Conversations and Controversies

Organization Theory
Volume 3: 1–79

DOI: 10.1177/26317877221129290
journals.sagepub.com/home/ott
SAGE

Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization

Shoshana Zuboff

Abstract

Surveillance capitalism is what happened when US democracy stood down. Two decades later, it fails any reasonable test of responsible global stewardship of digital information and communications. The abdication of the world's information spaces to surveillance capitalism has become the meta-crisis of every republic because it obstructs solutions to all other crises. The surveillance capitalist giants–Google, Apple, Facebook, Amazon, Microsoft, and their ecosystems–now constitute a sweeping political-economic institutional order that exerts oligopolistic control over most digital information and communication spaces, systems, and processes.

The commodification of human behavior operationalized in the secret massive-scale extraction of human-generated data is the foundation of surveillance capitalism's two-decade arc of institutional development. However, when revenue derives from commodification of the human, the classic economic equation is scrambled. Imperative economic operations entail accretions of governance functions and impose substantial social harms. Concentration of economic power produces collateral concentrations of governance and social powers. Oligopoly in the economic realm shades into oligarchy in the societal realm. Society's ability to respond to these developments is thwarted by category errors. Governance incursions and social harms such as control over AI or rampant disinformation are too frequently seen as distinct crises and siloed, each with its own specialists and prescriptions, rather than understood as organic effects of causal economic operations.

Harvard Business School, Boston, MA, USA

Corresponding author:
Shoshana Zuboff, Harvard Business School, Soldiers Field, Boston, MA 02163, USA
Email: info@shoshanazuboff.com

In contrast, this paper explores surveillance capitalism as a unified field of institutional development. Its four already visible stages of development are examined through a two-decade lens on expanding economic operations and their societal effects, including extraction and the wholesale destruction of privacy, the consequences of blindness-by-design in human-to-human communications, the rise of AI dominance and epistemic inequality, novel achievements in remote behavioral actuation such as the Trump 2016 campaign, and Apple-Google's leverage of digital infrastructure control to subjugate democratic governments desperate to fight a pandemic. Structurally, each stage creates the conditions and constructs the scaffolding for the next, and each builds on what went before. Substantively, each stage is characterized by three vectors of accomplishment: novel economic operations, governance carve-outs, and fresh social harms. These three dimensions weave together across time in a unified architecture of institutional development. Later-stage harms are revealed as effects of the foundational-stage economic operations required for commodification of the human.

Surveillance capitalism's development is understood in the context of a larger contest with the democratic order—the only competing institutional order that poses an existential threat. The democratic order retains the legitimate authority to contradict, interrupt, and abolish surveillance capitalism's foundational operations. Its unique advantages include the ability to inspire action and the necessary power to make, impose, and enforce the rule of law. While the liberal democracies have begun to engage with the challenges of regulating today's privately owned information spaces, I argue that regulation of institutionalized processes that are innately catastrophic for democratic societies cannot produce desired outcomes. The unified field perspective suggests that effective democratic contradiction aimed at eliminating later-stage harms, such as "disinformation," depends upon the abolition and reinvention of the early-stage economic operations that operationalize the commodification of the human, the source from which such harms originate.

The clash of institutional orders is a death match over the politics of knowledge in the digital century. Surveillance capitalism's antidemocratic economic imperatives produce a zero-sum dynamic in which the deepening order of surveillance capitalism propagates democratic disorder and deinstitutionalization. Without new public institutions, charters of rights, and legal frameworks purpose-built for a democratic digital century, citizens march naked, easy prey for all who steal and hunt with human data. Only one of these contesting orders will emerge with the authority and power to rule, while the other will drift into deinstitutionalization, its functions absorbed by the victor. Will these contradictions ultimately defeat surveillance capitalism, or will democracy suffer the greater injury? It is possible to have surveillance capitalism, and it is possible to have a democracy. It is not possible to have both.

Keywords
democracy, digital economy, digitalization, disinformation, information, institutional theory, internet governance, privacy, social media, surveillance capitalism

Our Accidental Dystopia: Surveillance Capitalism as Institutional Order

In an information civilization individual and collective existence is rendered as and mediated by information. But what may be known? Who knows? Who decides who knows? Who decides who decides who knows? These are the four questions that describe the politics of knowledge in the digital age. What knowledge is produced? How is that knowledge distributed? What authority governs that distribution? What power sustains that authority? The contests over the answers to these questions will shape "the division of learning in society" as the fundamental construct of social order in an information civilization. Right now, however, it is the surveillance capitalist giants–Google/Alphabet, Facebook/Meta, Apple, Microsoft, Amazon–that control the answers to each of these questions, though they were never elected to govern.

This condition reflects a larger pattern. From the dawn of the public internet and the world wide web in the mid-1990s, the liberal democracies failed to construct a coherent political vision of a digital century that advances democratic values, principles, and government. This failure left a void where democracy should be, a void that was quickly filled and tenaciously defended by surveillance capitalism. A handful of companies evolved from tiny startups into trillion-dollar vertically integrated global surveillance empires thriving on an economic construct so novel and improbable, as to have escaped critical analysis for many years: *the commodification of human behavior*. These corporations and their ecosystems now constitute a sweeping political-economic institutional order that migrates across sectors and economies. The institutional order of surveillance capitalism is an information oligopoly upon which democratic and illiberal governments alike depend for population-scale extraction of human-generated data, computation and prediction (Cate & Dempsey, 2017).

The consequences of this democratic failure are amplified in the global context. Since at least 2010, the Chinese state evolved a highly intentional theory and practice of digital design and deployment that advances its domestic systems of authoritarian rule and exports them to dozens of countries in nearly every region (Hoffman, 2022; Menendez, 2020; Mozur et al., 2019; Murgia & Gross, 2020; Sherman & Morgus, 2018). In contrast, the United States and other Western democracies have been compromised and ambivalent, torn between the digital seductions of surveillance-enabled social control and the rights-based principles of liberal democracy.

The political failure of the void forfeited the critical first decades of the digital century to surveillance capitalism. It deprived an increasingly connected world community of a clear alternative to the Chinese vision of the digital century. Without a path to a democratic *and* digital future, the democracies abandoned whole societies to new forms of digitally mediated violence from both state and market actors. Most treacherous is the potential *fusion* of these spheres in a digital-century incarnation of the surveillance state defined by unprecedented asymmetries of knowledge about people and the instrumentarian powers of behavioral control that accrue to such knowledge (Zuboff, 2019). Without new public institutions, charters of rights, and legal frameworks purpose-built for a democratic digital century, citizens march naked, easy prey for all who steal and hunt with human data. In result, both the liberal democracies and all societies engaged in the struggle to build, defend and strengthen democratic rights and institutions now stumble toward a future that their citizens did not and would not choose: an *accidental dystopia* owned and operated by private surveillance capital but underwritten by democratic acquiescence, cynicism, collusion, and dependency.

As an economic power, surveillance capitalism exerts oligopolistic force over virtually all digital information and communication spaces (Manns, 2020). But for those who would

approach analysis strictly through the lens of concentrated economic power and its remedies in economic regulation and antitrust law, there is more to consider. When the economic operations that drive revenue are founded on *the commodification of the human*, the classic economic playing field is scrambled. Concentration of economic power produces collateral concentrations of governance and social powers. Surveillance capitalism's institutional development braids these three vectors of power into a hydra-headed force that leads with economic operations and then competes with democracy for governance and social control. Oligopoly in the economic realm shades into oligarchy in the societal realm.

Characteristics of the giants' market power reflect the distinction between, on the one hand, their varied individual business models and, on the other, their shared participation in, and benefits from, the overarching economic logic of surveillance capitalism and its related strategies of institutional reproduction. These institutional elements spread through the giants' ecosystems and a growing majority of market enterprises across the commercial universe (Power, 2022). While this institutional order functions as an oligopolistic force, a reality already reflected in the term "Big Tech," individual firms may nevertheless exert monopoly or duopoly power within the narrower competitive spheres of their specific business models—for example, mass retail, mobile services, and online targeted advertising. In result, surveillance capitalism now intermediates nearly all human engagement with digital architectures, information flows, products, and services, and nearly all roads to economic, political, and social participation lead through its institutional terrain.

These conditions of practical and psychological "no exit" conjure the aura of inevitability that is both a key pillar of surveillance capitalism's rhetorical structure and critical to all institutional reproduction (Zuboff, 2019, pp. 221–224). Jepperson (2021) observes that institutionalization is the opposite of action. An institutional order is judged as robustly institutionalized when its durability and elaboration do not depend upon "recurrent collective mobilization," but rather are sustained by self-reproducing internal routines (p. 39). "Institutions," Berger and Luckmann (1966) write, "control human conduct by setting up predefined patterns of conduct ... primary social control is given in the existence of an institution as such." They note that external forms of human action are only required when "the processes of institutionalization are less than completely successful" (p. 55).

These formative processes do not, however, imply a one-way ticket or a solitary journey. Institutional orders form and develop, but they may also "deinstitutionalize" or even "reinstitutionalize" in a new form (Jepperson & Meyer, 2021). Such radical shifts in trajectory are triggered by contradiction that overtly challenges or implicitly undermines the aura of inevitability. For example, external shocks can unravel inevitability and erode institutionalization. Shifts can be initiated by collective action, the intensification of contradictions with competing institutional orders, or by an accumulation of internal contradictions that generate conflict among institutional elements. In each case of fundamental change, the force of contradiction is substantial enough to threaten self-acting reproductive mechanisms. Under these circumstances, the institutional order is forced to resort to active measures to protect and defend territory once considered inevitable, inviolable and invincible. *Action signals threat*, and because action is weaker than institutionalization, the destiny of such contests is uncertain. A return to the developmental path? Deinstitutionalization and destruction? Eventual reinstitutionalization? Each is possible.

These dynamics of contradiction require situating surveillance capitalism's institutional development within a larger contest among institutional orders. Specifically, surveillance capitalism's two-decade developmental trajectory can only be understood in relation to the institutional order that gave it birth and nourished it to adulthood: the liberal democratic state.

This paper examines the ways in which the institutionalization of surveillance capitalism has produced the deinstitutionalization of the democratic order through the erosion of informational, societal, behavioral and governance capabilities essential to democracy's sustenance and reproduction. Seen from this vantage point, surveillance capitalism's developmental thrust is revealed as an epistemic counterrevolution, an antidemocratic coup that aims for knowledge dominance and strikes at the essence of democratic viability.

Surveillance capitalism is the young challenger, its pockets full of magic. Born at the turn of a digital century that it helped to create, its rapid growth is an American story that embodies many novel means of institutional reproduction. Chief among these has been its ability to keep law at bay. The absence of public law to obstruct its development is the keystone of its existence and essential to its continued success. It is, therefore, dedicated to nourishing and rewarding the continued failures of democratic leadership (Zuboff, 2019, pp. 37–82; Chander, 2014).

Despite this history, the liberal democracies do pose an existential threat to the surveillance capitalist regime because they alone retain the requisite institutional force and capabilities to contradict, interrupt, and abolish its foundational operations. Indeed, as surveillance capitalism grows, contradictions with its grizzled but still potent antagonist have intensified. Democracy is the old, slow and messy incumbent, but those very qualities bring advantages that are difficult to rival. Foremost among these are the ability to inspire action and the legitimate authority and necessary power to make, impose, and enforce the rule of law. It now falls to the democratic order to reclaim the void for the sake of every society and people desperately trying to outrun dystopia.

In summary, the clash of institutional orders is a death match over the politics of knowledge in our information civilization, and the prize is the governance of governance. Surveillance capitalism's intrinsically antidemocratic economic imperatives produce a zero-sum dynamic in which the deepening order of surveillance capitalism propagates democratic disorder and deinstitutionalization. Only one of these contesting orders will emerge with the authority and power to rule, while the other will drift into deinstitutionalization, its functions absorbed by the victor. Will these contradictions ultimately defeat surveillance capitalism, or will democracy suffer the greater injury? At stake is the social order of our information civilization: the many or the few? Epistemic equality or subjugation? It is possible to have surveillance capitalism, and it is possible to have democracy. It is not possible to sustain both.

The sections that follow aim to reframe the requirements for successful democratic contradiction and thus to fortify the efforts of all who seek to avert the drift into accidental dystopia. To this end, I examine surveillance capitalism as a unified field of institutional development. The developmental stages of this two-decades-old institution reveal cause-and-effect relationships between earlier novel economic operations and later dystopian harms to democratic governance and society. This unified field perspective suggests that effective strategies for the elimination of downstream dystopian harms, such as "disinformation" or the illicit modification of collective behavior exemplified in extreme "polarization," depend upon interrupting, abolishing and reinventing the upstream economic operations in which such harms originate.

To preview the organization of this paper: the following section discusses surveillance capitalism's institutional development from the unified field perspective. The succeeding sections each discuss one of the four already visible stages of surveillance capitalism's development, each one marked by deeper and more comprehensive conflict with the democratic order. The concluding section anticipates the next phase of this work. Please see the Section Overview, below.

SURVEILLANCE CAPITALISM or DEMOCRACY?

Section Overview

Our Accidental Dystopia: Surveillance Capitalism as Institutional Order

The Unified Field Perspective

Figure 1: Four Stages of the Surveillance Capitalist Institutional Order

Foundational Stage One: The Commodification of Human Behavior (Economies of Scale)

The Economic Operations
Supply of Human-Generated Data
Demand for Human-Generated Data
The Governance Vector: The Annexation of Epistemic Rights
The Social Harm Vector (1): The Destruction of Privacy
The Social Harm Vector (2): The Rise of Epistemic Chaos

Stage Two: The Concentration of Computational Knowledge Production and Consumption (Economies of Learning)

The Economic Operations
The Governance Vector: Epistemic Authority
The Social Harm Vector: Epistemic Inequality

Stage Three: Remote Behavioral Actuation (Economies of Action)

"The Tools"
The Economic Operations
The Governance Vector: The Governance of Collective and Individual Behavior
The Social Harm Vector: The Artificial Construction of Reality

Stage Four: Systemic Dominance (Economies of Domination)

The Economic Operations
Revenge of the Void
Showdown
Apple-Google Contribute to US Failures
The Governance Vector: The Governance of Governance
The Social Harm Vector: The Desocialization of Society

Conclusion: The Golden Sword

The Unified Field Perspective

The public and its lawmakers are whipsawed by each day's headlines bleating surveillance capitalism's latest atrocities.[1] Comprehension of this hourly parade is thwarted by category errors: social harms are siloed and treated as disparate crises. For example, the collapse of privacy or the rise of disinformation are regarded as discrete phenomena, each with its own etiology, specialists, and prescriptions.

The unified field perspective offers a solution for this fractured tower of Babel by demonstrating the organic and temporal interdependencies across hierarchically integrated stages of institutional development. Discrete harms are revealed as the products of path dependencies, with causes and effects linked across time and developmental complexity in an overarching process of growth and institutionalization.

The four stages of surveillance capitalism's institutional development are each identified by their novel economic operations. These are: (1) The Commodification of Human Behavior; (2) The Concentration of Computational Knowledge Production and Consumption; (3) Remote Behavioral Actuation; and (4) Systemic Dominance. An adequate understanding of each stage, however, only begins with its economic action.

Over a century ago a young Durkheim (1964) bent to the task of explaining "the division of labor in society" as the basis of social order in an emerging industrial age. He cautioned his readers, "The division of labor appears to us otherwise than it does to economists" (p. 275). So too, the developmental stages of the surveillance capitalist institutional order appear to us otherwise than they do to economists. In addition to economic accomplishments, each stage pushes further into the void produced by the democracies' early failure to claim dominion over digital information and communication spaces. In this process two collateral vectors of dystopian consequences are set into motion by and inextricably linked to each stage's novel economic operations. I refer to these as "the governance vector" and "the social harms vector."

The governance vector is constituted by an accumulation of governance prerogatives enabled by newly consolidated economic operations. While it has been understood that Big Tech aims to govern (Balkin, 2017; Goodman & Powles, 2019; Klonick, 2020; Pasquale, 2017b), the unified field of institutional development clarifies the governance vector as a core reproductive mechanism of continuously expanding scope. It demonstrates the expansion and hierarchical integration of specific governance elements over time, their tight coupling with economic operations, and the ways in which earlier achievements coalesce to create the conditions for later-stage governance conquests.

From the perspective of the confrontation of institutional orders, each governance function is sucked into the surveillance capitalist orbit, leading to a simultaneous hollowing-out of the democratic order. Some governance carve-outs are difficult to decipher because the governance functions themselves are not yet formally codified, as we shall see below in the case of epistemic rights. Others are explicit challenges to the rule of public law. Most concerning is the extent to which the democratic order assists in or fails to challenge these attacks.

Apple CEO Tim Cook provides an insight into the essential developmental thrust that unifies each stage of governance victories when he describes Apple's determination to disrupt the healthcare industry. His statement captures the direction, movement, and purpose of the governance vector more generally. "*We are taking what has been with the institution*," Cook says, "*and empowering the individual*" (Feiner, 2019, para. 72).

In a similarly rare display of candor, Uber founder Travis Kalanick once described to a group of MIT students the great "taking" that produced Uber's success. He called it "regulatory disruption" and quickly added, "We don't talk about that a lot in tech" (MIT Sloan School of Management, 2013, para. 6; see also, Fleischer, 2010; Riles, 2014; Terry, 2016, 2017)

Both CEOs celebrate the work of carving out governance functions from an institutional zone of public law and their transfer to friction-free

market spaces where they are resurrected shorn of legal constraints and indentured to a private institutional logic. When Cook describes "empowering" the individual, he declares Apple's prerogative to supplant existing institutions and laws. Apple Inc. asserts itself as the source of authority that "empowers" and therefore its equivalent authority to disempower individuals just as quickly with a flick of its terms of service or operating system.

The CEOs' statements are classic renderings of corporate strategies known as "disruption," fragrant with libertarian themes of the sovereign individual unjustly subjugated to society and its outdated institutions. Cook's script weaves the illusion of Apple as a 21st-century Robin Hood, emancipating valuable assets held hostage by powerful institutions and redistributing them to unjustly diminished individuals. Cook's false flag of liberation alienates the individual from society to obscure the inconvenient-to-Apple truth that only democratic society can authorize and protect the rights and laws that sustainably empower and protect individuals.

Democracy has no intrinsic value or inviolable status in the disruption equation. The market mythology of godlike omniscience that naturally optimizes for superior economic outcomes is exploited to justify its elevation over democratic institutions and laws. The point is illustrated by Clay Christensen, originator of disruption theory, and his co-authors in a 2012 essay on the great "taking" from the news industry sadistically entitled "Breaking News." The piece quickly cites and dismisses journalism's mission-critical role in the sustenance of democracy: "Journalism institutions play a vital role in the democratic process and we are rooting for their survival. But only the organizations themselves can make the changes required to adapt ..." This *laissez-faire* agnosticism and *sang froid* intellectual remoteness prefigures Tim Cook's ambitions. Christensen et al. dismiss the democratic project with an Emperor's casual thumbs-down after a poorly matched gladiatorial contest. The Fourth Estate, conceived as an essential pillar of democracy and the means of holding power to account, is brushed aside, "a function of life in the old world." Incumbents lose because they foolishly "stay the course" on the "quality" of content. Winners are the "low end," "low-cost," "personalized" new entrants (Christensen et al., 2012, paras. 14, 15).

