and other mechanisms of coercive choice architecture that concentrate biopower.

Researchers are already developing tools to identify and analyze dark patterns. One team at Princeton University developed a semi-automated method for identifying dark patterns on over 11,000 retail shopping websites.³³⁷ The greatest obstacle to developing these tools is distinguishing between socially beneficial and harmful applications of biopower, which would require courts and regulators to identify when helpful nudges become harmful sludge. Examples of useful nudges and expressions of biopower are plentiful. They include choice architecture, such as well-placed signs, that encourages people to wash their hands and wear masks to prevent the spread of COVID-19.

Useful nudges deployed over populations can promote educational opportunities, scientific discovery, and professional advancement. When used for public health purposes, they can reduce death rates from motor vehicle accidents, smoking, and alcohol poisoning. However, examples of harmful nudges and expressions of biopower are equally plentiful. They include dark patterns that keep people engaged with

³³⁷ See Arunesh Mathur, Gunes Acar, Michael J. Friedman, Elena Lucherini, Jonathan Mayer, Marshini Chetty & Arvind Narayanan, *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, 3 PROC. ACM ON HUM.-COMPUT. INTERACTION 81:1, 81:1-2 (2019).

digital services for unhealthy periods of time, choice architecture that coerces users to reveal more information than they would want to disclose, and targeted advertisements and newsfeeds that exploit people's mental and physical susceptibilities.

Determining where to draw the line between useful nudges and harmful sludge is paramount, and the distinction likely turns on their effects on user autonomy, dignity, deception, and exploitation.³³⁸ Some degree of manipulation is not categorically bad for individuals or society. Beneficial uses of biopower can manipulate people without deceiving them while respecting their autonomy. For instance, a smoking cessation app that helps people fight cravings for cigarettes is one example that can decrease morbidity, extend one's lifespan, and reduce healthcare costs. Even though the app may manipulate users to discourage them from smoking, it does not deceive them because they use it willingly, and it simultaneously empowers them. If the app is effective, it provides a competitive advantage to the developer that is earned fairly.

In contrast, harmful and oppressive uses of biopower manipulate people by deceiving them or restricting their autonomy. Dark patterns deployed to coerce people into disclosing more data than they intend to share exploit millions of people daily. They restrict autonomy, foreclose personal and professional opportunities, and can impact one's physical and mental health. Because they exploit people through deception and coercion, dark patterns provide competitive advantages that are unfairly earned.

Operationalizing these concepts will be challenging and should be the subject of future research. It will require regulators to familiarize themselves with dark patterns and data flows. Some scholars are developing tools to quantify and categorize dark patterns.³³⁹ Jamie Luguri and Lior Strahilevitz believe a quantitative approach to identifying dark patterns is achievable.³⁴⁰ However, incorporating these tools into competition and antitrust regulation will require specialists. For these reasons, Congress should create a digital competition agency that can lend expertise to antitrust authorities.

³³⁸ See CASS R. SUNSTEIN: THE ETHICS OF INFLUENCE: GOVERNMENT IN THE AGE OF BEHAVIORAL SCIENCE 3 ("Ethical states focus above all on four values: welfare, autonomy, dignity, and self-government.").

³³⁹ See Mathur, *supra* note 337, at 81:2; see also Luguri & Strahilevitz, *supra* note 94, at 43.

³⁴⁰ See Luguri & Strahilevitz, *supra* note 94, at 45.

The following Section explains how these concepts should be incorporated into merger review to update antitrust enforcement for the Digital Age.

E. Revitalizing Merger Control to Block Cross-Market Data Flows, Minimize Coercive Choice Architecture, and Prevent Biosupremacy

This Section proposes updates to antitrust doctrine consisting of novel structural and behavior remedies that acknowledge cross-market data flows and dark patterns. As described above, conglomerate and concentric mergers are means through which firms expand their surveillance and control networks. By purchasing firms that produce sensing units in new markets, acquiring firms enhance their surveillance of consumers in markets where they previously lacked access, establishing cross-market data flows. Similarly, by acquiring firms that produce motor units in new markets, they exert control in markets where they previously lacked influence, establishing beachheads through which they can exert biopower to manipulate populations and shift social norms.

1. Structural Remedies

Congress and the antitrust agencies should revitalize tools of conglomerate merger control from the 1960s and update them for the Digital Age. Moreover, Congress should introduce legislation to regulate concentric mergers, a more recently acknowledged phenomenon that is increasingly common in digital economies.

Through structural remedies, regulators should halt conglomerate and concentric mergers that expand sensing and control networks to concentrate biopower. To do so, they must determine the point at which networks of sensing and control become too expansive, and the point at which biopower becomes so concentrated that biosupremacy is within reach. In other words, regulators must develop methods for quantifying biopower and establish thresholds for triggering merger review. To that end, tools for quantifying dark patterns will be beneficial because the greater a firm's ability to deploy dark patterns, and the more effective those patterns, the greater its ability to concentrate and exert biopower.

Some antitrust scholars recommend creating thresholds for merger control related to market concentration and the size or value of firms.³⁴¹ For instance, Tim Wu recommends reviving structural presumptions,

³⁴¹ See WU, *supra* note 7, at 128-29.