From the vantage point of this ideological fortress—Cook's fortress—it was impossible to admit, or perhaps even to perceive, that "low end" and "low cost" were not the conditions to produce news but rather to produce fake news. Or that the "old world" stood for codified principles of information integrity, truth telling, and factualization that a decade later would not be regarded as fusty nostalgia, but rather be as oases of rationality in a corrupted information hellscape. Beginning in the United States, and in spite of the stakes, the democracies stood down, bystanders to the birth of their own diminished futures.

Thanks to the disruption reduction, the news industry was quickly forced to join the surveillance capitalist order and contribute to its reproductive routines. By 2017, Princeton researchers found that news websites contained more embedded tracking codes than those of any other industry in the study, as publishers chased revenues in the new targeted ad markets established by Google and Facebook. The disciplines of surveillance capitalism's economic imperatives shaped both print and television news with pages and newscasts specifically designed to optimize social media engagement for the purpose of maximum human data extraction (Narayanan & Reisman, 2017; NewsWhip, 2019; Stroud et al., 2014).

This defeat bites hard in Pew Research's detailed 2020 survey of 979 tech business leaders, policy specialists, developers, innovators,

researchers, and activists. About half of those surveyed predicted that "humans' use of technology will weaken democracy ... due to the speed and scope of reality distortion, the decline of journalism and the impact of surveillance capitalism" (J. Anderson & Rainie, 2020).

The point here is that Christensen and Cook's disruption strategy was never intended to develop institutions, but rather to eliminate them. They envisioned new privately mediated relationships with "individuals" that first bypass institutions, then eliminate the functions that institutions were designed to protect, and ultimately render institutions irrelevant. Because institutions are the gatekeepers that develop, contain, impose, and enforce qualifying standards of conduct and content in their respective domains, their diminishment or elimination paves the way for fakes: fake news, famously, but also fake healthcare, fake education, fake cities, fake contracts, fake public squares, fake governance, and so on.

They "don't talk about that a lot in tech" because the companies prefer to camouflage their governance moves behind the Robin Hood illusion, when in fact their carve-outs prepare the ground for the opposite: the eventual substitution of private computational governance for democratic governance. This shift emerges in stage four's expressions of systemic dominance when the democratic order itself becomes the target for disruption.

A second vector produced at each stage is constituted by the production of new social harms, calculated as the cost of institutional reproduction and treated as externalities. The two vectors are complementary. Governance carve-outs facilitate institutional reproduction by bulking up surveillance capitalism, amplifying its authority and power at the expense of the democratic order. Social harms facilitate reproduction through direct attacks that disorient, distract and fragment the democratic order. Weaknesses produced by each governance carve-out create the conditions and opportunities for attack by successive social harms that further diminish society's ability to repel governance carve-outs.

Each stage's causes and effects create the conditions and construct the scaffolding for the next. Each stage builds on and extends what went before. Each is carried by the momentum of earlier means of institutional self-reproduction, and each produces novel means that sustain, extend, and elaborate the new institutional order. As is typically the case in stage-based theories of development, the stages are ideal-typical abstractions that disclose the inner logic of an institutional order in perpetual motion, compelled to survive, grow, and evolve. The stages constitute a unified field of hierarchically integrated and path-dependent causes and effects. Seemingly disparate phenomena are thus revealed as later-stage consequences of earlier-stage operations and their reproductive mechanisms. All three dimensions–economic, governance, and social–move together across time in a single comprehensive architecture of institutional growth and intensification (see Figure 1).

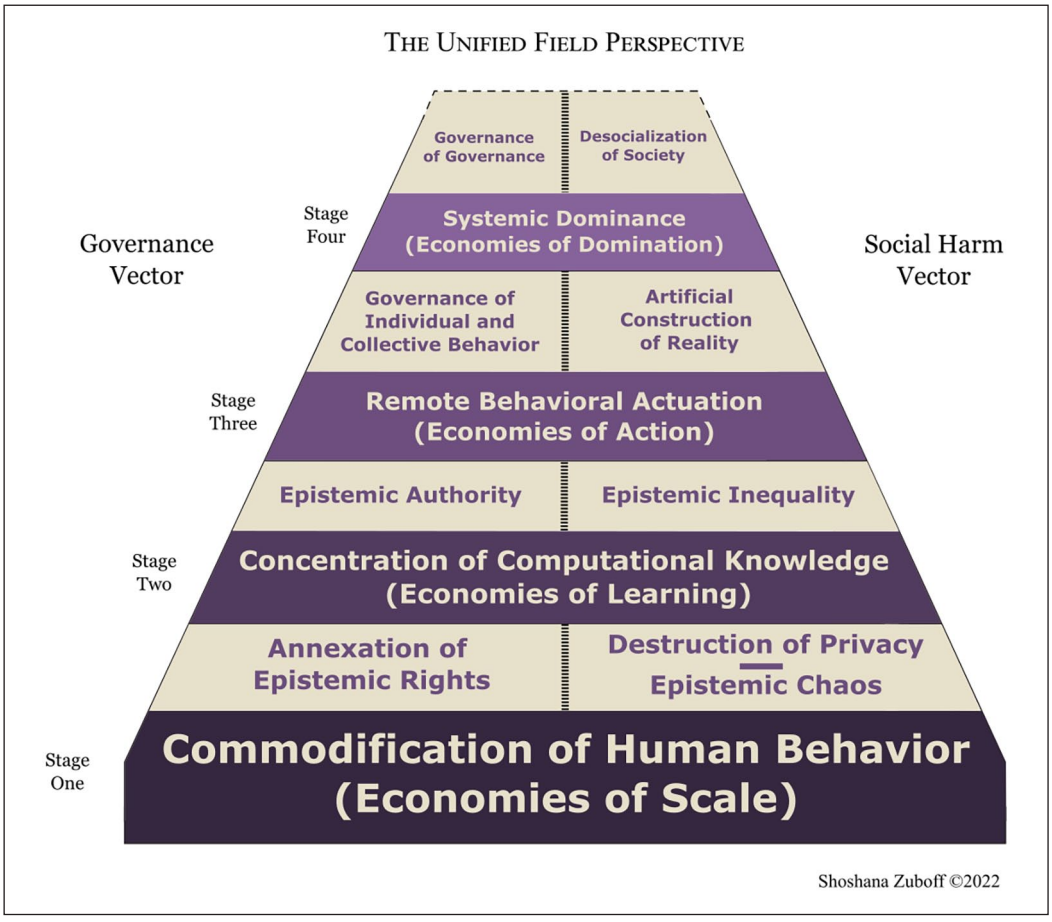

Figure 1. Four Stages of the Surveillance Capitalist Institutional Order.

The lesson for effective strategies of democratic contradiction is that later-stage social carnage can only be addressed effectively through direct confrontation with earlier stage economic operations. Durable solutions must be directed toward the foundations from which all harms originate.

Finally, the stage descriptions that follow sometimes rely on case evidence from the lead corporations to illustrate the interdependencies of economics, governance and social harms within and across stages. Key to a stage-based analysis is that the dynamics examined here accrue not only to the corporate protagonists featured in these cases, but to the larger institutional order in which they participate. My focus is on the development of the institution, as it accrues data, knowledge, authority, power and ambition. Each of the corporate giants, and for that matter the legions of firms across the commercial landscape already enmeshed in the surveillance capitalist order, presents a unique configuration of each stage's achievements. Some are more advanced than others. Some have more specialized roles and capabilities within the larger spectrum. Each of them contributes to and is nourished by institutional advance.

Foundational Stage One: The Commodification of Human Behavior (Economies of Scale)

The Economic Operations

The first stage introduces the commodification of human behavior operationalized in the secret massive-scale extraction of human-generated data. This formative achievement is enshrined in the Google breakthrough that laid the foundation for all that follows.

In the year 2000, when only 25% of the world's information was stored digitally (Hilbert & López, 2011), a tiny but brilliant Silicon Valley internet startup called Google faced an existential threat during the financial crisis known as the dotcom bust. Founders Larry Page and Sergey Brin had not yet discovered a way to turn their search engine miracle into money. Between 2000 and 2001, as the company's investors threatened defection, the Google team stumbled into a series of discoveries that offered a rescue plan (Zuboff, 2019, pp. 63–97). Data scientists learned to identify behavioral signals embedded in the "data exhaust" left over from users' search and browse activities. These discarded behavioral traces (Power, 2022) were a surplus—more than what was required for product improvement. The signals embedded in this behavioral surplus, they discovered, could be aggregated and analyzed to predict user behavior. The team soon broke through by learning how to predict a "click-through rate," the solid gold computation that saved the little company from financial ruin. It launched the online targeted ad industry, best understood as *surveillance advertising*—the Trojan horse that conceals the complex machinery of secret massive-scale extraction of human-generated data.

Google founder Larry Page laid out the essence of Google's business in 2001 as search and seizure. "If we did have a category," he ruminated, "it would be personal information ... Everything you've ever heard or seen or experienced will become searchable. Your whole life will be searchable" (Edwards, 2011, p. 291). Google's business plan had called for selling search engine licenses to corporate clients. Instead, the young company found a fast track to salvation by repurposing its search engine as a sophisticated surveillance medium, a loss leader for massive-scale extraction of "your whole life." People thought they were searching Google, but Google was searching and seizing them.

The term of art was "user engagement," a coded expression for a new subject-object social relation in which commodity resources targeted for extraction just happen to be sentient human beings. Google's inventions depended on the secret invasion of once-private human experience to implement a hidden taking without asking. Such action is normally characterized as theft, and it was on the strength of this original sin of secret theft that users' private lives were declared as corporate property. Some of Google's earliest patents chronicle the company's frank pursuit of behavioral surplus across the internet, including methods that aimed to exploit and construct user profile information (UPI) with methods that knowingly bypassed users' agency, awareness, and intentions. For example, a 2003 application explains that UPI "may be inferred," "presumed," and "deduced," even when users did not knowingly provide such information or when they intentionally left information incomplete "because of privacy considerations, etc." It notes, "UPI for a user ... can be determined (or updated or extended) even when no explicit information is given to the system ... An initial UPI may include some expressly entered UPI information, though it doesn't need to" (Bharat et al., 2016, sec. 4.2.3).

The invention and its antidemocratic social relations were twin born. Page feared the consequences if users, lawmakers or competitors were to grasp the true nature of its operations. Anything that might "stir the privacy pot and endanger our ability to gather data" was scrupulously avoided (Edwards, 2011, pp. 240–245).

A single law that pulled back the curtain and redefined Google as a thief would end the prospect of financial salvation.

This corporate "hiding strategy," as it was called (S. Levy, 2011, p. 69), also served to conceal the astonishing financial implications of Google's new capabilities. Between 2001, when surveillance economics were first applied, and 2004, when Google went public, its revenues increased by 3,590% (Google Inc., 2004, p. 19). This *surveillance dividend* established the secret massive-scale extraction of human-generated data as the illegitimate, illicit and perfectly legal foundation of a new economic order. Every investor would want it. Every startup would endeavor to supply it ... and there was no law to stop it.

In 2008, after a series of costly blunders that incited user rebellion, Facebook founder Mark Zuckerberg turned to Google for answers, hiring Sheryl Sandberg, Google's head of global online advertising, as his second in command (Hempel, 2008). With Sandberg in charge of operations, Facebook quickly learned to extract behavioral surplus from every behavioral trace, irrespective of what people voluntarily shared. She recognized that Facebook had a front row seat on what Page had called "your whole life," as unsuspecting users poured their lives onto Facebook pages. The result was a company with, as Sandberg observed, "better information than anyone else" and more "real data", not "the stuff other people infer" (Kirkpatrick, 2011, p. 266).

A year from Sandberg's arrival, the new executive duo changed Facebook's privacy policy to pave the way for surveillance economics. *TechCrunch* summarized the corporation's strategy: "If there is significant backlash against the social network, it can claim that users willingly made the choice to share their information with everyone" (Kincaid, 2009, para. 6). Mr Zuckerberg's hard-won appreciation of surveillance economics steeled him to the realpolitik of a new economic order: "[W]e decided," he explained, "that these would be the social norms now, and we just went for it" (B. Johnson, 2010, para. 15; see generally Srinivasan, 2019).

The novel economic foundations of surveillance capitalism begin with its original sin. Human experience is claimed as free raw material for market action, beginning with its secret extraction and translation into behavioral data. These data are the gateway to new realms of highly predictive inferential constructions: emotions, personality, political and sexual orientation, and more. Surplus data are immediately redefined as corporate assets, private property available for the proprietary computation of individual and collective profiles and predictions.

Surveillance capitalists compete on the power of their predictions to reduce uncertainty. This most fundamental commercial objective dictates the requirement for *massive-scale* commodity extraction, production, and refinement of human-generated data, comparable to tons of wheat or barrels of oil. Prediction products are sold to business customers in a new kind of commodity market that trades in human futures. The point is illustrated in a 2016 Facebook document describing its "AI Backbone", known as FBLearner Flow. Thanks to the absence of democratic contradiction, Facebook's AI "ingests trillions of data points every day" to produce thousands of models. These computations are fed to its "prediction service" that churns out "more than 6 million predictions per second" (Dunn, 2016). These are the building blocks of prediction products sold to companies, advertisers political campaigns, and other buyers with an interest in knowing, reinforcing, or inhibiting the predicted behavior of individuals and groups (Biddle, 2018b).

The "click-through rate" was only the first globally successful prediction product, and online targeted advertising was the first thriving market in human futures. Surveillance capitalism was thus "declared" into being and the only witnesses to its birth were sworn to secrecy (Searle, 2010, pp. 85–86, 13).

The secret accumulation of behavioral surplus in scale and scope belies the notion of an "attention economy," because the defining work here is accomplished outside the attentional field. Indeed, the notion has skewed public perception in a dangerous way by promoting the false belief that one can control exposure to extraction operations by controlling one's attention. The facts are different. Withholding

one's attention is no barrier to or protection from the secret extraction of signals produced and captured beyond the range of human awareness or control. One may take refuge in the fiction of choice (Kim, 2013; Radin, 2012) with respect to a discrete decision to share specific information with a corporation, but that information is insignificant compared to the volume of behavioral surplus that is secretly captured, aggregated, and inferred. The principle of concealment operationalized in secret surveillance is thus essential to this foundational stage of economic operations and becomes a critical mechanism of institutional reproduction (Binns, 2022, p. 21).

In the second decade, the initial successes of surveillance capitalist pioneers, such as Google and Facebook, drew surveillance economics into the "normal" economy, now symbolized in Walmart's competition with Amazon for human-generated data collection, computation, prediction and targeting (Tobin, 2022). Surveillance capitalism metastasized across diverse sectors from insurance, retail and finance, to agriculture and transportation, to the most intimate and predictive data residing in the two critical sectors of education and healthcare.

Every product called "smart" and every service called "personalized" are now loss leaders for the human data that flow through them. Most "apps" begin their lives for sale and distribution through Apple's and Google's app stores. Once downloaded, and no matter how apparently benign, they function as data mules shuttling behavioral signals from "smart" devices to servers primarily owned by the tech giants and the ad tech data aggregators. As one Silicon Valley data scientist described it to me, "The underlying norm of virtually all software and apps design now is data collection. All software design assumes that all data should be collected, and most of this occurs without the user's knowledge" (DS I, see Note on Method).

The concept of "all data" is ever-expanding. Location tracking is now institutionalized: global, ubiquitous and inescapable (Zekavat et al., 2021). An industry analysis forthrightly notes that location tracking "enables businesses to identify customer behavior ... and mitigate the uncertainties in the market" (Grand View Research, 2022). The notion of "all data" consistently evolves toward the more exquisitely predictive, such as decoding speech from brain waves or using eye gaze behavior to infer sensitive information including personality, emotions, and sexual preference (Kröger et al., 2020; Moses et al., 2019). Indeed, it is already understood that augmented reality, or the "metaverse," for all its futuristic verbiage, is intended as an intensification of stage one foundational extraction mechanisms (H. Murphy, 2022; Heller, 2021; Martin, 2021).

Research from the Irish Council for Civil Liberties (ICCL) illustrates the current state of play (Ryan, 2022). The giants continuously aggregate once-private personal information to compute user locations, behavioral surplus, profiles, and predictions. These are broadcast to human futures markets for real-time bidding (RTB), where advertisers bid on the opportunity to place their ad on your screen. IAB, the nonprofit research consortium that supports RTB in the ad tech industry, lists nearly 400 data categories that refine user profiles, including "Coffee/Tea," "Road-Side Assistance," "Incontinence," "Panic/Anxiety Disorders," "Ethnic Specific," and "Personal Finance." The RTB categories also include "Incest/Abuse Support," "Women's Health," "Dating," "Marriage," "Travel," "Pregnancy," "Babies and Toddlers," and "Adoption," data all too easily trained on stalking potential abortion seekers in a polarized America, where many states have criminalized a woman's right to choose. (IAB Tech Lab, 2016, sec. 5.1).

Google is the largest RTB company, channeling targeting data to 4698 firms in the United States, or 10% of US broadcasts, and 1058 firms in Europe, accounting for 14% of European broadcasts. The ICCL findings suggest that current legal regimes mitigate but do not abolish these operations. The average person in the United States, where the federal government has yet to pass basic privacy protections, has their online activity and location data exposed 747

times each day. In Europe where data protection laws lead the world, it's 376 daily exposures. The data flow with no means to control their destinations or assess their fate.

The entire economic edifice of surveillance capitalism is built on this illegitimate but not illegal foundation. Nothing here was "technologically determined". Nothing was or is inevitable. That the democracies failed to mount the contradictory force capable of thwarting surveillance capitalism's development was the result of specific ideological and historical contingencies, beginning in the United States.

Supply of Human-Generated Data

Freedom from law justified by a radical and antidemocratic economic ideology guaranteed the limitless supply of human data.

Public access to the world wide web in the mid-1990s was a slow-gathering wave. Legal scholar Anupam Chander describes the US milieu of the 1990s, when all three branches of the government converged on a cobbled-together "industrial policy favoring Internet entrepreneurs" and their maximum freedom of operation unobstructed by law. Lawmakers in Europe and Asia typically sought to protect established principles of individual privacy, intermediary liability, and the sanctity of intellectual property laws as they oversaw the rise of the internet. In the United States, the Clinton administration, Congressional lawmakers and jurists rallied to the rhetoric of "innovation" by aggressively conflating freedom of internet commerce with "freedom of speech." "U.S. authorities (but not those in other technologically advanced states) acted with deliberation to encourage new Internet enterprises by both reducing the legal risks they faced and largely refraining from regulating the new risks they introduced," writes Chander (2014, p. 645). The upshot was the "stunning pattern" of a legal environment "specifically shaped to accommodate" the internet companies (Chander, 2014, pp. 644–645, 648–649; see also, Citron & Franks, 2020; Tribe, 2021; Pasquale, 2017a; Chander & Le, 2014; Rozenshtein, 2021).

This pattern reflects a period in which US lawmakers coalesced around a radical free market ideology forged in the aftermath of the Second World War as a response to the collectivist nightmares of German and Soviet totalitarianism and theorized by the neoliberal thought leader Friedrich Hayek (Burgin, 2012; Mirowski, 2013). The politics of knowledge defined the core of Hayek's thesis. It was the intrinsic "ineffability" of "the market," he argued, that necessitates maximum freedom of action for market actors, an idea that shaped the libertarian creed and its insistence on absolute individual freedom (Hayek, 2007, p. 234).

The epistemic challenge and its politics of knowledge dominated Hayek's thinking from his 1937 preoccupation with "the division of knowledge" as a central concern of economics,[2] to his 1988 description of the market as an unknowable "extended order" that supersedes the political authority of the state. "Modern economics," he wrote, "explains how such an extended order ... constitutes an information-gathering process ... that no central planning agency, let alone any individual, could know as a whole, possess, or control" (Hayek, 1988, pp. 14–15). The genius of markets, he argued, had to be protected from any countervailing institutional force or external authority. That such systems would produce substantial inequality of rights and wealth was accepted, and even welcomed, as a necessary feature of a successful market system, a goad to human betterment, and a force for progress (Hayek, 1945, pp. 88–89; Mirowski, 2013, pp. 53–67).

It was University of Chicago economist Milton Friedman who later surpassed Hayek in popular recognition and influence. In addition to his academic research, for which he received the Nobel Prize, Friedman simplified free market ideology for public consumption. From the 1960s to just a few years before his death in 2006, Friedman tirelessly asserted his bedrock theme in every speech, lecture, essay, and public appearance: radical market freedom is justified as the one source of truth and the origin of political freedom. On an infamous 1975 visit to Chile, he counseled the dictator Augusto

Pinochet and his generals that only radical free market economics would return the country to political freedom (Friedman et al., 2012). He told students at Brigham Young University, "The economic market is a more effective means for achieving political democracy than is a political market" (Friedman, 1976, 2017a, p. 116). He warned alumni at Pepperdine University, "If you don't have economic freedom, you don't have political freedom" (Friedman, 2017b, sec. 5).

Historian Angus Burgin observes that Friedman's insistence on the universal application of radical economic freedom made him an "unprecedented anomaly" even among the neoliberal economists of late 20th-century United States. Friedman described himself as a "radical," "kook" and "extremist" (Burgin, 2012, pp. 154–155, 183–184, 212–213, 176–177).

As the old collectivist enemies receded, many conservative economists moved toward greater recognition of the role that democratic governments play in sustaining market economies. Friedman instead doubled down on sharp dualisms, absolutes and unequivocal policy positions, naming fresh collectivist dangers to battle. As early as 1951 he worried that democratic "collectivism" would undermine "political democracy."

By the late 1970s, he argued, that time had come. He identified the new collectivist threats: state regulation and oversight, social legislation and welfare policies, labor unions and the institutions of collective bargaining, public education, and even foundational democratic principles such as equality, social justice and majority rule. Friedman saw the field of combat clearly: the market must dominate, democratic institutions must recede. Instead of democracy regulating the market, the market must regulate democracy.[3] In 1970, the professor declared in the *New York Times Magazine*, "There is one and only one social responsibility of business–to use its resources and engage in activities designed to increase its profits so long as it stays within the rules of the game" (Friedman, 1970, para. 33).

By the late 1970s and for decades to follow, politicians and policy makers were expected to internalize contempt for their own power as they learned how to design, play, and defend a game in which the only rule was the absence of rules. Democratic submission to market truth required democratic officials, leaders and lawmakers instructed in and converted to a new role in the political ordering of knowledge, one that yields to the unconscious but superhuman truth of the market over the conscious direction of democratic governance. Unimpeded competition and supply-side reforms, including comprehensive deregulation, privatization, lower taxes, and corporate self-regulation, were to be the new solutions to growth.

Friedman's political message "had the effect of a bombshell," Thomas Piketty (2014) observes, and "created the intellectual climate in which the conservative revolution of 1979–1980 became possible" (p. 549). By 1979, it was Friedman who advised presidential candidate Ronald Reagan; then Friedman who advised the White House during Reagan's eight-year tenure; Friedman who traveled the world declaiming the primacy of radical economic freedom to elites in every region; and Friedman who preached his dogma on American Public Television.

In 2002, four years before his death, Friedman reevaluated his lifelong view of economic freedom in favor of an even more antidemocratic formulation. In what would become a gross misreading of the future, Friedman explained, "Hong Kong ... persuaded me that while economic freedom is a necessary condition for civil and political freedom, political freedom, desirable though it may be, is not a necessary condition for economic and civil freedom." Democracy, he reasoned, is after all too risky, too much of a wild card. Political freedom should no longer be understood as an inviolate good but rather as an unpredictable condition that "under some circumstances promotes economic and civic freedom, and under others, inhibits economic and civic freedom." Economic freedom was to be the one absolute and the only necessity. Democracy, Friedman concluded, is

expendable (Ebenstein, 2012, pp. 105–106; Friedman, 2002).

Though Friedman's dogma was adopted most comprehensively in the United States and the UK, its consequences spread to every region of the global economy. And so it was that three days after Friedman's death in November 2006, Larry Summers, former Clinton Treasury Secretary and soon to be director of Obama's National Economic Council, authored a memorial essay in the *New York Times*. "[A]ny honest Democrat will admit that we are now all Friedmanites," he wrote, and not as lament. "Mr. Friedman ... never held elected office but he has had more influence on economic policy as it is practiced around the world today than any other modern figure." Summers (2006) observed that Friedman transformed the "previously unthinkable" into the acceptable and necessary. With Friedman, "heresies had become the orthodoxy." Friedman's greatest skill was to imbue his radical ideas with the aura of inevitability (paras. 2, 5, 7).

Friedman's libertarian conception of freedom converged with the libertarian culture of Silicon Valley and its second-generation entrepreneurial stirrings in the late 1970s (Flichy, 2007; Isaacson, 2014; Mosco, 2004; Markoff, 2005; Naughton, 1999; Turner, 2006; see also, Chafkin, 2021). With the release of the Mosaic browser in 1993, the world wide web was on its way to becoming a popular global medium of information production and consumption, communication, and commerce. These new connected spaces were quickly claimed for Friedman's radical freedom. Former Google CEO Eric Schmidt celebrated this triumph on the first page of his 2014 book on the digital age when he described "an online world that is not truly bound by terrestrial laws ... the world's largest ungoverned space" (Schmidt & Cohen, 2014, p. 3).

This historical nexus finds iconic expression in the 1997 Clinton-Gore white paper setting out the administration's policy vision for "Global Electronic Commerce" (Clinton & Gore, Jr., 1997). It begins with the document's bedrock principle: "The private sector should lead." The people, science, capital, software, chips, wires, cables, servers, and so forth that constitute the web and its new companies were mythologically fashioned as "cyberspace," an extra-societal zone in which the norms and laws of real-world democracies do not apply.

The white paper is a Manchurian candidate-like testament to the internalized disciplines of democratic submission. It denigrates to the point of caricature the US government's role in the governance of digital information and communication spaces, insisting on minimal government involvement or intervention. "Business models must evolve rapidly ... government attempts to regulate are likely to be outmoded by the time they are finally enacted ... Existing laws and regulations that may hinder electronic commerce should be reviewed and revised or eliminated to reflect the needs of the new electronic age" (Clinton & Gore, Jr., 1997, secs. 2, 4). The administration's approach was not only to get out of the way, but to proactively cede whole governance functions to the internet companies, including the most sensitive: "privacy, content ratings, and consumer protection." The absence of constraints on privacy-invasive operations was thus gifted by democracy, and it was this gift that enabled surveillance capitalism's explosive growth. Friedman's dogma would eventually guarantee the secret but legal massive-scale supply of human-generated data.

Fifty years after Friedman's declaration in the *New York Times*, presidential candidate Joe Biden offered his own declaration: "I think there's going to be a willingness to fix some of the institutional inequities that have existed for a long time. *Milton Friedman isn't running the show anymore*" (Grunwald, 2020; emphasis mine). In 2022, former Obama Administration Chair of the Federal Trade Commission, Jon Leibowitz, aired his frustration with US lawmakers in the *Wall Street Journal*. A decade earlier, Leibowitz and his FTC colleagues had submitted a report to the US Congress sounding the alarm that "industry self-regulation of privacy was not working for American consumers" and arguing for strict curbs on data collection. But in 2022, Leibowitz observed with dismay

that in the years since that report, "surveillance capitalism has only gotten worse," yet "legislation has languished" (Leibowitz, 2022).

The lesson is that there can be no end to Friedman's show unless and until there is an end to surveillance capitalism, the digital-century avatar of his extremist vision and information civilization's preeminent beneficiary of his legacy.

Leibowitz was not the first to sound the alarm. As early as 2000, a majority of FTC commissioners, including Chair Robert Pitofsky, concluded that self-regulatory initiatives "cannot ensure that the online marketplace as a whole will follow the standards adopted by industry leaders ... notwithstanding several years of industry and governmental effort" (Pitofsky et al., 2000, p. 35). They proposed a detailed framework for basic federal privacy protections that would have set the United States and the world on a different path to the digital century, but history and chance had other plans.

Demand for Human-Generated Data

With supply assured, the US response to the 9/11 terrorist attacks, known as "the war on terror," guaranteed continuous demand for human-generated data.

According to Peter Swire, chief counselor for privacy in the Clinton administration and later a member of President Obama's Review Group on Intelligence and Communication Technologies, "With the attacks of September 11, 2001, everything changed. The new focus was overwhelmingly on security rather than privacy." The legal provisions debated just months earlier vanished from the conversation more or less overnight, giving way to an obsession with "Total Information Awareness." A "state of exception" was invoked to unleash a new data imperative: velocity and volume at any cost. In this new environment, "Congress lost interest in regulating information usage in the private sector," Swire recounts. "Without the threat of legislation, the energy went out of many of the self-regulatory efforts that industry had created" (Swire, 2013, pp. 845, 846).

In the United States and across the European Union, legislation was quickly enacted to expand surveillance activities (I. Brown, 2012, p. 230; Pasquale, 2013; Prodhan & Nienaber, 2015; Rubin, 2015; Schwartz, 2012, pp. 289, 296; Scott, 2015; Voss, 2016). Instead of federal legislation to outlaw the novel surveillance practices, the new aim was to enrich the conditions for their expansion and application outside constitutional, legislative, and regulatory constraints. Yale's Jack Balkin explained that while the US Constitution inhibits surveillance by government actors, privacy protections for information held in private servers is "limited if not nonexistent." If the intelligence community was to indulge its obsession to ascertain the future, then it would have to "rely on private enterprise to collect and generate information for it" (Balkin, 2008, pp. 16–17, 19). The contours of a new interdependency between public and private agents of information dominance began to emerge, born of a mutual magnetism originating in complementary interests and reciprocities. The result was an unwritten doctrine of *surveillance exceptionalism* that guaranteed robust demand for secretly extracted human-generated data (Zuboff, 2019, pp. 112–121).

The license to steal would become the persistent elephant in the room, joining free market dogma to shape an environment in which the internet companies developed without legal impediments. But it also sentenced these companies to a future of political activism, collaboration, appeasement, lobbying, threat, confrontation, legal battle, and propaganda. These actions have been required to defend and fortify privileges precisely because they were never inevitable.

Because action is weaker than institutions, Big Tech was compelled to surpass all prior lobbying records, including Big Oil and Big Tobacco. Ninety-four percent of all members of Congress with jurisdiction over privacy and antitrust issues received Big Tech PAC or lobbyist contributions, amounting to US$3.2m in 2020 alone (Chung, 2021). "[T]he four biggest technology companies and their third-party groups spent $35.3 million during the first half

of 2022, a 15% increase over ... the first half of [2021]" (Diaz & Birnbaum, 2022).

In 2010, former NSA director Mike McConnell acknowledged collaboration between the internet companies and the intelligence community, noting, "the challenge is to shape an effective partnership with the private sector so information can move quickly back and forth from public to private" (McConnell, 2010, para. 15).

By 2013, that partnership was not only fully operational but normalized. Speaking at a public tech conference in March that year, CIA Chief Technology Officer Gus Hunt cheerfully described the central riddle of the CIA's urge toward total information. "We have to connect the dots ... Since you can't connect dots you don't have, it drives us into a mode of, we fundamentally try to collect everything and hang on to it forever." (Hunt, 2013, 19:14–20:11). Hunt exalted the tech companies as the means to this end.

The hallmark of the CIA's technology mission was to "protect national security," Hunt explained. It required the agency "to take advantage of the massive information streams that have emerged on the planet." Hunt acknowledged the CIA's gratitude toward Google ("a very big provider of things"), Facebook (where "35% of all the world's digital photography" was already posted), YouTube ("the only Exabyte scale or bigger repository ... on the planet"), Twitter (4500 tweets per second), and the telcos (global text messaging and mobile phone calls). In recognition of ubiquitous location tracking, Hunt instructed his audience, "You're already a walking sensor platform," and he concluded with a stunning admission: "I think we're at high noon in the information age ... It really is very nearly in our grasp to be able to compute on all human-generated information" (Hunt, 2013, 1:22–1:32, 5:55–5:57, 6:25–6:44, 7:05–7:21, 10:57–11:02, 26:05–26:17).

Despite the dramatic content of Hunt's presentation, his audience of IT professionals and journalists barely blinked, apparently more interested in food than the shocking specter of tech power and governmental collusion. Hunt began by apologizing for keeping the group from its midday meal, and when he ended his astonishing remarks 28 minutes and 47 seconds later in a lackluster drizzle of applause, the announcer waived off his offer to take questions. "I think we're getting ready for lunch, but people can find you, I'm sure, floating around" (Hunt, 2013, 28:00–28:05). The clutch of rumpled suits wandered off in search of sandwiches and drinks, leaving behind the one man in the room whose brain was on fire. His name was Edward Snowden (Hunt, 2013, 28:00–28:05; Snowden, 2019, pp. 247–248).

Bart Gellman broke the 2013 Snowden PRISM story in the *Washington Post*, chronicling the NSA's data collection from nine companies, including Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, and Apple. In his 2020 analysis Gellman concludes that the NSA "shared more information obtained from American internet companies than from any other source." PRISM, he writes, "had become a principal engine of the U.S. surveillance machine ... Never in history had there been richer troves of personal information" (Gellman, 2020, pp. 113, 117, 121).

The United States was not alone in its demand for the surveillance capitalists' extraconstitutional flows of human-generated data. Cate and Dempsey (2017) describe the expansive aggregation of personal data from private sector companies by 13 countries, including the democracies of France, Germany, Israel, Italy, Brazil, Canada, the United States, Australia, India, Japan, and South Korea. They conclude that every government in their study practiced "bulk collection"–mass data collection "without particularized suspicion"–all of it to collect the dots in the hope of one day connecting them. "Every government in the world claims the power to compel disclosure of this data by the companies that hold it," Cate and Dempsey observe. They ask if such capabilities can ever be consistent with human rights principles of necessity and proportion (p. xxvi; see also, I. Brown, 2012; Pasquale, 2013; Rubin, 2015; Schwartz, 2012; Scott, 2015; Voss, 2016). More recently, evidence of

US government practices of purchasing extra-constitutional data, such as location tracking, has been identified as a form of "data laundering" designed to evade Fourth Amendment protections (Rahbar, 2022).

Surveillance exceptionalism has meant that the United States and, to varying degrees, every liberal democracy chose surveillance capitalism and its utilities for domestic surveillance over democratic principles and governance. This choice forfeited the crucial first decade of the digital century as an opportunity to advance a distinctly democratic digital future, while secrecy deprived the public of the right to debate and combat. Gellman mourns the result: journalists were "in the dark," "plaintiffs could bring no constitutional challenge," "Congress faced no public pressure," "internet companies encountered little demand for stronger defense of privacy," and "voters and consumers could not ask for change because they did not know the truth" (Gellman, 2020, p. 127). This was the price that the democracies paid for the insatiable drive "to compute on all human-generated information."

Thanks to these historical conditions, surveillance capitalism's epistemic counterrevolution proceeded without constraint, preamble to a growing disjuncture between the emerging institution of surveillance capitalism and the democratic order. The audience was seated, the lights were dimmed, the orchestra had begun to play, but the curtain had yet to rise.

The Governance Vector: The Annexation of Epistemic Rights

Extraction operations invade and extract domains of human experience that in modern democratic societies have been considered as "private." It is not surprising that these operations have been understood as violations of privacy, and that legal theory and practice have typically aimed to establish or protect a "right to privacy" and to strengthen existing privacy law (Citron, 2022; Citron & Solove, 2022). Yet, despite rising public concerns—and, in the EU at least, the historic enactment of the General Data Privacy Regulation (GDPR)—privacy as it was understood as recently as the year 2000 has been extinguished.

The focus on privacy as the object of attack obfuscated to the point of invisibility an epic chapter in the history of the politics of knowledge. Elemental rights to private knowledge of one's own experience, which I shall refer to as "self/knowledge," were expropriated *en masse*, concentrated in the emerging surveillance capitalist order, and annexed to its self-asserted governance authority. With the term "elemental," I mean to mark a distinction between tacit rights and juridical rights. Others have addressed this distinction, and Searle's "pragmatic considerations of the formulation of rights" are useful here (Searle, 2010, pp. 194–195).

Searle argues that tacit assumptions of prerogatives, which are experienced as something like "rights," adhere to conditions of existence in a time and place. They are crystallized as formal "human rights" only at that moment in history when they come under systematic threat. For example, the ability to speak is an elemental right born of a human condition. The right to "freedom of expression" is a juridical right, which only emerged when society evolved to a degree of political complexity that the freedom to express oneself came under threat. Searle observes that speech is no more central to human life than breathing or being able to move one's body. No one has declared a "right to breathe" or a "right to bodily movement," because these elemental rights have not come under attack and therefore do not require legal codification. What counts as a fundamental human right, Searle argues, is both "historically contingent" and "pragmatic."

Elemental rights to self/knowledge belong to a larger class of "epistemic rights" that confer inalienable entitlements to varieties of knowledge and knowing (Radin, 1987). Scholars and jurists have begun to identify the speciation of these rights, such as the right to be forgotten (Allen & Rotenberg, 2016; Rosen, 2012), the right to the future tense, the right to sanctuary (Zuboff, 2019), the right to exercise human

intelligence (Risse, 2021), the right to freedom of thought (Alegre, 2022), the right to truth (Kerner & Risse, 2021), the right to revise one's identity (Tutt, 2014).

Epistemic rights are decision rights, and in the realm of self/knowledge, such rights are the cause of which privacy is the effect. US Supreme Court Justice William O. Douglas illuminated this hidden layer of epistemic rights in a 1967 dissenting opinion on a Fourth Amendment case entailing questions of illegal search and seizure (US Supreme Court, 1967, para. 66):

> Privacy involves the choice of the individual to disclose or to reveal what he believes, what he thinks, what he possesses ... Those who wrote the Bill of Rights believed that every individual needs both to communicate with others and to keep his affairs to himself. That dual aspect of privacy means that the individual should have the freedom to select for himself the time and circumstances when he will share his secrets with others and decide the extent of that sharing.

Douglas's formulation clarifies the elemental epistemic right to self/knowledge as inalienable authority over whether to disclose or withhold that knowledge, to whom, to what degree, and for what purpose. Privacy is the effect of Douglas's "choice" and "freedom to select." The secret seizure of once private experience and its rendition as behavioral data extinguishes this individual freedom and resurrects it inside the surveillance capitalist order. The epistemic rights embedded in the "freedom to select" are thus accumulated as corporate rights. Since privacy is contingent upon this freedom, the result is that privacy is expropriated, sequestered and concentrated in the domain of surveillance capital (see for example, P. Roberts, 2012). These concentrations of epistemic rights and of the privacy they enable become essential mechanisms of institutional reproduction. For example, an Amazon press release on its Rekognition system is but one tiny fragment of evidence suggesting that Searle's historical contingency is upon us. "Face analysis generates metadata about detected faces ... With this release ... we have improved accuracy for emotion detection ... and added a new emotion: 'Fear'" (Amazon Web Services, 2019, para. 1). Though one does not grant Amazon knowledge of one's fear, the corporation secretly takes it anyway, another data point in the trillions fed to the machines that day. Extraction methods enjoy privacy while robbing their targets of epistemic rights, including the right to decide "who knows me", and the right to contest the nullification of such rights.