“such as a simple but *per se* ban on mergers that reduce the number of major firms [in an industry] to less than four.”³⁴² However, variables such as bigness, value, and market concentration do not necessarily correlate strongly with biopower, and regulators should expand their view of digital economies by stepping back to observe how different markets interact to generate power. Instead of being guided by market share alone, or by market dominance, regulators should look at the global market for biopower and analyze the extent to which mergers expand each firm’s share of it. Because biopower is difficult to quantify, sensing and motor units in different industries can serve as proxies for it.

Antitrust agencies should revise their declaration that mergers below a certain threshold size raise no competitive concerns. In other words, it should not be the size of a firm that matters most. Instead, the quantity and diversity of sensing and motor units added to its networks, and how it will use them to access data and exert biopower, should be primary considerations for triggering merger control.

To constrain digital biopower, antitrust agencies should analyze and regulate conglomerate bigness, requiring them to assess a firm’s market diversification, including its portfolio of sensing and motor units and the sectors in which they operate. Instead of focusing on the leverage created through tying and bundling arrangements, as was common in the 1960s and 70s, regulators should focus on how firms leverage cross-market data flows that concentrate and exert biopower.

Presumptions could be implemented to block mergers that concentrate sensing and motor units in a certain number of sectors. For instance, if an acquiring firm accesses data flows and exerts control through sensing and motor units in three industries, and a proposed merger would increase the number of industries from which it draws data and exerts control to more than four, then the merger could be presumed to overconcentrate biopower, and it could be blocked. Such presumptions should be irrebuttable or nearly-irrebuttable. Merger control should also assess the impact of acquisitions on firms’ ability to use dark patterns and other forms of coercive choice architecture.

2. Behavioral Remedies

In addition to structural remedies, antitrust agencies should impose conduct or behavioral remedies on merging firms to limit the concentration of biopower.³⁴³ Behavioral remedies allow a merger to continue provided that the resulting firm abstains from engaging in

³⁴² See *id.* at 131-33.

³⁴³ See KWOKA, *supra* note 5, at 93.

certain anticompetitive behaviors.³⁴⁴ The European Commission's behavioral remedies for the Google-FitBit merger require the merged firm to abstain from using FitBit data for advertising. In other words, it requires Google to create a data silo. However, as described above, this behavioral remedy is poorly adapted to the goal of restraining biopower because it fails to account for how firms like Google leverage data to exert dominance in numerous markets. Nevertheless, more effective behavioral remedies, including more robust data silos, could be implemented to constrain biopower. For instance, the European Commission could have required Google to use FitBit data only for fitness tracking by users. A smaller, more robust data silo could block cross-market data flows and prevent Google from leveraging FitBit data to influence other markets and using data from those markets to influence FitBit users. Antitrust regulators could also prohibit companies from using dark patterns and require them to submit to regular sludge audits as conditions on mergers.

John Kwoka points out that for a variety of reasons, the record of behavior remedies is unimpressive.³⁴⁵ They require firms to act in ways that are inconsistent with their profit maximizing mandate, and consequently, they can be difficult for regulators to enforce.³⁴⁶ Monitoring and enforcing behavioral remedies is another area where a digital competition agency would prove useful. The agency could specialize in dark patterns, cross-market data flows, and biopower, and advise antitrust regulators on crafting and enforcing behavioral remedies.

CONCLUSION

Biopower is an evolving form of concentrated power that enables corporations to influence the behavior of populations. The digital panopticon, consisting of networks of sensing and control, is a Digital Age equivalent of Bentham's panoptic prison. It is the ultimate tool for concentrating biopower and achieving biosupremacy, monopolistic power over human behavior.

Leading technology companies execute conglomerate and concentric mergers with firms that produce internet-enabled software and devices in new markets. Though these unregulated acquisitions, they gain sensors that expand their surveillance networks, tapping new data streams that flow toward them across market boundaries.

³⁴⁴ See *id.*

³⁴⁵ See *id.* at 94.

³⁴⁶ See *id.*

Simultaneously, acquiring new software and devices in untapped markets expands their control networks and establishes beachheads from which companies influence behavior to shift prevailing social norms. By deploying dark patterns and other coercive design features, tech companies leverage intelligence gained from the sensing net to nudge users to act against their interests and surrender data they would otherwise not reveal. These actions raise costs to consumers, harm competition, reduce product quality, and impede innovation. Above all, they promote biosupremacy, monopolistic power over human behavior, which threatens democracy and human autonomy. Regardless of one's theoretical orientation, biosupremacy and concentrated biopower should be curtailed. Moreover, as the legal discipline tasked with constraining private power, antitrust should be adapted for this purpose.

To prevent tech platforms from achieving biosupremacy, antitrust regulators should incorporate the concept of biopower into merger control. They should block mergers that overconcentrate sensing and motor units, which serve as proxies for concentrated biopower, and use behavioral remedies to prevent merged firms from deploying dark patterns. These approaches will require the development of methods for quantifying biopower and coercive choice architecture, and Congress should create a digital competition agency to aid these efforts.