As is the case with all elemental rights, most epistemic rights have not been codified in law because it has not yet been necessary to do so. This fact reflects the many ways in which the absence of democratic contradiction is essential to surveillance capitalism's developmental success. A new age has dawned in which individuals' inalienable decision rights to self/knowledge must be codified in law if they are to exist at all. Searle's historical contingency is now. His pragmatism reflects the conditions of existence into which we are thrown (Flyverbom, 2022).

The Social Harm Vector (1): The Destruction of Privacy

The destruction of individual privacy is the queen of social harms, a harsh measure but necessary to secure the foundations of a novel economic logic. Secret massive-scale extraction of the human and privacy cannot coexist. Page and Brin knew it. Zuckerberg and Sandberg knew it. All who worked with them and for them or invested in them knew it. For surveillance capitalism to succeed, privacy must fall. And fall it did. Most striking is that the destruction of privacy and all that follows from it has been perpetrated for the sake of the banality that is commercial advertising. This new era of surveillance advertising has brought great wealth to the few–the surveillance giants, their clients, investors, and ecosystems–but for the many it is the engine of the commodification of the human and all that follows from it. In result, the battered but not broken privacy standard of the year 2000 now appears as the final hour of a long age of innocence.

The very notion of "privacy" has become a zombie category, though discussions and contests plow ahead. Most of this discourse is trained on damage control after secret massive-scale extraction has been institutionalized: data protection, minimization, portability, security, access, deletion, transparency, interoperability ...

The giants' rhetoric, honed over two decades of crises and polished to high art in a global network of legal services and public relations war rooms, further confuses the field with deliberate campaigns of disorientation and misdirection that are themselves core strategies of institutional reproduction (see for example, *Wall Street Journal*, 2021b). One illustration plucked from the welter occurred in April 2019, when Mr Zuckerberg dramatically unveiled the company's new strategic direction to his annual developer conference: "The future is private," he solemnly proclaimed (Statt, 2019, para. 3). Less than two months later, Facebook's attorneys were in a California courtroom, repelling a class action suit concerning privacy violations brought by its own users. The lawyers argued that on Facebook, "the social act of broadcasting your personal information ... negates, as a matter of law, any reasonable expectations of privacy" (US District Court—San Francisco, 2019, p. 8).

The Social Harm Vector (2): The Rise of Epistemic Chaos

Information civilization earns its name from new conditions of existence that require persons, and increasingly all that is animate and inanimate, to be rendered as and mediated by digital information. Inclusion in the coordinates of the world's atlas means that one must be as, be in, and move through this computer-mediated realm (Flyverbom, 2022). Under these conditions, information stewardship is critical to the democratic project, beginning with the necessity of information integrity: its quality, fidelity, wholeness, and intactness free from inorganic, exogenous, willful, or secret corruption. *In an information civilization, systemic threats to information integrity are systemic threats to society and to life itself.*

Thanks to the democratic void, the question of information stewardship was never genuinely engaged. The early conflation of internet commerce and freedom of expression enabled the giants to defend their practices with a twisted notion of "free speech fundamentalism" that equated any discussion of stewardship with censorship and a denial of speech rights (Pasquale 2017a). That the democratic order has failed to confront this condition is demonstrated in countless ways around the world, as corrupt information dominates social communication and news engagement, producing mayhem across every human domain. In the United States, Allcott and Gentzkow defined "fake news" as "distorted signals uncorrelated with the truth" that impose "private and social costs by making it more difficult ... to infer the true state of the world." They found that in the lead-up to the 2016 US presidential election there were 760 million instances of a user reading such intentionally distorted signals online, or about three corrupt stories for each adult American (Allcott & Gentzkow, 2017). Research conducted by the German Marshall Fund concluded that in the last quarter of 2020, before and after another American presidential election, Facebook posts linked to deceptive sites received 1.2 billion interactions–nearly one-fourth of all posts that included links to the 200,000 US-based sites in the study. During the same period, the sharing of corrupt content on Twitter reached a new high, with 47 million "shares" by verified accounts, nearly a third of the 155 million "shares" linked to US sites (Goldstein, 2021). By 2022, 69% of Americans regarded disinformation as a more critical social problem than "Infectious disease outbreaks," "Gun violence," "Quality of education," "Illegal drug use or abuse" or "International terrorism" (McCorkindale & Henry, 2022, p. 7).

Disinformation on Facebook is known to have distorted elections, produced violence, and degraded social discourse in nearly every world region (Akinwotu, 2021; Del Vicario et al., 2016; Hao, 2021a, 2021b; Mozur & Scott, 2016; Silverman et al., 2022; Wong, 2021). In 2020, 81 countries suffered the

effects of "cyber troop activity," defined as "government or political party actors" engaged in the systematic manipulation of public opinion online (Bradshaw et al., 2021). In the second decade, 2010–2020, as Facebook became a fully operational surveillance capitalist medium of global social communications, the share of the world's population living in autocracies increased from 48% to 68%. A key mechanism in this transformation has been disinformation campaigns spread through social media, principally Facebook (Alizada et al., 2021; Reed, 2019, 2022).

In a May 2022 CNN interview, the Biden-appointed Commissioner of the US Food and Drug Agency, Dr Robert Califf, discussed his finding that "misinformation" had become the leading cause of death in the United States, with a "disturbing" effect on Americans' life expectancy (Califf, 2022; Doctor Radio NYU, 2022). How is a failure of information integrity on this scale even possible in an affluent, connected, information-rich society?

Dr Califf's tragic observation rests on Facebook's shocking, even murderous, record as the COVID-19 pandemic collided with the world's most populous social media platform to produce an endless wave of corrupt health information (Allington et al., 2021; Frenkel et al., 2020; ISD, 2020; Kouzy et al., 2020; Simon et al., 2020; World Health Organization, 2020). In August 2020 Avaaz documented the failure of Facebook's weak mitigation efforts as COVID disinformation websites attracted billions of views, far in excess of the leading public health sites (Avaaz, 2020). By October researchers determined that as many as 60% of the then 217,000 COVID deaths in the United States were unnecessary, the primary causes of these deaths originated in corrupt information (Redlener et al., 2020). As vaccines became available, the focus of information corruption shifted to anti-vaccine campaigns, obstructing the most vital public health solutions to the COVID-19 pandemic (Germani & Biller-Andorno, 2020; Loomba et al., 2021; *Perri et al. v. Robinhood Markets, Inc. et al.*, 2021; Wilson & Wiysonge, 2020).

There are many sources of disfigured information, and Facebook does not author this corruption. In the examples reviewed here and countless others, Facebook's machine systems simply worked as engineered, continuously reproducing operations that advance economic imperatives. How do the imperatives of surveillance capitalism create the conditions for corrupt information to flourish, yielding epistemic chaos within and across societies? My examination of this question focuses primarily on Facebook, the world's largest social network, but the answer actually begins with a 74-year-old treatise.

Claude Shannon's 1948 publication "A Mathematical Theory of Communication" blazed across established intellectual boundaries toward the new frontier of machine-to-machine communications and the information science it would spawn. "The fundamental problem of communication," Shannon wrote, "is that of reproducing at one point either exactly or approximately a message selected at another point." The exclusive focus was the perfect reproduction of the signal. Shannon wrote,

> Frequently the messages have meaning; that is, they refer to or are correlated according to some system with certain physical or conceptual entities. These semantic aspects of communication are *irrelevant* to the engineering problem. The significant aspect is that the actual message is one selected from a set of possible messages. The system must be designed to operate for each possible selection, not just the one which will actually be chosen, since this is unknown at the time of design (Shannon & Weaver, 1963, pp. 31–32; emphasis mine).

The engineering solution to "the engineering problem" was this *blindness by design*. Systems were optimized for fidelity to the signal while structurally indifferent to questions of the signal's fidelity to its subject. Engineered blindness equated to formal disinterest in the content of messages. The machines convey signals according to a priori instructions; they do not decipher or evaluate meaning.

With meaning out of the way, Shannon's systems were free to focus on the communication challenges faced by the Allies in the Second World War and their need for high-volume, high-velocity, precise machine-to-machine communications for signals processing, codebreaking, and encryption. These demands born in emergency later became fixtures of the Cold War milieu. The application domains were primarily mathematical content for machine-to-machine communications in high-level military research and complex engineering projects, as well as telephony, TV, and radio. In these contexts, it made sense to narrow the engineering focus to the accuracy, scale, and speed of transmission. A wholly new automated communications domain was thus constructed to serve the efficacy of transmission, while indifferent to the substance of what is transmitted.

Shannon's biographers described this "bomb" of an insight and observed, "If some humans can achieve indifference to meaning only with great, practically ascetic effort, our machines are wired for this indifference: they have it effortlessly" (Soni & Goodman, 2018, p. 135). This essential point, overlooked almost entirely in contemporary discussion, was articulated by mathematician and computer science pioneer Warren Weaver in his preface to the 1963 edition of Shannon's text:

> The word "information," in this theory, is used in a special sense that must not be confused with its ordinary usage. In particular, *information must not be confused with meaning*. In fact, two messages, one of which is heavily loaded with meaning and the other of which is pure nonsense, can be *exactly equivalent*, from the present viewpoint, as regards information. (Shannon & Weaver, 1963, p. 8; emphasis mine)

Shannon feared that existing appropriations of his work, and many more still to come, would ignore its highly restrictive definitions of "communication" (Grafton et al., 2021, p. 246). Despite his misgivings, the engineering solution to high volume and velocity of digital communications is considered the source of "all the advanced signal processing that enables us to send high-speed data" (Soni & Goodman, 2018, p. 275). Surveillance capitalism's information project is the unanticipated heir to Shannon's breakthroughs, and Facebook is the Pandora's Box that finally justifies Shannon's fears.

Facebook is a signals-processing behemoth based on the massive-scale extraction and bulk commodity processing of human-generated data. However, the signals that Facebook processes differ from Shannon's in that they are human-generated. In these systems, blindness by design is no longer a feature restricted to machine-to-machine communications. Now it is applied to *social communications* in the interests of high-speed massive-scale *human* signals processing. This mash-up produces systems for social communications in which the "semantic aspects of communication are *irrelevant* to the engineering problem." Such systems can neither decipher the meaning of what is transmitted nor assess its fidelity to "physical or conceptual entities." The result is automated human-to-human communications systems that are blind by design to all questions of meaning and truth.

From the ancestral disciplines of oral witness to the traumatic shift from the spoken to the written word, each turn in the material history of information and communication further abstracted "reality," imposing a problematic distance between the living subject and the knowable world. Every fundamental advance in symbolic media–the alphabet, mathematic notation, printed text–produced social and psychological upheaval. These conditions eventually required societies to bridge the gap between symbol and "reality" with explicit standards of information integrity and new institutions to govern those standards (Clammer, 1976; Clanchy, 1979; Goody, 1986; Ong, 1982; Stock, 1983).

Now the computer mediation of vast swathes of human existence introduces a wholly new threat paradigm to the reality problem. The extreme intensification of abstraction transforms society, social relations and social communications into symbolic objects without recourse to sentient channels of lived experience. The "death of distance," once celebrated,

imposes a new quality of distance expressed in the untraversable fissure between the sentient subject and "reality," "truth," "fact," "meaning," and related measures of information integrity. Fissure becomes chasm, as blind-by-design systems saturate society—systems that are not only antisocial but aggressively, eerily, *asocial*.

Executives have occasionally spoken frankly about this institutionalized indifference to the meaning of information. In Facebook's case, a leaked document from executive Andrew Bosworth describes the perfect complementarity between Shannon's engineering solution and Facebook's growth imperatives as they converge on blindness by design:

> We connect people. That can be good if they make it positive. Maybe someone finds love ... That can be bad if they make it negative ... Maybe someone dies in a terrorist attack ... The ugly truth is that ... anything that allows us to connect more people more often is *de facto* good ... The best products don't win. The ones everyone uses win ... make no mistake, growth tactics are how we got here. (Mac et al., 2018, sec. 2)

Shannon declared the irrelevance of meaning to the engineering problem. *Surveillance capitalism declares the irrelevance of meaning to the economic problem*. Economies of scale in behavioral signals processing require that all data are treated as equivalent though they are not equal, just as Weaver described. Facts or truth cannot have formal standing because such criteria restrict data flows. Human-generated data are and must be treated as a bulk commodity and driven through machine systems that function as supply chains, computational factories and prediction markets.

I have called this institutionalized relationship to human-generated data "radical indifference" (Zuboff, 2019, pp. 376–377). It means that neither the machines nor their owners care if your messages are fact or fiction, malicious or angelic, fashioned to produce violence or joy. They have no interest in curing your disease or what you do, or say, or buy, or eat, or think, or whom you love, or why you grieve. They simply must insist that these and every other facet of your existence is lived in ways that allow their machines to extract the predictive signals that reduce others' uncertainty about what you will do next and thus contribute to others' profit.

The aim is always to widen and accelerate the inextricable cycle of engagement> extraction> prediction> revenue (henceforth, I refer to this cycle as 'EEPR'). A consequential example was Facebook's 2018 decision to launder the kinds of sensationalized and defactualized "news" stories known to boost EEPR through the standardized presentation of its News Feed. "All news stories looked roughly the same as each other ... whether they were investigations in the *Washington Post*, gossip in the *New York Post*, or flat-out lies in the 'Denver Guardian,' an 'entirely bogus newspaper'" (Thompson, 2018, para. 22). Similarly, Facebook and Google "bankroll" clickbait farms (Hao, 2021b) as just another means of driving EEPR. The institution wants you perpetually engaged but does not, cannot, and must not–for the sake of its own economics–care what engages you. In this way blindness by design is a crucial systems principle and an essential mechanism of institutional reproduction.

These observations imply two conclusions: one cause and the other consequence. First, economics: radical indifference is an economic imperative because corrupt information is good for business. Recent research demonstrates that Facebook amplifies misinformation because it drives EEPR. Median engagement with misinformation is higher than engagement with reliable information regardless of its political orientation. But because the bulk of misinformation is produced by publishers on the far right, its superior economic value means that right-wing misinformation is consistently privileged with every EEPR optimizing algorithmic amenity (Edelson et al., 2021). Freed from the burdens of meaning and the responsibilities of witness that such burdens entail, corrupt information drives EEPR, which proceeds with the discipline of the cyclops voraciously consuming all it can see and blind by design to meaning or truth.

Second, social consequence: in the 20th century, the engineering imperative of blindness by design yielded an historic breakthrough in the volume and velocity of machine-to-machine signals transmission. In the 21st century, the engineering imperative of blindness by design yields catastrophic harms as all bits and bytes are welcomed into the global information bloodstream for immediate human-to-human transmission. The lesson: *When social information is transmitted as a bulk commodity through blind systems optimized for volume and velocity, the result is epistemic chaos characterized by widespread uncontrollable information corruption*.

Confirmation of these propositions is provided by yet another leaked internal document, this time composed in 2021 by Facebook privacy engineers on the Ad and Business Product Team. The group's functional responsibility is described as "the center" of Facebook's "monetization strategy and is the engine that powers Facebook's growth" (Franceschi-Bicchierai, 2022, para. 4). The document chronicles the growing anxiety of key employees who know that the engineering of Facebook's systems is incompatible with emerging and anticipated democratic contradiction. "We face a tsunami of inbound regulations that all carry massive uncertainty," they write (Facebook Ad and Business Product Team, 2021).

The engineers expect regulatory action, beginning in the EU, that will restrict the use of first-party data and ultimately require user consent for any deployment of personal information in the advertising process. They anticipate that increased democratic governance will trigger a doomsday scenario in which Facebook is categorically unable to comply at the required scale. They write:

> We do not have an adequate level of control and explainability over how our systems use data, and thus we can't confidently make controlled policy changes or external commitments such as 'we will not use X data for Y purpose.' And yet, this is exactly what regulators expect us to do, increasing our risk of mistakes and misrepresentation. (Facebook Ad and Business Product Team, 2021)

The engineers describe their "open" systems in contrast to the "closed" systems that they regard as necessary for legal compliance. The contrast reflects the limitations of blindness by design when applied to social information and communications. "For more than a decade, openness and empowering individual contributors has been part of our culture. We've built systems with open borders." This "openness" reflects back to Shannon's original privileging of the signal irrespective of its meaning and arcs forward to the economic imperative of massive-scale human-generated data. Indeed, as justification for its open systems, the engineers cite the volume of data required to produce a single inferential ad feature: "There are 15K features used in ads models." Approximately six thousand data tables are required to produce a single feature such as, "user_home_city_moved." The engineers compare their data flows to a bottle of ink poured into a lake. "How do you put that ink back in the bottle? How do you organize it again, such that it only flows to the allowed places in the lake?" (Franceschi-Bicchierai, 2022). Their answer? You can't.

The engineers admit that their systems are fundamentally mismatched with lawmakers' and the public's expectations. Only "closed" systems would allow Facebook to "enumerate" the data it has, "where it is; where it goes; how it's used." Without those capabilities the company simply cannot "make commitments about it to the outside world ... We fundamentally lack closed-form properties in Facebook systems" (Facebook Ad and Business Product Team, 2021).

No matter how often and loudly the public and its lawmakers are stirred to outrage insisting that Facebook must take responsibility (Donovan, 2020; see also, Atlantic Council, 2021; Browning & Mac, 2022; Frenkel, 2021; Harwell & Oremus, 2022), the engineers say that the company simply cannot comply. Worse still, the company cannot admit that it cannot. Instead, executives and staff are forced to duck and weave, misdirect, lie, and buy time. This helps to explain why Facebook continually says

that it is acting, and its actions continually fall short or fail entirely. For example, Facebook announced it would downrank groups that repeatedly share misinformation in order to reduce their total engagement. A team of French researchers investigated the intervention's effects. They concluded that while specific posts saw a reduction of engagement, behavior and quality of content were not altered. Ultimately, "the total engagement generated by repeat offender groups" did not decrease over time (Vincent et al., 2022, sec. 2, para. 3). The pattern is consistent wherever you look: Facebook knew that labeling Donald Trump's false claims did little to limit engagement (Silverman & Mac, 2020). It failed to curb murderous activities of a Mexican drug cartel or Middle Eastern human traffickers (Scheck et al., 2021). It promised to end polarizing recommendations by political groups, but the numbers grew instead (Faife & Ng, 2021; Feathers, 2021; Waller & Lecher, 2022). It established a task force to police violent political content, then throttled back on enforcement (Silverman et al., 2022). Facebook promised, then failed, to curb hate speech in Kenya and election misinformation in Brazil (Global Witness, 2022a, 2022b). Facebook, Google and Twitter each pledged to "crack down" on anti-vax disinformation but failed to do so (CCDH & Anti-Vax Watch, 2021).

Only Facebook's privacy engineers, in the assumed confidentiality of their internal communications, admit that *blindness by design is incompatible with any reasonable construction of responsible stewardship of global social communications*.

The engineers propose short-term solutions that might at least create the appearance of trying to comply with expected regulations. Possibilities include "curated data sources" and "manual" visits to "tens-of-thousands of call sites and code paths" (Facebook Ad and Business Product Team, 2021, p. 10). But action is weak, and institutionalization is strong. These engineers and their bosses know that there can never be enough content moderators, fact checkers, labelers, or any other exogeneous active measures to make a dent in the blind-by-design global automaton that is Facebook. In the meantime, the privacy engineers are bystanders to the endless con of information-integrity theatre, its fantasy remedies and excuses. They appear gripped by dread as they reckon with the widening gulf between reality and fiction, anticipating the day when the breakwater of lies is breached and the consequences flood their company and their careers.

The harsh truth for law and policy makers is that epistemic chaos cannot be "regulated" out of existence. When the engineers consider genuine solutions, they acknowledge the need for a discontinuous leap toward redefinition of the "fundamental problem of communication," as it is now entangled with the fundamental problem of surveillance capitalism. "Data Infra[structure] will need to have some semantic awareness of its data assets," they acknowledge. "Building this will take multiple years and will require data infrastructure (DI) investment" (Facebook Ad and Business Product Team, 2021, pp. 7–8). Their statement is an admission that information civilization has thus far been built on a novel genus of social information that blindly blends fact and fiction, truth and lies in the service of private economic imperatives that repurpose social information as an undifferentiated bulk commodity. Blindness by design is in charge, though it violates the most basic sociological principles of communication and common sense. The consequences of this sociological rupture are explored more deeply in the discussion of stage four, below.

Mr Zuckerberg, his executives and allies defend blindness by design as the protection of free speech, another rhetorical sleight of hand that aims to distract lawmakers and the public from noticing the facts that alarm Facebook's own engineers (Scola, 2019). A comprehensive Civil Rights Audit of the company commissioned by Zuckerberg and Sandberg condemns this misdirection strategy and Zuckerberg's "selective view of free expression as Facebook's most cherished value ... even where that has meant allowing harmful and divisive rhetoric that amplifies hate speech and threatens civil rights" (L. W. Murphy & Cacace, 2020, p. 9).

Indeed, blindness by design advances the aims of every purveyor of corrupt information, a windfall for those who benefit from the global dystopian drift. Any entity motivated by social destruction–repressive governments, illiberal politicians and their networks of allies and vassals, fevered groups of radicalized extremists, oligarchs, autocrats, outlaws–can exploit the affordances of blindness by design to inject defactualized content straight into the global information bloodstream without constraint. This is a social experiment without historical precedent nihilistically imposed upon "subjects" who can neither consent nor escape because the experimenters and their manipulations are both hidden and ubiquitous (Alizada et al., 2021; Allam, 2020; Bradshaw et al., 2021; Cunningham-Cook, 2021; Frantz et al., 2020; D. Gilbert, 2021; Holt, 2021).

In the weeks leading up to the 2020 US presidential election, Mr Zuckerberg disbanded Facebook's Civic Team, which had been tasked with producing solutions to mitigate epistemic chaos. One of the team's most respected leaders, Samidh Chakrabarti, spoke out on the company's failure to stem the flood of corrupt inflammatory content across its pages. In a series of tweets quoted in the *Wall Street Journal's* "Outrage Algorithm" podcast, Chakrabarti took aim at the destructive collision between blindness by design and social communications on Facebook's pages. According to the *Journal*, Chakrabarti observed that "treating all engagement equally, irrespective of content, will 'invariably amplify mis-info, sensationalism, hate and other societal harms. I wish this weren't the case, but it is so predictable that it is perhaps a natural law of social networks ... The challenge is almost a philosophical one that Facebook can't solve alone'" (*Wall Street Journal*, 2021a). Chakrabarti is correct. Only the democratic order can solve this one.

Three lessons from the unified field perspective can be drawn thus far. First, nothing here is inevitable. Surveillance capitalism as an institutional order was founded on the intentions of human actors in specific times and places. What is done by people can be undone by people.

Second, the social harms of privacy destruction and epistemic chaos are effects of foundational economic causes set into motion by the commodification of human behavior and the resulting imperative of massive-scale human data extraction and processing. The examination of successive developmental stages will underscore this point. The further downstream one goes, the more critical it becomes to recognize that the solutions are upstream, where the causes of harm originate.

Third, as Facebook's own engineers make clear, there is no hope for post factum solutions when the foundational mechanisms are misaligned to their task. Mitigation activities arising from outside the institution will not unseat causal operations. The purposes of democratic contradiction, as the engineers understand, will not be achieved by regulating a system that is inherently incapable of adapting to regulators' demands. A theme emerges that will be revisited several times as the unified field analysis unfolds: No amount of regulation can turn this spider into a swan, just as one does not regulate the hours a child may work in a factory. *Five hours a day for a five-year-old. Ten hours a day for a ten-year-old*. Regulatory initiatives caught in this vacuum waste precious time, breeding frustration and cynicism. *Genuine solutions will depend upon abolition and reinvention, not post-factum regulation.*

Stage Two: The Concentration of Computational Knowledge Production and Consumption (Economies of Learning)

The Economic Operations

With stage-one foundations of massive-scale extraction and datafication well established, the accelerating thrust of institutional development propelled fresh dangers to a new frontier. Stage two produces extreme concentrations of knowledge production and learning capabilities that build on earlier concentrations of human-generated data. These institutionalize competitive advantage

in ways that are self-reproducing and, in the absence of system-level contradiction from the democratic order, impregnable.

The value of the massive-scale human-generated data obtained in stage one cannot be realized without computational systems of knowledge production known as machine learning and artificial intelligence. These systems, in turn, cannot perform without an ever-expanding diet of massive-scale human generated data. The next step in the struggle for dominance over the politics of knowledge unfolds in stage two as data are transformed into information and knowledge with these proprietary computational 'means of production' along with the authority to determine what is produced, and who consumes it.

Information scholar Martin Hilbert observed in 2012 that the world's volume of digitally stored information exceeded the global capacity to learn from that information. "The only option we have left to make sense of all the data," he counseled, "is to fight fire with fire," using "artificially intelligent computers" to "sift through the vast amounts of information ... Facebook, Amazon, and Google have promised to ... create value out of vast amounts of data through intelligent computational analysis" (Hilbert, 2012, sec. 2, para. 1). Hilbert's forecast would be realized, but with a twist: The surveillance capitalists create value, but the value is for them.

A comprehensive 2021 investigation of the global market structure of artificial intelligence by Jacobides, Brusoni and Candelon (2021) emphasizes this extreme market asymmetry, noting "the remarkable and growing concentration in AI" by a handful of Big Tech companies and the resulting "economies of learning" in which "scale begets learning through the accumulation of data and increases competitive advantage ... We find that AI is adopted by and benefits the small percentage of firms that can both digitize and access high-quality data" (p. 418).

These extraordinary knowledge rewards reflect the path dependency of institutional development and all that was done in the name of data: invasion, theft, secrecy, annexation of rights, destruction of privacy, and epistemic chaos. Jacobides et al. (2021) observe that the cumulative advantages of data aggregation (stage one) create substantial barriers to entry for AI production and consumption (stage two). This dynamic is intensified in the case of computational knowledge aimed at behavioral prediction, because larger datasets increase predictive accuracy. Competitive advantage is thus linked to the giants' massive-scale data that supplies "an extraordinarily rich set of information on their customers" (Jacobides et al., 2021, pp. 421, 418; see also, Agbehadji et al., 2020; Aiello et al., 2020; Gao et al., 2019; Hinds & Joinson, 2019; Iqbal et al., 2022; Ma & Sun, 2020).

Massive-scale volume and varieties of data also facilitate the lateral spread of predictive computation as surveillance capitalism reorders industries far from Silicon Valley. Healthcare offers an example. Each of the surveillance giants pursues grand strategies for the extraction of health data, which are coveted for their lucrative predictive power. The approaches vary, but each begins with data culled from their already established systems. Google announced its intentions to "harness the billion health-related questions people ask it every day," queries which amount to 7% of daily searches, as the foundation for its efforts "to provide better healthcare" (M. Murphy, 2019, paras. 1–2).

Speaking to a gathering of health industry IT professionals, Alphabet/Google's Eric Schmidt conveyed the corporation's vision to render healthcare as the kind of computational prediction problem that only a company like Google can solve (Schmidt, 2018, 7:46–7:52, 10:17–10:59). Schmidt exhorts his audience:

> The really powerful stuff right at the edge of what I do is prediction ... Can you imagine when we have the combination of sensor data plus continuous behavioral data, which you're gonna get from your smartphone and the various smartwatches that are coming, plus all the molecular data? This data explosion is profound ... Healthcare is becoming essentially an information science.

Amazon owns the limitless health-related queries, purchases, and sales of 310 million consumers and 5 million sellers. Its One Medical acquisition provides access to the 8000 companies that offer One Medical access as a health benefit, enabling the integration of medical data with apps and ads for health products and services (Amazon, 2022; Kaziukėnas, 2021; Pifer, 2022; Quaker, 2022). Apple's Chief Operating Officer Jeff Williams, who led the engineering work on the Apple Watch, notes, "We have tens of millions of watches on people's wrists, and we have hundreds of millions of phones in people's pockets" (Fitzpatrick, 2018). Facebook and Microsoft each follow distinct paths to a similar objective (Feathers et al., 2022; Guthrie & Benjamin, 2022; McGuinness, 2022).

In 2010, former NSA director Mike McConnell publicly acknowledged that "more than 90 percent of the physical infrastructure of the web" was owned by the private internet companies (McConnell, 2010). Since then, surveillance capital has doubled down on building the vast capabilities and infrastructures required to transmit, store, and compute massive-scale data. The giants dominate research and application in frontier machine intelligence and advanced microchips (Lohr, 2019; Rosenbush, 2022). They build the largest computer networks, data centers, populations of servers, and undersea transmission cables (J. M. Lima, 2017; C. Metz, 2017a). Infrastructure dominance began in North America and Europe and now relentlessly proceeds to swallow the global south (Ahmad & Salvadori, 2020; Birhane, 2020; Stowell & Ramos, 2019). Google, Amazon and Microsoft became "hyperscalers," creating cloud computing platforms first to run their own analyses and later as an important line of business. The cloud platforms broaden the corporations' AI ecosystems and extend control over AI development with customers for and contributors to their cloud solutions (Jacobides et al., 2021, pp. 415, 417, 418). In 2022, Facebook, already a leader in real-time data processing and machine learning (Chen et al., 2016; Hazelwood et al., 2018), completed work on what it describes as the world's most powerful artificial intelligence supercomputer (Bhattacharyya, 2022).

In the second decade, surveillance capitalists further leveraged their capital and institutionalized their knowledge advantage with another self-reproducing mechanism: acquisition. They acquire and hoard scarce human, technological, and scientific resources required for knowledge production (Peterson, 2020). This reproduction strategy ignited an arms race for the 10,000 or so specialists on the planet who know how to coax knowledge from surveillance capital's vast data continents (C. Metz, 2017b). The giants purchased the most promising artificial intelligence companies (Richter, 2020), decisively deepening and institutionalizing their knowledge dominance capabilities (Bass & Brustein, 2020). The 2022 Stanford Artificial Intelligence Index reports that state-of-the-art AI results depend upon "extra training data," a trend that "favors private sector actors with access to vast datasets." In 2021, private investment in AI reached US$93.5bn, more than double the private investment levels of 2020. Concentration increased as more money chased fewer companies, with 746 newly funded AI companies in 2021 compared to 1051 in 2019 (Zhang et al., 2022).

The giants also exerted control over labor markets in critical knowledge production expertise including data science and animal behavior research (McBride & Vance, 2019; Murgia, 2019a), poaching the top scientific talent and elbowing out would-be competitors as well as startups, universities, governmental bodies and less wealthy countries. Until 2004, the year of the surveillance dividend, no AI scholar had yet traded a university post for a corporate machine-learning lab (Jacobides et al., 2021, p. 420). Between 2004 and 2018, and especially after 2010, more than 211 AI professors accepted full-time or part-time industry positions, lured by high salaries and computing resources (Gofman, 2021). By 2016, 57% of American computer science PhD graduates took jobs in industry, while only 11% became tenure-track faculty (National Academies of Sciences, Engineering, Medicine, 2018).

The surveillance empires own most of the scientists and the science. Their data scientists publish most of the research papers in AI, "an extraordinary situation compared with any other field of science" (Jacobides et al., 2021, p. 420). With so few teaching faculty, colleges and universities have had to ration computer science enrollments, which has significantly disrupted the knowledge transfer between generations (Gofman & Jin, 2022). In the UK, university administrators contemplate a "missing generation" of data scientists (Sample, 2017). A Canadian scientist laments, "The power, the expertise, the data are all concentrated in the hands of a few companies" (Murgia, 2019a, para. 11).

The problem extends to even more fundamental questions of what kind of knowledge is produced in the first instance. The giants dominate AI funding both within their ecosystems and within the academy (Jacobides et al., 2021, p. 412). The needs of their commercial operations, such as search or social media, shape the global research agenda. One prominent academic researcher observes, "Where academia might explore how social media changes how people think, a corporate social network might ask: If people post sad things, do they use our product for longer?" (Waddell, 2018, para. 12).

The successful assertion of property rights over illicit data in stage one advances in stage two with a declaration of property rights to the knowledge produced from those data. Property rights converge with epistemic rights to obscure the illegitimacy of this fresh declaration that assigns to the giants and their ecosystems the unprecedented knowledge that originates in secret extraction from the lives of unsuspecting and undefended populations.

Finally, once knowledge production is narrowed to the progress of institutional interests, that knowledge itself is concealed. Observing this blackout, Jacobides et al. (2021) note of the giants, "Secrecy, rather than patenting, remains the preferred strategy to protect their research findings" (p. 420). Under these conditions, private surveillance capital's means of production and production of meaning can only be inferred from the products and services on offer.

This use of concealment as a reproductive routine also applies more generally (Pasquale, 2017a). For example, Facebook has come under broad criticism for withholding access to data sets from social media researchers who investigate algorithmic operations and their social effects, a problem that has intensified since government inquiries into Cambridge Analytica, including its role in the UK Brexit referendum and the 2016 US presidential elections (Benesch, 2021; Bruns, 2018, 2018, 2019; Ghaffary, 2021; Gibney, 2019; Puschmann, 2019; Tromble, 2021). The company imposes onerous limitations on data use and terms of research publication (Bobrowsky, 2021; J. Horwitz, 2020; Murgia et al., 2021). Legal scholar Michael Karanicolas argues for the codification of public rights to "platform information" modeled after freedom of information laws (Karanicolas, 2021). The need for such rights reflects the conditions of institutional power shaped by concentrations of epistemic rights, privacy, data, knowledge production, and knowledge consumption in combination with the absence of democratic contradiction.

The Governance Vector: Epistemic Authority

The privatization of data about people and society in stage one founds the privatization of the means of knowledge production and consumption in stage two. Illicit concentrations of data in stage one create the conditions for stage two's illicit concentrations of knowledge. What the economist sees as oligopolistic market dominance is revealed from the sociological angle as a knowledge oligarchy in which private governance privileges over the division of learning in society are institutionalized.

Oligopolistic ownership and operational control over the means of knowledge production convey the oligarchic governance prerogatives over knowledge that define *epistemic authority*. First, the giants govern decisions over what may become knowledge in the first

instance. As we have seen, knowledge that advances their commercial interests eliminates or narrows the pursuit of other forms of knowledge, *imposing excessive opportunity costs on global society*.

Second, the giants leverage the conditions of ownership of scarce AI resources and the ability to conceal what they know in order to govern knowledge distribution. Their action to control distribution, per Searle, further declares their authority over that distribution. What may be known? Who knows? Who decides who knows? In taking command of the answers, the giants exercise the epistemic authority to command the division of learning in society.

Epistemic authority underpins the giants' confidence in their abilities to set terms of engagement with the democratic order. For example, surveillance capitalists insist that AI solutions are vital to national security and economic growth, while it is they who will most benefit from public funding—a paradox for democratic governments. In some cases, this is true both of corporations and of their executives and allies who participate as individual investors. For example, Schmidt, Google's former CEO and chairman, is a leading champion of AI in national security debates, as well as an investor in these technologies (Tech Transparency Project, 2022). In 2018, the EU pledged US$24bn over three years to spur European innovation in AI (Fioretti, 2018). Without fundamental institutional change in surveillance capitalism's control of the global AI market structure, however, such outcomes remain difficult to achieve and public funding is most likely to strengthen surveillance capitalism's dominance (Waters, 2022).

This paradox has played out with unique clarity in the United States, where democratic contradiction has been weakest. The state of play between the two institutional orders as they converge over AI is illustrated in the work of the US National Security Commission on Artificial Intelligence (NSCAI), established by the US Congress in 2018 and tasked to recommend an effective path to the militarization of AI as essential to the modernization of the United States' 21st-century war-fighting capabilities.

The NSCAI's Interim Report, published in November 2019, is particularly revealing. The report opens on lofty principles, pledging "AI systems ... consistent with, and in service of, core values Americans hold dear and the rights enshrined in our founding documents" (Schmidt et al., 2019, p. 14). However, the commission's meetings, materials, and the Interim Report itself were held in secrecy. Reports were eventually made public, but only after a contested FOIA request followed by a court order.

Equally incongruous was the commission's membership. Despite the stated democratic aspirations, the NSCAI was chaired by Alphabet/Google's Eric Schmidt. The vice-chair position went to Robert Work, a former Deputy Secretary of Defense under President Obama. Mr Work is known for his "Third Offset Strategy," a doctrine that articulates an imperative for 21st-century US military supremacy in AI as necessary to maintain historical "overmatch" with military rivals, especially China (Work, 2015; Korb & Evans, 2017). Of the 13 remaining members, 11 were tech executives, including top leaders of the three hyperscale giants, Google, Amazon and Microsoft. The rest had careers in national security or computer science. There was not a single legal scholar, privacy expert, social scientist, political scientist, or historian. There were no leaders representing civil society or labor, no civil rights, human rights, privacy, or civil liberties advocates. There was not a single constitutional expert or democracy activist. There was minimal racial, gender, or age diversity.

The report appears oriented toward renewal of another doctrine: surveillance exceptionalism. As the persuasive power of the old justifications shaped by the war on terror wore thin, Work's Third Offset Strategy helped the commission articulate a new national security case to compel doctrinal renewal. "Developments in AI cannot be separated from the emerging strategic competition with China and developments in the broader geopolitical landscape," the report declares. "We are concerned that America's role as the world's leading innovator is threatened ... that strategic competitors and

non-state actors will employ AI to threaten Americans, our allies, and our values."

With "national security" claimed to be at stake, the commission demands a reassertion of the Clinton-Gore style commitment of private-sector primacy complete with guarantees of absolute freedom of action for the giants: no law, no EU-style regulation, and no interference in corporate prerogatives. "American companies remain world leaders in AI research and some areas of application," the report says. "Our market-based economy and low regulation has created three-quarters of the world's top 100 AI startups". It argues that while public funding once produced vital R&D that drove private sector innovation, "the reversal of the Cold War paradigm" has put government into "perpetual catch-up mode," a junior partner in the quest to militarize artificial intelligence (Schmidt et al., 2019, pp. 45, 20).

The democratic failure at the turn of the digital century produced the conditions that now frame the state of play in this contest for authority over the politics of knowledge. The same companies that once depended on the democratic order's encouragement and protection now, as prefigured by Gus Hunt's 2013 remarks, hold a hand full of aces as the critical suppliers of human-generated data and its computation. This helps explain the report's audacious language and blunt assessment of the power dynamics that bend a now supplicant and compromised democracy to the surveillance capitalists' control of mission-critical resources. The commission warns that should a subordinate state attempt to rein in the giants, it will simply be forsaken by the talent and capital required to achieve its objectives:

> The government depends on the commercial sector, while the AI industry, far from depending on government business, often sees government regulations and bureaucracies as hindrances to their business models and therefore an unworthy pursuit ... the government lacks wide expertise to envision the promise and implications of AI, translate vision into action, and develop the operating concepts for using AI ... gains from AI-enabled systems can only be realized through transformation of organization structures and business processes; the inherent rigidity of government in this respect poses a major obstacle. (Schmidt et al., 2019, p. 22)

The NSCAI had reason to feel confident in its strident language and bold imposition of terms of engagement. In February 2019, just six months after the NSCAI was formed and eight months before the Interim Report, White House Executive Order 13859, "The American AI Initiative," signaled the Trump administration's eagerness to align with Silicon Valley and "remove barriers to AI innovation" (The White House, 2019). The accompanying "Guidance for Regulation of Artificial Intelligence Applications," sounding a lot like Clinton-Gore, pledged "to reduce barriers to the development and adoption of AI technologies" by rolling back existing regulations, overriding state laws and avoiding new regulations (Vought, 2020, p. 1).

Viewed through the lens of the giants' accretion of governance powers, the aggressive language of the NCSAI report also provides a glimpse of their Achilles heel. Institutionalization is the opposite of action, and the report's threatening and muscular rhetoric is a form of action. As such, it reminds us that the economic and governance gains of the surveillance capitalist order depend upon freezing every democratic impulse toward contradiction. The long game of dominance over the politics of knowledge rests on a bet that fragile democracies and their civil society communities can be bullied and bribed into submission—forms of action that require continuous attention, expenditure and effort.

The Social Harm Vector: Epistemic Inequality

Economic and social power blur. Information oligopoly shades into information oligarchy as it produces a wholly new axis of social inequality, expressed in the growing gap between the many and the few now defined by *the*

difference between what I can know and what can be known about me. Knowledge is scraped from human lives but accrues to the improvement of the few, not the many. The dogma that Big Tech democratizes knowledge obscures this new source of injustice. Early-stage harms create the conditions for later-stage harms as the destruction of privacy in stage one gives way to extreme epistemic inequality in stage two.

Durkheim again provides an historical parallel. When the young scholar wrote *The Division of Labor in Society*, the title itself was controversial. The division of labor was understood as a means of achieving labor productivity through the specialization of tasks in the new manufacturing concerns of the late 19th century, but that was not what held Durkheim's fascination. Instead, he trained his sights on social transformation far from the factory floor, observing that the division of labor as "specialization" was gaining influence in politics, administration, the judiciary, science and the arts. He grasped a more general phenomenon: the division of labor was becoming the central organizing principle not just of the economy but of society. "Whatever opinion one has about the division of labor," he wrote, "everyone knows that it exists, and is more and more becoming one of the fundamental bases of the social order" (Durkheim, 1964, p. 41).

Economic imperatives predictably mandated the division of labor in production, but what was the purpose of the division of labor in society? This new principle of social order, Durkheim reasoned, was summoned by the breakdown of traditional communities and the sources of meaning that had "mechanically" bound people to the rules and rituals of culture, place, religion, clan and kin. How would society cohere without those ancient authorities? Durkheim's answer was "the division of labor in society" as it united diverse members of a modern industrial society in a larger prospect of "organic solidarity." Society's need for coherent new sources of meaning and structure was the cause, and the effect was an ordering principle capable of enabling and sustaining a modern community. The reciprocities of the division of labor would breed interdependence and mutual respect, imbuing it not only with economic advantage but with moral force. "The most remarkable effect of the division of labor," Durkheim explained, "is not that it increases the output of functions divided, but that it renders them solidary ... it passes far beyond purely economic interests for it consists in the establishment of a social and moral order sui generis... If we specialize it is not to produce more, but it is to enable us to live in new conditions of existence that have been made for us" (Durkheim, 1964, pp. 60–61, 275).

The division of learning follows the same migratory path from the economic to the social domain once traveled by the division of labor. Now it is the division of learning that "passes far beyond purely economic interests." How does an information civilization find a path to social solidarity? The answer is a just division of learning in society as the critical new source of social solidarity. But there are complications.

Durkheim recognized that the birth of a new social order can take a dark turn, resulting in what he called a "pathological division of labor" in which organic solidarity yields to social distance, injustice and conflict. The source of such pathology, he argued, was the destructive effect of social inequalities in societies marked by extreme asymmetries of power that make "conflict itself impossible" by "refusing to admit the right of combat" (Durkheim, 1964, pp. 353–378).

The economic interests of the surveillance capitalist institutional order depend upon extreme asymmetries of knowledge production and consumption. In result, the emerging division of learning in society is already mired in the pathology of oligopoly. Privatization and concentration of the means of knowledge production do not summon a new organic solidarity. Nor do they remedy the conditions of inequality, exclusion, and risk that already plague many democratic societies, a pattern that more or less reflects the extent to which each capitulated to the Friedman consensus.

On the contrary, the division of learning now subsumes the division of labor, which becomes an expression of the new conditions of epistemic inequality. This dynamic is already visible in two key developments. First, as economist Daron Acemoglu's analysis of AI-driven automation and wage inequality concludes, AI is used to achieve "excessive" cuts in labor costs and task deskilling. These effects are not linked to the technologies per se but rather to corporate choices that favor surveillance, control and labor substitution over task enrichment and worker initiative, with destructive consequences for social solidarity and democracy (Acemoglu, 2021, pp. 2–3; Acemoglu & Restrepo, 2021; Zuboff, 1988). Second, stage two knowledge asymmetries are reflected in the international division of learning: A new kind of AI serfdom employs impoverished "gig" workers across the global south who earn starvation wages "training" AI algorithms and "moderating" content (Hao, 2022; Hao & Hernández, 2022; Perigo, 2022; see also, Birhane, 2020).

In short, the pathological division of learning obstructs the development of global society's capacity to shape and benefit from the knowledge production and consumption that defines information civilization. This diminishes the available intelligence to wrestle with existing threats while it also produces new threats. The individual and social sacrifices of stage one are not redeemed with service to the greater good in stage two, as Hilbert once imagined. Following the trail from commerce to society and economics to sociology, there is little good news.

Stage Three: Remote Behavioral Actuation (Economies of Action)

"The Tools"

Sometimes power arrives careening down the slopes that ring the valley, stallions thrashing at a gallop in a dusty whirlwind, men with bloody slaughter in their hearts riding hard to crush us at the gates. But in these days of abstraction and mediation, a new power moves lightly, unannounced, smiling like Alice's Cheshire cat. This new power is an odorless invisible poison whose signature is this: the very moment that we become aware of peril is the moment that is too late.

New power in stage three stands on the shoulders of earlier accomplishments. In stage one, the massive-scale extraction of human data supported behavioral prediction, which in turn necessitated the volume and velocity of blind-by-design information systems, which then facilitated the dissemination of corrupt information resulting in epistemic chaos. In stage two, those unprecedented flows of trillions of data points each day converge with unprecedented computational capabilities to produce unprecedented concentrations of illegitimate though not illegal knowledge: epistemic inequality.

In stage three, the capabilities enabled by these conditions come to fruition in the transformation of illegitimate knowledge into illegitimate power. Surveillance capitalism's global architectures are now sufficiently knowledgeable to shift into a higher gear from behavioral monitoring, datafication, and computation to remote behavioral actuation. Expansive and intimate knowledge about people is deployed to exploit, intensify, and weaponize epistemic chaos for targeted influence operations, including behavioral modification at scale: economies of action. Such capabilities rupture the organic integrity of individual and collective behavior, challenging human autonomy and asserting a new form of power over individual lives and societal dynamics. These developments are illustrated in a brief narrative of the Trump 2016 digital campaign's successful effort to nullify the political power of Black citizens.

In September 2020, London's Channel 4 News reporters revealed their investigation of leaked documents from the Trump 2016 presidential campaign featuring a dataset of more than 5000 files and nearly 5 terabytes. The data were amassed by the Trump campaign, largely through Facebook and the legal purchase of commercial datasets that could be linked back to Facebook profiles. The files also included Facebook data illicitly acquired by the political consultancy

Cambridge Analytica as well as data compiled by the Republican Party (Rabkin et al., 2020).

The campaign cache contained details on almost 200 million individual US voters along with the analyses, scoring and algorithmic models used to assess personality traits, political attitudes, behavioral dispositions, interests, concerns, finances, sexual orientations, vulnerabilities, and more. These were marshalled to microtarget and manipulate voter behavior in 16 states that the campaign considered essential to a Trump victory, especially the key swing states of Michigan, Wisconsin and Ohio. Campaign political advisor Steve Bannon remarked at the time, "I wouldn't have come aboard ... if I hadn't known they were building this massive Facebook and data engine" (Green & Issenberg, 2016, para. 20).

Brad Parscale, Trump's digital director, had gambled his modest budget entirely on Facebook, where corporate staff members embedded within the campaign helped the Trump team dominate surveillance capitalism's key operational mechanisms, referred to within Facebook as "the tools" (see generally, Kreiss & McGregor, 2018; Scola, 2017). With Facebook's help, Parscale pursued an unconventional digital strategy. The campaign identified three groups *least* likely to support Trump–idealistic white liberals, young women, and African Americans—and labeled these as "audiences" for "deterrence." "The tools" were deployed to persuade these citizens, especially Black citizens, not to vote. As one Trump official boasted, "We have three major voter suppression operations underway" (Green & Issenberg, 2016, para. 17).

Despite the campaign's determination to conceal its activities, the Channel 4 investigation amassed evidence detailing the "deterrence" efforts aimed at Black voters. Among the three selected audiences, 54% were people of color, including 3.5 million Black citizens. The disproportionate selection of Black citizens for "deterrence" held within each state. For example, in Wisconsin Black voters accounted for 5.4% of the population but were 17% of the campaign's "deterrence" audience (Rabkin et al., 2020).

"The tools" included nothing more than the standard range of algorithmic targeting mechanisms used daily to shape the behavior of Facebook users: subliminal cues, engineered social comparisons, psychological microtargeting, recommendations, real-time rewards and punishments, gamification, and more. Trump's data scientists, including some from the consultancy Cambridge Analytica who had worked on the Brexit "Leave" campaign, collaborated with Facebook staff to master these "tools."

Black citizens were targeted with messaging tailored to detailed individual profiles. One prominent strategy was designed to produce negative views of Hillary Clinton. For example, a proportion of Black voters were bombarded with doctored videos showing Hillary Clinton describing Black youths as "super predators." According to the Channel 4 investigation, nearly six million distinct versions of these and similar ads were injected directly into the feeds of target citizens. Most were delivered as "dark posts"—nonpublic messages whose viewership was tightly controlled by the campaign, right down to the individual voter. As Parscale described it, "Only the people we want to see it, see it" (Green & Issenberg, 2016, para. 18). All the messages advanced the campaign's dominant objective: convince Black citizens that the most effective expression of Black protest was simply not to vote.

Subsequent analyses suggest that unprecedented knowledge produced unprecedented power. According to Pew Research, "The Black voter turnout rate declined for the first time in 20 years in a presidential election, falling to 59.6% in 2016 after reaching a record-high 66.6% in 2012. The 7-percentage-point decline from the previous presidential election is the largest on record for Blacks" (Krogstad & Lopez, 2017, sec. 1). A *Washington Post* analysis sharpened the picture. Compared to 2012, the 2016 Black voter turnout rate declined by 5.3 percentage points in swing states, where the Trump campaign targeting was said to be most focused, compared to 4.3 percentage points in non-battleground states (Fraga et al., 2017). Drilling down further, Channel 4 News

analyzed voter turnout in the City of Milwaukee, home to the majority of the state's Black voters. In Precinct 116, 80% (1152) of the 1440 potential voters were Black. Nearly half of the precinct (636) was marked for "deterrence." Of that targeted group, only 206 individuals cast a vote. Overall turnout in Precinct 116 dropped from 75% in 2012 to 56% in 2016.

What happened here? The episode traces the arc of institutional progression and the way that each stage summons the next. Data demands computation. Computational knowledge fulfills its economic or political promise by shaping communications tailored to bite hard on the behavioral systems of the data subject. "Microtargeting" is the euphemism for the range of digital cueing mechanisms engineered to tune, herd and condition individual and collective behavior in ways that advance commercial or political objectives. Illegitimate knowledge is thus transformed into illegitimate power. Radical indifference means that even in a democracy, microtargeting and manipulation to deter voting is equivalent to microtargeting and manipulation to sell a new jacket.

In the case of the Trump campaign, citizens of one of the world's oldest democracies relinquished their most solemn democratic right—the right to vote—without anyone ever holding a gun to their heads or showing up in the dead of night to drag them to the gulag or the camp. Instead, these citizens ceded the right to self-govern in response to pernicious hidden mechanisms of remote behavioral actuation. Stage three's matching and targeting capabilities exploited the abundance of corrupt information established in stage one, combined with the detailed individual profiles established at stage two until enough people chose to silence their own voices and exclude themselves from political participation in a triumph of remote actuation.

This was not the totalitarian nightmare of Big Brother ready to break bodies and bend souls to its single truth. Nor was there a presiding autocrat threatening imprisonment, terror, torture, and murder. The work here was accomplished by a specific form of epistemic power that I have called *instrumentarian power* (Zuboff, 2019, pp. 351–352, 379–382). It is covertly wrung from massive asymmetries of knowledge, harnessed to the diminishment of human agency through the friction-free conquest of human action, and mediated by the Big Other of connected, pervasive, blind-by-design architectures of digital instrumentation (Zuboff, 2015, 2019, Chapter 13).

Instrumentarian power is an affordance of surveillance capitalism, available to own or rent. It works its will invisibly. No violence. No blood. No bodies. No combat. Indeed, the Trump team understood that win or lose the White House, Mr Trump had bought himself a limitless power source. "We knew how valuable this would be," Parscale said. Reflecting on the consequence of this new power, he crowed, "We own the future of the Republican Party" (Green & Issenberg, 2016, para. 22).

In January 2020, as the United States braced for another ugly election year, Bosworth laid Trump's success at the feet of Facebook's "tools." Mr Trump was elected, he said, "because he ran the single best digital ad campaign I've ever seen from any advertiser. Period." Bosworth praised Parscale, insisting that Trump 2016 "remains the high water mark of digital ad campaigns," and explained that this "unbelievable work" was the product of a simple discipline: "They just used the tools we had to show the right creative to each person" (B. Gilbert, 2020, paras. 5, 10). A senior campaign official observed, "There's really not that much of a difference between politics and regular marketing." Parscale confirmed this conclusion with style: "I always wonder why people in politics act like this stuff is so mystical. It's the same shit we use in commercial, just has fancier names" (Green & Issenberg, 2016, paras. 11, 29).

Surveillance capitalism, then, with its unique affordances and incentives, tipped the scales for Trump. Its limitless industrialized tons of human data, computational capabilities, and knowledge production created the instrumentarian power that leveraged all of it for remote behavioral actuation and turned the tides of

collective behavior to a Trump victory. Parscale's dark triumph reset the political bar. By the next US presidential election cycle in 2020, an MIT report concluded that "campaign apps" in the United States, India and other countries had become "part of a larger system of surveillance capitalism" (Gursky & Woolley, 2020).

The Economic Operations

In the wake of Brexit, Trump's election, and evidence of Russian participation in remote behavioral actuation, Facebook launched an "internal effort to understand how its platform shaped user behavior and how the company might address potential harms" (J. Horwitz & Seetharaman, 2020, para. 5). Internal research in 2017–2018 conducted by newly formed cadres of scientists and engineers called "Common Ground" and "Integrity" teams warned that the company's own algorithms amplified polarizing content as a means of driving the cycle of EEPR. These algorithmic interventions nourished the growth of far-right extremism, both in the United States and around the world (J. Horwitz & Seetharaman, 2020, sec. 2, para. 3). For example, a 2016 internal study tracked the rise of extremist content and extremist groups in Germany, where 64% of all group joins were due to Facebook's targeted recommendations. By early 2018, however, Zuckerberg lost interest in mitigating these and other social harms. News Feed was in trouble.

When first introduced in 2006, News Feed was a crucial blow to user privacy. Despite angry public pushback, Mr Zuckerberg was intransigent. If Facebook is a nervous system, News Feed was to be its aorta, the largest pipe carrying behavioral surplus from everyone everywhere to the corporation's computational heart. The feed was controlled by a secretive predictive algorithm derived from Facebook's proprietary god view of what is estimated to be more than 10,000 data elements continuously computed to assess the "relevancy" score of thousands of potential content choices. It became the most significant driver of EEPR and thus the epicenter of the corporation's financial success (Merrill & Oremus, 2021; Oremus, 2021; Zuboff, 2019, pp. 458–461).

In early 2018, as the new teams were busy reimagining Facebook, Zuckerberg announced a dramatic shift in the News Feed paradigm. The changes were presented to the public as a happy face solution to corrupt polarizing information and a defense against foreign "interference." Zuckerberg stressed a return to intimate positive connections that create more "value" for the individual, improve "well-being," enrich communities, and "bring people closer together." The revamped algorithm was to favor posts from friends and family, especially those that "spark conversations" and "inspire back-and-forth discussion." This new approach, Zuckerberg told members of the US Congress, demonstrated the company's determination to "police the ecosystem" (Hagey & Horwitz, 2021; Mosseri, 2018; *Wall Street Journal*, 2021a).

The "Facebook Files," exfiltrated from company servers and brought to the public in the fall of 2021 by whistleblower Frances Haugen, tell a sharply different story, but one that is predicted by the theory of surveillance capitalism. According to the *Wall Street Journal* reporters who studied the documents, the varied atrocities of the 2016 US election produced an alarming decline in Facebook's "engagement metrics" throughout 2017. These results triggered panic among executives, who diagnosed the cause as a shift to passive viewing of professionally produced content. The algorithmic redesign, labeled "Meaningful Social Interactions," was engineered to reverse the decline in comments and other signals of engagement. This solution for the threat to EEPR "would reward posts that garnered more comments and emotion emojis" (Hagey & Horwitz, 2021).

The logic of system design to optimize for EEPR had been baked into the cake from the start, as noted in our discussion of epistemic chaos. Mechanisms like those that drove German extremism were well established. The difference in 2018 was that now News Feed, the driver of the nervous system, was harnessed

to this single goal. The new algorithm measured multiple dimensions of interaction, assigning points to detailed signals: likes, shares, reactions, emojis, the anger button, comments, RSVPs, and so on. The higher the score of an interaction, the more "significant" the engagement, the more widely the algorithm disseminated that interaction as bait for more engagement.

The News Feed algorithm was a social communications system engineered to follow the math not the meaning of interactions, just as Shannon had prescribed for his machines. Unsurprisingly, the News Feed system reengineered to maximize interaction did not favor content from family and friends for amplification. Instead, the content that earned the highest engagement scores, as it reliably "sparked conversations" and provoked the most "back-and-forth discussions," was the worst content: corrupt, defactualized, grotesque, hateful, false, polarizing, extremist, and anger-inducing. By the summer of 2018 the decline in key engagement metrics had slowed and, in some cases, reversed (Hagey & Horwitz, 2021). But user surveys showed that the degraded quality of the News Feed diminished people's sense of well-being. A slide from a 2018 Facebook presentation read: "Our algorithms exploit the human brain's attraction to divisiveness" (J. Horwitz & Seetharaman, 2020), a phenomenon already identified in academic research (Vosoughi et al., 2018).

Once again, internal studies identified the measurable effects of engagement engineering on polarization (Hao, 2021b). The difference now was that the all-powerful News Feed was specifically reengineered to optimize EEPR. Behavioral effects spread widely and quickly as every individual user, publisher, organization, or troll farm found themselves chasing the proof of life that Facebook's validating metrics provided. Any person, group, or entity that wanted to participate in the attentional slipstream of likes, shares, comments, audience, and so on, had to engage in the macabre "back and forth" of social outrage. As they did so, both they and their "lookalikes" were targeted with more toxic content for more EEPR, and on, and on ...

A global social network optimizes its central operations for EEPR, saturating the information and communication space with corrupt content and targeting those who can be goaded into making the largest contribution to its commercial aims. Facebook operates like a planetary Skinner box, and the consequences for collective behavior spread. Poland's political parties joined others across Europe, claiming that the arrival of the euphemistically labeled "meaningful social interactions" in 2018 "changed the nature of politics for the worse." The political parties observed that Facebook's emphasis on resharing content "systematically" rewarded "provocative, low-quality content" and they found themselves adapting to Facebook by publishing "far more negative content than before" (R. Metz, 2021). In Spain, Facebook pages related to social and political debate saw a 43% increase in threats and insults (Constella, 2021). Positive headlines and policy posts simply did not contribute to EEPR.

As Facebook's pages turned uglier, the teams proposed mechanisms to at least mitigate the intensification of chaos. For example, one proposal outlined new moderation techniques for private groups and methods to limit the number of posts on inflammatory subjects. Another team developed a method to reduce the spread of content favored by hyperpartisan hyperactive users. The teams understood that, contrary to Friedman, implementation would interfere with EEPR. Some of their ideas were "antigrowth" and implied "a moral stance" (J. Horwitz & Seetharaman, 2020, sec. 3, para. 3).

There were political concerns too. As we have seen, surveillance exceptionalism imposes an enduring political burden that ricochets between appeasement and conflict. In 2018 Facebook was already on the political defensive, accused by Republican lawmakers of systemic anti-conservative bias (US Senate Committee on Commerce, Science, & Transportation, 2016). Because polarizing hyperpartisan misinformation was disproportionately produced by conservative and right-wing sources, beginning

with then President Trump, Facebook executives feared political retaliation if they curtailed such content (Dwoskin et al., 2020; Evanega et al., 2020).

Facebook's new teams battled with politically wary executives, but in the end their proposals were killed or fatally weakened (Roose & Isaac, 2021; Timberg, 2020). By late 2018, Mr Zuckerberg informed his staff that he had lost interest in reorienting the company toward "social good" and asked that they refrain from bringing him more proposals. The Common Ground team disbanded, and many senior staff involved in the remediation efforts left the company. Employees were told that Facebook's priorities had shifted "away from societal good to individual value" (J. Horwitz & Seetharaman, 2020, sec. 4, para. 11).

As engagement and polarization grew, concern over the 2020 US election season deepened. In April 2019, a data scientist with the Civic Team advanced a method for reducing the spread of "deep reshares" associated with virality and known for their negativity and sensationalism. According to documents provided by Haugen, the method was proven effective in tests on civic and health information. Once again, Zuckerberg stood down, citing his concern that the change would reduce "positive" engagement. A parade of substantive proposals, from eliminating the "reshare button" to restricting comments, and more, met the same fate "because the company determined it would hurt user engagement" (*Wall Street Journal*, 2021a; see also, Hagey & Horwitz, 2021). Active interventions are typically only favored post-factum, once extreme damage, such as the 6 January 2021 riot on Capitol Hill, risks democratic contradiction or widespread user withdrawal (for examples, see Merrill & Oremus, 2021).

The Governance Vector: The Governance of Collective and Individual Behavior

Instead of solutions, Mr. Zuckerberg wantonly pounds his algorithmic keyboard of humanity's collective behavior, reinforcing or extinguishing the actions and attitudes of billions of people at will, as ordained by the economic imperatives to which he is pledged. He strikes this key or that from his celestial perch, and qualities of human behavior and expression rise or fall. Anger is rewarded or ignored. News stories are more trustworthy or unhinged. Corrupt information is showcased or sidelined. Publishers prosper or wither. Political discourse turns uglier or more moderate. People live or people die.

From the point of view of economic operations, remote behavioral actuation is a means to economies of action and their commercial ends (Zuboff, 2019, pp. 293–299; see also, Merrill & Oremus, 2021; Oremus, 2021). But from a governance perspective, it signals the assumption of systemic governance powers over the content, pattern, and flow of individual and collective behavior. This compromise of behavioral integrity, as seen in the case of the Trump 2016 campaign, is a stealth attack that originates from outside the social, denying its victims the right of combat by distorting the social order without triggering awareness.

Facebook has explicitly engaged in detailed tracking of collective behavior since at least 2009, when it went public with its Gross National Happiness Index continuously compiled from users' posts. The *New York Times* reported that the company was also analyzing the ethnic and racial status of its users, how groups interact, and how those interactions change over time as an "important indicator of the state of the nation" (Cohen, 2009, para. 20; Siganos et al., 2014). Facebook's metric for large-scale monitoring of "Violence and Incitement Trends" was first reported in 2020 (Mac & Silverman, 2020, para. 3). There is little public information regarding how these and other proprietary forms of behavioral knowledge are used to remotely actuate and suppress collective behavior.

Zuckerberg's decisions between 2018 and 2020 demonstrate Facebook's reliance on remote behavioral actuation for continued growth. This shift of focus from tracking collective behavior to actuating behavior is not new. It emerges from a long period of incubation, most clearly identified with Facebook's

published contagion experiments (Bond et al., 2012; Kramer et al., 2014) before public backlash alerted Zuckerberg to the need for secrecy (Zuboff, 2019, pp. 304–309). Both studies designed and tested remote actuation capabilities aimed at measurably influencing collective behavior. In the first, targeting mechanisms based on engineered social comparisons and subliminal cues were deployed to influence users to vote in midterm elections. In the second, subliminal cues were manipulated to induce feelings of sadness or happiness among users. While many academics and tech observers reacted in horror, the company researchers celebrated the successes of their experiments, noting that it was possible to manipulate online triggers to influence real-world behaviors and emotions at scale without engaging user awareness. Indeed, the company publicly touted its ability to influence election outcomes on its "success stories" page, before removing those links in early 2018 (Biddle, 2018a, para. 1).

Contemporary studies by academic researchers have closely examined many of the dynamics identified in this discussion and their causal role in rising societal polarization and diminished social resilience (Cinelli et al., 2021; R. Levy, 2021; Rathje et al., 2021; Santos et al., 2021; Tokita et al., 2021; Vasconcelos et al., 2021). While there remains a great deal to learn, the preponderance of findings illuminates the relationships between algorithmic design, the swell of corrupt content and social polarization. This pattern is so prominent that it suggests the hypothesis that the corporation is now engaged in a mega-massive-scale contagion experiment, *this time trained on triggering social contagions of polarization*.

Considered from this perspective, the Haugen documents provide an updated view of contagion science after a decade of intensive, and intensively concealed, development. Experimental principles are similar to those in earlier work. Persons are objects of tailored stimuli and forms of reinforcement that operate outside of awareness to impel thought, feeling, and action. These interventions appear capable of evoking, selecting and reinforcing behavior in ways that disrupt human agency, alter behavioral trajectories, and abrogate "the right to the future tense" (Zuboff, 2019, pp. 329–348). The difference now, one decade after the published experiments, is that "the experimenters" employ far more powerful computational capabilities along with more vast and varied accumulations of behavioral surplus. These enable exquisitely fine-tuned delivery systems with a more diverse and effective range of targeting weaponry.

Indeed, the power and capabilities to modify collective behavior at this kind of scale are closely associated with "information warfare" (Corn & Taylor, 2017; Hollis, 2018; Libicki, 2017; Lin, 2019). For example, Crețu et al. (2022) demonstrate how massive-scale anonymous datasets on human interactions reveal individual identities and sensitive information that can be used for "matching attacks" or other attacks based on "behavioral profiling."

Information warfare is widely assumed to be a capability of the State for the purposes of political, cultural, or military destabilization, just as behavioral modification or surveillance were once considered projects of the State. Now the affordances of the surveillance capitalist order reconfigure information warfare as a market project. Indeed, it is only on the strength of this construction that State or non-State actors can succeed as parasites on surveillance capitalism's host body, using its "tools" to wage information war on civilian populations for commercial or political purpose, as illustrated by the Trump 2016 campaign.

Equally threatening to democratic freedoms is the fusion scenario, in which the information appetites of the state produce a relentless source of demand that merges with the relentless supply of human-generated data from the surveillance giants. Such operations, once legitimated by a "war on terror," have been turned on civilians in a full-on display of citizen-targeted information warfare that plaintively illustrates how the democratic void leaves us naked and vulnerable. Surveillance advertising once again plays the Trojan horse. For example, RTB data have been used to profile Black activists, obtain warrant-less phone

tracking, and surveil individuals (Ryan, 2022). Amazon has admitted to giving data from its Ring doorbells to law enforcement officials without warrants or the knowledge and consent of owners (Díaz, 2020; Biddle, 2022; Selinger & Durant, 2022). Law enforcement agencies at every level of government acquire location tracking data captured by apps and aggregated in the private market (Burke & Dearen, 2022; Shenkman et al., 2021).

The fusion scenario is now vividly on display in a United States where state-level abortion bans turn law enforcement and judicial authorities toward data from the giants as a means of transforming pregnant women into prey (Collier & Burke, 2022; Linebaugh, 2022; Nix & Dwoskin, 2022; Ohlheiser & Kiros, 2022; Zakrzewski et al., 2022). Most disturbing is the speed with which these operations are normalized. American women are warned that their cell phones are now a "reproductive privacy risk" (Li, 2022). An article in the *Washington Post* begins calmly, "Everything you do online is already tracked," and it advises women "to avoid leaving a digital trail." This includes warnings and guidance more typically associated with CIA spymaster training: restrict communications to secure encrypted messaging; set messages to disappear; deactivate biometric authentication and location sharing on devices; avoid apps, health-tracking wearables, Google, license plate and facial recognition software readers; beware of cross-site tracking and check-in software at your doctor's office; scramble your identity and location on all devices; log out of accounts; maximize privacy settings; use alternate transportation ... (Kelly et al., 2022). If today communities of color, activists, and now the vast category of pregnant women and their allies can become targets of information warfare, then tomorrow it can and will be any and all persons or groups. "First they came for ... "[4]

Recent scholarship in information warfare has begun to theorize these interdependencies. Dawson (2021) observes that the US government has been sounding the alarm on targeted influence operations on social media without understanding that the "digital surveillance economy" is the cause. "[T]his economic structure of trading free access for data collection about individuals' lives poses a national security threat." She notes that the unique commercial capabilities of this economic institution are "increasingly harnessed for mass population control ... with virtually no oversight or regulation" (p. 63).

Just as systemic threats to information integrity are threats to the social order of an information civilization, systemic threats to behavioral integrity are threats to the very possibility of social order. In recognition of this phenomenon, an important paper by an international team of scholars argues that the study of collective behavior "must rise to a 'crisis discipline' ... with a focus on providing actionable insight to policy makers and regulators for the stewardship of social systems" (Bak-Coleman et al., 2021). Without clarity on the source of such threats, however, there is little prospect of effective contradiction. For example, Bak-Coleman et al. repeatedly identify "technology" as the causal force. They note that "information flows" once shaped by natural selection are now at the mercy of "emerging communication technologies," thus necessitating careful study of "the impact of emerging technology on global behavior." But in other instances, their argument implies a generalized economic causality, citing "engineering decisions made to maximize profitability" and "vested interests" that have "taken advantage of new communication technology to spread misinformation" (pp. 1–2, 4).

The power to compromise the integrity of individual and collective behavior cannot be attributed to the internet, social media, communications technologies, the information economy, information capitalism, shadowy vested interests, or even the profit motive per se. The unprecedented power to exercise secret illegitimate governance over human behavior at scale, as described here, is produced by specific path-dependent economic operations and capabilities developed in time and guided by the historically unprecedented logic, mechanisms, and imperatives of surveillance capitalism, in

which revenues flow from the commodification of human behavior.

This distinction is good news, because it means that despite the scale and force of surveillance capitalism as an institutional order, nothing about it is inevitable. The governance achievements and social harms discussed here are not the product of technological *or* economic necessity. While technological evolution is a fact of modernity, surveillance capitalism is but one economic logic among many other possible logics for bringing digital technologies to life, constructing an internet or its successors, building an information economy, and structuring the social order and moral milieu of an information civilization. It is wholly within the capabilities of the democratic order to abolish surveillance capitalism and free the digital from its iron cage in order to reimagine, reinvent and reclaim our information civilization for a democratic future nourished by data, information, and knowledge.

The Social Harm Vector: The Artificial Construction of Reality

In *The Social Construction of Reality*, Peter Berger and Thomas Luckmann (1966) famously observe that the miracle of durable social order rests on "commonsense knowledge." This knowledge is not the same as "shared values." It operates at a tacit level. The phone rings. You answer with "hello," and the caller replies, "hello." It is "the knowledge I share with others in the normal, self-evident routines of everyday life" (p. 23). Daily traffic patterns, for example, depend upon far more than obeying laws.

"All societies are constructions in the face of chaos," write Berger and Luckmann (p. 103). Because norms are summaries of common sense, norm violation is an important element of terrorism, stoking fear precisely because it repudiates the most taken-for-granted social certainties upon which an orderly society rests. Without the social construction of reality, everyday life is unbearably precarious. The death of the king or, in a democracy, the peaceful transfer of power are critical moments that heighten societal vulnerability, which explains why the prescriptions that guide these junctures are treated with maximum gravity. The legitimacy and continuity of institutions are essential because they buffer society from chaos by formalizing common sense in norms, rules and laws. So, for example, when Zuckerberg decided that the destruction of privacy should be the new norm, and he "just went for it," that was a profound violation of the norms that express commonsense knowledge. It was a form of terrorism from which the democratic order failed to protect its peoples.

The social construction of reality rests on a common sense of what is "normal," what is a deviation from the norm, and what is a destructive deviation. Formula One driving is thrilling on the track but a norm-defying form of terror in the neighborhood. Racetracks and neighborhoods can coexist because there is durable faith that everyone agrees on the appropriate behavior in each setting. This faith depends significantly on trustworthy, transparent, and respectful institutions of social discourse, especially when there is disagreement. Even destructive deviations do not require censorship in an open society because, thanks to common sense, they "normally" rise and fall and fade at the fringe, where they belong.

Surveillance economics, as we have seen illustrated at Facebook, produce the opposite of these conditions. The company operates as a chaos machine where "norm violation" drives EEPR and corrupt information is good for business. Zuckerberg, like other owners of social media, portrays his network democracy's "public square," protected—in the liberal democracies, at least—by a guaranteed right to freedom of speech. Mr Zuckerberg's "free speech fundamentalism" has provoked much academic debate and paralyzed the public response (Shapiro, 2021). Considering the US case, constitutional scholar Laurence Tribe tirelessly explains that First Amendment rights do not apply to Facebook's discourse, because its social media spaces are not public spaces and do not operate under public law. They exist

under the jurisdiction of private capital, not governmental authority. Tribe writes, "The First Amendment, like the entire Bill of Rights, addresses only government action, not the action of private property owners. That's not a bug but a feature" (Tribe, 2021, para. 5; see also, Citron & Franks, 2020; Fidler, 2021; Horder, 2021; Gingerich, 2021; Shattuck & Risse, 2021; Wu, 2017).

This jurisprudential analysis of freedom of expression is complemented by an implicit sociological vision that situates these rights in specific conditions of existence. US Supreme Court Justice Oliver Wendell Holmes drew upon this vision in his 1919 dissenting opinion in *Abrams et al. v. United States* (1919). "The ultimate good desired is better reached by free trade in ideas," Holmes wrote. "The best test of truth is the power of the thought to get itself accepted in the competition of the market ... That at any rate is the theory of our Constitution" (para. 58). Holmes's characterization speaks to the societal warp that complements the juridical woof of speech rights. It assumes that the social function of free speech protections is the renewal of society. Under conditions of freedom and rule of law, ideas that renew society—even those that arise at the margin—will ultimately find wide acceptance through fair and free debate. This sociological vision of a public square ordered by the natural selection of good ideas through open discourse and common sense is idealized, but it expresses the societal aspirations and purpose attached to speech rights.

On the path toward accidental dystopia, the public square and its "social construction of reality" are vanishing, replaced by a private zone of digital information and communication ruled by the imperatives of surveillance capital. Algorithmic engineering supplants the social construction of reality with an artificial construction. The corrupt information that increasingly dominates this private space does not migrate to the center of social discourse in a free and fair competition of ideas. Rather, it is placed and held at the center by a process of *unnatural* selection dictated by surveillance capitalism's political-economic objectives (see also, Balkin, 2017; Riemer & Peter, 2021; Ward, 2022).

This unnatural selection, optimized for EEPR, violates the integrity of collective behavior, reshaping thought, speech, and action. Corrupt content is selected for first-class privileges of targeted dissemination and amplification. In the absence of contradictory institutional forces that impose and defend measures of information integrity already discussed, such as "truth," "fact," "reality," and "meaning," blind-by-design systems artificially marginalize commonsense speech as a means to others' commercial or political ends. These dynamics produce the opposite of the societal qualities that juridical speech rights are intended to foster. Because these operations are hidden, the whole process proceeds theatrically, as if its consequences are organic social constructions rather than privately owned and operated artificial productions authored by economic imperatives and political accommodations.

Facebook executive Andrew Bosworth once again does his job by denying this bait and switch of an artificially constructed reality for a social construction. In the blizzard of criticism accompanying the Haugen revelations, Bosworth became the spokesperson for a desperate new line of rhetoric. Now, "individual humans" were to blame for spreading misinformation on Facebook, and he questioned the company's right even to identify misinformation. "I'm very uncomfortable with the idea that we possess enough fundamental rightness ... to exercise that kind of power on a citizen, another human, and on what they want to say and who they want to listen to" (Feuer, 2021, para. 14; C. Lima, 2021).

Bosworth reminds us that concealment and Orwellian communications remain essential to institutional survival and development. These mechanisms intensify in an increasingly desperate bid to buy time, as the veil is drawn on Facebook's displacement of organic social processes in favor of its own self-interested designs for humanity.

Stage Four: Systemic Dominance (Economies of Domination)

The Economic Operations

Stage four is marked by an increasingly visible competition with democracy over the governance of governance. The successes of economies of scale, learning and action in combination with the continued absence of effective democratic contradiction produced historic concentrations of data, knowledge, authority, power, capital, and infrastructure control. These come to fruition in the giants' increasing confidence in their ability to leverage absolute control of critical digital infrastructure to bend democratic governments to their will: systemic dominance.

In earlier stages, the surveillance capitalist institutional order challenged rights and capabilities that are mission-critical to a democratic society, including privacy, information integrity, knowledge production, social solidarity, common sense, and the integrity of individual and collective behavior.

Stage four exploits the conditions produced by these early and ongoing governance carveouts and societal attacks. A new offensive emerges aimed at democratic institutions. The giants' control over critical digital infrastructure is leveraged as a means of weakening and then usurping the governance prerogatives of the democratic state. Examples of this emerging competition for systemic dominance appear with increasing frequency.[5] In this discussion I examine one such case played out between an alliance of Apple and Google versus the democracies of the European Union, as global plague spread fear across the continent.

Revenge of the Void. It was on April 10, 2020, as the world faced the most dangerous public health emergency in a century, that Apple and Google abruptly introduced a COVID-19 exposure-notification protocol for iPhones and Androids that was incompatible with exposure-notification and contract tracing applications already in development by EU teams (Holmes & Langley, 2020; Wuerthele, 2020). A coalition of 130 data scientists from eight European countries, including teams of German, French, Italian and Spanish technologists, had been working on an approach they called "Pan European Privacy Protecting Proximity Tracing" (PEPP-PT). Their aim was a smartphone-based set of "standards, mechanisms, and services" that could (1) inform individuals of COVID-19 exposures and test results; (2) operate seamlessly across the EU and other borders; (3) support public health authorities' research, policy development and oversight; and (4) accomplish these objectives while complying with the stipulations of the GDPR and related EU privacy laws (PEPP-PT, 2020).

Ultimately, the revenge of the void would sink its claws deep into the data scientists and privacy experts on the PEPP-PT teams, as well as many watching from the sidelines. It was a professional group all too familiar with the threat of illegitimate surveillance. Despite its leadership in privacy law and data protection—or more likely because of it—the EU became a key theater of engagement in a mounting battle between trust and fear, organic solidarity and libertarian values. This discussion examines key highlights of these events as they illustrate the contest for systemic dominance at the frontier of surveillance capitalism's developmental progression (see Note on Method).

Some context is useful. Public health professionals routinely employed the language of "surveillance" long before the term was burdened with the dystopian themes of the digital century. Public health "surveillance systems" effectively eradicated smallpox in the 1970s, tuberculosis in the 1990s and SARS in 2003. These victories typically depended upon individual case data in some combination with epidemiological statistical tracking, as dictated by disease dynamics (Bay, 2020; Hellewell et al., 2020; Sontani et al., 2020). Public health scholars were already grappling with the implications of disease surveillance in the digital century when COVID-19 overwhelmed health authorities across the globe (Ramjee et al., 2021; Sekalala et al., 2020; Stoto, 2008).

On the eve of pandemic Europeans enjoyed high degrees of trust in their public health authorities (Wellcome, 2019). Eighty-three percent of Germans indicated substantial trust in their government's medical and health advice. In the UK it was 81%, 77% in Spain, 70% in France, 63% in Italy, compared to only 59% in the United States (Archer & Levey, 2020).

The COVID-19 pandemic evoked what was for many a new appreciation of social solidarity and the positive role of government, but it also produced exceptional conditions of vulnerability and digital dependency that some governments and corporations exploited to extract more data, consolidate more powers or both (Lyon, 2022; Rahman-Shepherd et al., 2021). In the EU, the Hungarian government used the pandemic to justify an indefinite "state of emergency," authorizing the government to rule by decree and weaken parliamentary oversight (Zoltán, 2020). The Polish government pounced on the health crisis as an excuse to schedule elections during the first pandemic wave, in defiance of existing laws, the Polish constitution and a Senate resolution (Radjenovic et al., 2020). The UK's National Health Service (NHS) announced a data-sharing agreement with Google, Microsoft, and the secretive data mining analytics firms Palantir and Faculty. Described as "the largest handover of NHS patient data to private corporations in history," the NHS claimed the companies would provide a "single source of truth" with which to track the pandemic (Fitzgerald & Crider, 2020).

Similar moves in the United States were mitigated only by the Trump administration's incompetence and general disinclination to govern. The White House unleashed a tech sector bonanza as it turned to the giants for solutions, supposedly "to leverage the tech industry's powerful tools," but certainly to lend a patina of competence to chaotic White House operations (Grind et al., 2020; Romm, 2020, para. 2). The Trump administration hired Palantir to build a comprehensive system for virus tracking (Banco & Ackerman, 2020). Other proposals ran the gamut from the terrifying to the slapstick. Trump's son-in-law, Jared Kushner, announced the tech companies' collaboration on a "National Coronavirus Surveillance System" (Cancryn, 2020). The White House consulted with the companies on comprehensive location tracking (Romm et al., 2020). Trump boasted the immediate implementation of a nationwide system for screening and testing to be implemented by an obscure Alphabet subsidiary, Verily, an organization that had neither knowledge of the project nor experience in building and managing such systems (MacMillan et al., 2020).

It was against this background of a global dystopian surge that Apple and Google encountered an extraordinary opportunity to display and enhance systemic dominance. Their success depended largely upon the revenge of the void. The democracies' two-decade failure to claim digital spaces for democratic values and the rule of public law had abandoned citizens to the incursions of private and public mass surveillance, igniting its own pandemic of suspicion and mistrust. In the absence of epistemic rights, comprehensive new legal frameworks, and the public institutions and enforcement powers purpose-built to protect them, many feared that COVID-19 would quickly morph into COVID-1984. Without explicit legal protections, such as strict purpose limitation, sunset laws, transparent verification procedures, and more, it was easy to imagine that COVID surveillance undertaken in the name of public health would never be unwound (Amnesty International, 2020; Timberg & Harwell, 2020). These fears stirred disagreement among the PEPP-PT teams (Abboud et al., 2020; M. Johnson et al., 2020).

Led by French and German scientists, the PEPP-PT consortium published its mission statement on April 1, 2020. Citing the emerging evidence from COVID surveillance in illiberal societies, it stated a commitment to "strong European privacy and data protection laws and principles," while maximizing the effectiveness of a "national pandemic response." Data would be shared with health authorities to facilitate COVID monitoring, analysis and policymaking in a way that "enforces GDPR and ensures scalability" (PEPP-PT, 2020, paras. 4, 7).

A dissenting faction had emerged in March that year, led in part by Professor Carmela Troncoso, head of the Security & Privacy Engineering Laboratory at Switzerland's École Polytechnique Fédérale de Lausanne (EPFL) (VIScon, 2020, 47:50–49:00). A security and privacy specialist and recent recipient of a Google Research Award, Professor Troncoso was alarmed at the prospect of COVID-19 exposure data held in government servers and, she argued, vulnerable to "data grab," deanonymization, and other symptoms of "function creep." The group's proposed solution was a "decentralized" model in which data and computation would be strictly confined to one's smartphone, eliminating the "risks of privacy abuse." Troncoso swiftly recruited colleagues from EPFL and EHZ[6] to pursue this model. Experts from across Europe soon joined this team. Initially, the dissenters remained within the larger PEPP-PT undertaking. But as "things soured pretty quickly," they withdrew to focus exclusively on their own approach, while attempting to shut down the PEPP-PT effort (Abboud et al., 2020, para. 15).

On April 3, the dissenters, by then 25 strong, published their protocol for what they called "Decentralized Privacy-Preserving Proximity Tracing (DP-3T)" (Troncoso et al., 2020a). Their technical strategy was distinguished from what they described as PEPP-PT's "centralized approaches with very different privacy properties" (Troncoso et al., 2020b, sec. 6). The language choice of "decentralized" versus "centralized" was a public relations coup that produced an immediate media explosion in a Europe already on edge. While neither term had appeared in the PEPP-PT mission statement, the image of "decentralization" immediately conjured associations with pro-social democratic ideals and fundamental rights, while the word "centralized" triggered fears of Big Brother and Chinese-style surveillance. "Methods are introduced to strictly control data flows in order to avoid accumulating any contact data on a centralized server," the DP-3T team wrote (Troncoso et al., 2020c, p. 2).

According to one public official I interviewed, this rhetorical structure was "a marketing triumph" that took EU leaders by surprise:

> At the time, we didn't know where the label "centralized" came from, but that language took over very quickly. Who likes "centralized"? Suddenly, everyone was scared that authorities would surveil them. No one seemed able to imagine or believe that a so-called "central" server can be used constructively and safely by the health authorities in the member states according to our laws and fundamental rights, without following you or keeping your data. (PO IV)

Indeed, a lack of trust in government was at the heart of the dissenters' rationale for "decentralization." In the opening lines of the April 3 DP-3T publication, decentralized system design was justified as the necessary response to a pandemic that races "across borders and jurisdictions with different levels of fundamental rights guarantees or in times where many governments are functioning under rules of exception" (Troncoso et al., 2020c, p. 1). But other arguments in the DP-3T materials suggest a broad loss of faith in the rule of law and a generalized distrust of all governments, including democratic governments. Indeed, proponents of the "centralized" model were criticized for trusting the rule of law. "They purely rely on legal norms ... This model advocates disproportionate collection of personal data, and assumes legal protections will be sufficient to protect populations which often is not the case" (Troncoso et al., 2020c, p. 1).

One DP-3T team member, EHZ computer scientist Professor Kenneth Paterson, described to an audience the project's "bunch ... of tight-knit academics" united in a mission "to build a system that didn't have any unintended side effects." He explained that only "a decentralized architecture ... where all of the work is done on the phone under the control of the user and not at some central server under the control of a government" can protect individuals from mass surveillance. "Do you trust your government?"

Professor Paterson asked his audience. "I don't ... I actually don't trust my government ... to competently handle that kind of data ... you shouldn't trust your government; you should trust decentralized designs ... This is about building trust for the public in the system so they can be encouraged to use it" (VIScon, 2020, 14:43–14:48, 39:00–40:02, 40:14–40:49).

Professor Paterson's views may sound extreme to some readers, but they place him in the mainstream of the libertarian ideology that passed through Hayek, Friedman and others to become the taproot of Silicon Valley's worldview. Data Scientist II explained:

> Libertarianism is the ideology of Silicon Valley. This community fosters a general mistrust of government and all institutions. There is a norm that centralization is always bad. Group identity in Silicon Valley is that government is out there trying to impose things on them. Government is a relic that can't understand or keep up. There is a myopia, a focus on the technical side of things rather than seeing these larger dangers of institutional politics and power. This made sense when they were little hacker startups, but now they are the most powerful corporations in the world, but somehow folks still think this way. (DS II)

Under these perceived conditions of pervasive assault and defense, Paterson regarded manual contact tracing as "highly privacy invasive." Epidemiological research was considered "data overreach." "We were not then in a position to collect additional data that could be useful for ... the health systems" (VIScon, 2020, 6:44–6:56, 15:11–16:03).

There were technical hurdles. Without the cooperation of the two technology giants that control the critical digital infrastructure of Europe's—and most of the world's—smartphone operating systems, it would be impossible to implement either DP-3T or PEPP-PT effectively and at scale. Both required Bluetooth low-energy beaconing in lieu of GPS-based location tracking. Without technical adjustments, COVID-19 applications were not able to maintain Bluetooth "in the background," quickly draining the cell phone battery.

A presentation by Professor Troncoso reviewed this early stage of the project in a series of PowerPoint slides, some of which feature a vividly portrayed Eye of Sauron bearing down on the words "security and privacy." When it comes to the question, "Who decides?" the answer is stated unequivocally: "The system design. Platform decides Exposure Notification." Another page reads: "Reality. Use Existing Infrastructure ... Apple must be involved ... Google and Apple must be involved ... Google and Apple implement the protocol and the API" (Troncoso, 2021, pp. 6, 14, 13).

The risks associated with trust were not eliminated but reassigned. Paterson stressed that without centralized authority and information, one must trust anonymous users and their "sense of morality to do the right thing" (VIScon, 2020, 35:06–36:06). Given the project's absolute dependency on cell phone operating systems, Apple and Google joined "anonymous users" as necessary objects of social trust. In their April 3 announcement the team wrote, "Since Apple and Google provide the operating system running on mobile devices, *one has to trust them*, since they could potentially learn information related to the proximity tracing system (who is infected, who infected whom, social graphs, etc.)" (Troncoso et al., 2020d, p. 4; emphasis mine). Recognizing that the giants offer no possibility of "exit" or "voice," the dissenters settled on "loyalty" as if it was a choice.

Early on, when the DP-3T first picked up speed in March, senior EPFL administrator Edouard Bugnion made contact with the office of Apple COO Jeff Williams. That led to a series of meetings between members of the DP-3T team and Apple personnel in which they discussed decentralized design and its technical implications (Barraud, 2020; Owen, 2020; VIScon, 2020, 26:03). Recall CEO Tim Cook's 2019 statement, "We are taking what has been with the institution and empowering the individual" (Feiner, 2019, para. 72). Williams is the executive who oversees the translation of this great "taking" into concrete accomplishments, such as the Apple Watch. The DP-3T project

might have impressed him as the apotheosis of Apple's grand strategy. The "decentralization" project had already grabbed the main stage of Europe's COVID-19 debates, largely because of its rebellious narrative featuring the scientists and their trustworthy *system* as digital-age Robin Hoods dedicated to taking from untrustworthy public institutions and empowering individuals. In this narrative, the new Sheriffs of Nottingham were democratic officials, public health authorities and their dastardly servers. Data Scientist I deepened the picture:

> As we undertook the exposure notification project, the working theory was to bypass epidemiology. They wanted to give information directly to individuals and empower people to act on their own behalf. You bypass the public health system in favor of individuals. (DS I)

Showdown. On April 5, 2020, Apple agreed to invest in the DP-3T solution, and in a public announcement on April 10 it joined forces with the other major owner of mobile communications critical digital infrastructure, Google (Apple Newsroom, 2020; Wuerthele, 2020). In a bizarre twist, this move cast both corporations as privacy champions defending Europe from the most comprehensive privacy protections on Earth. Bugnion and Paterson each celebrated their impact on the giants and, through them, the world (Owen, 2020; VIScon, 2020, 25:00–26:41).

The German, French, and other teams still laboring to deliver the PETT-PT application cycled from shock to anxiety over whether their systems would even work with Apple and Google's "decentralized" adaptations. Apple was intransigent, refusing all negotiations with the EU teams. (Abboud et al., 2020; Lomas, 2020a).

The European Commission published a "toolbox" of "essential requirements" for digital tracing applications on April 16, still hopeful that "digital technology ... could contribute to ... containing and reversing" the contagion. The tools were intended to support either "centralized" or "decentralized" designs (European Commission, 2020; Lomas, 2020b). In the same spirit of defusing the conflict, the European Data Protection Supervisor concluded that "data protection rules currently in force in Europe are flexible enough to allow for various measures taken in the fight against pandemics" (Wiewiórowski, 2020, para. 2). But the conflict was not to be so easily resolved. One day later, on April 17, the European Parliament called for coordinated action to combat the pandemic. The members channeled Clinton and Gore's leadership in democratic self-evisceration when they endorsed the "decentralised" approach and insisted, "The generated data are not to be stored in centralised databases." The Parliament stated its "demands that all storage of data be decentralised" (European Parliament, 2020, art. 52).

Ministers from Italy, Spain, Germany, and France decided to team up to convince Apple to adapt its operating system to the member states' needs. "Surely they did not have the temerity to reject the requirements of four sovereign European countries," Public Official II told me. But in the end, the official recounted, "Apple categorically refused our requirements, insisting that only their so-called 'decentralized' structure offered a privacy solution. It was impossible to argue with Apple."

On April 19, 2020, 300 data scientists, primarily from Europe, the United States and the UK, published a joint statement demanding that any COVID-related system design solutions "which allow reconstructing invasive information about the populations should be rejected *without further discussion*" (303 Scientists and Researchers, 2020, p. 1; emphasis mine). This was followed by an open letter to the German government from six civil liberties organizations that criticized the PPET-PT approach. Germany's Chancellor Angela Merkel, unsettled by the criticisms of privacy experts and driven by pragmatic concerns over network effects, cross-border interoperability, and a speedy rollout, abruptly abandoned the four-country effort to win Apple's support. Switzerland and Austria had already committed to Apple and Google. Once Germany

capitulated, Ireland, Italy, Spain, and the other EU member states quickly followed.

Only the French moved forward with their own application, forced to sacrifice interoperability and full alignment with smartphone operating systems and never achieving the uptake they had hoped for (Abboud & Miller, 2020; De Vynck et al., 2020; Hern, 2020b; M. Johnson et al., 2020). France's Minister for Digital Affairs, Cédric O, told Politico, "I don't want to be constrained by the internal policy choices of any company on a matter of public health" (Scott et al., 2020, para. 6). Later, he reflected, "The problem with a centralized protocol is that you have to be confident and to trust your state ... We're in a democratic state, we have checks and balances" (Corbet & Chan, 2020, para. 11). The Norwegians chose a similar path, only to dismantle their system in June, dogged by technical problems and criticism of data overreach and lack of legal safeguards (Singer, 2020). The UK continued to negotiate with Apple to no avail (Hern, 2020a) and by late April NHS officials announced they would move forward without the Apple-Google protocol (Kelion, 2020). By mid-June, technology glitches and criticism from privacy advocates forced the NHS to revert to the Apple-Google system (Warrell et al., 2020).

On the evening of April 22, European Commissioner for the Internal Market, Thierry Breton, held talks with Apple's Tim Cook. With the Commissioner seated at his desk and Mr Cook's face looming larger than life on a massive video monitor, Breton urged Cook "to work constructively with the national authorities so that the tracking apps developed in Europe run on the iPhone" (Purcher, 2020, para. 2). Even this high-level intercession yielded no accommodation from Apple.

Many researchers rejected the privacy advocates' unusually unscientific demand to proceed "without further discussion." Instead, they undertook the system testing and analysis that typically would have preceded a rollout of such significance. Not surprisingly, the new studies revealed a complex case, debunking many of the dissenters' claims (Bradford et al., 2020; Dehaye & Reardon, 2020; Gvili, 2020; Reardon et al., 2020; Vaudenay, 2020).

In a study of SwissCovid, the first Apple-Google Exposure Notification Protocol (ENP) in Europe, two EPFL scientists, Serge Vaudenay and Martin Vuagnoux, observed that Apple and Google had been exempted from Swiss transparency requirements, and Swiss law was left "powerless to protect people from using a non-transparent contact tracing system." The result was the giants' absolute control without accountability. In addition to identifying many privacy weaknesses in the Apple-Google protocol, they noted the political obfuscation in the language of centralization and decentralization. "Arguments against centralized systems have been overly exaggerated, and the ones in favor of decentralized systems have been oversold to a level that we found unethical ... In the former case, trust is based on a democratic system. In the latter case, trust is based on a commercial system." Without the benefits of epidemiological data for Swiss health authorities, Vaudenay and Vuagnoux (2022) questioned "whether SwissCovid is useful at all." They asked if it should be "shut down," and concluded, "Citizens have no longer anything to say about it except taking it as a whole or refusing it. This is a major loss of government's digital sovereignty" (sec. 2, para. 4; sec. 3, para. 5–6; see also, Crețu et al., 2022; Ng, 2021; Singer, 2020).

Apple-Google Contribute to US Failures. The Apple-Google US rollout was even more chaotic. Unlike Europe, the United States entered the pandemic era with record-low trust in government institutions. The Trump administration intensified these conditions, boasting of plans for high-tech COVID surveillance while actively demeaning US public health professionals, health institutions, and state officials. COVID-related disinformation, much of it originating with then President Trump, further battered institutional trust (Evanega et al., 2020). In many communities, these conditions undermined contact tracing and responsible epidemiological information gathering (Raskin, 2020).

The Apple-Google juggernaut exacerbated these problems. As in Europe, US public health authorities found themselves pleading unsuccessfully with Apple for a more flexible design. By June 2020, only three states had committed to using the Apple-Google technology. The rest either remained uncertain or decided to pursue manual contact tracing and follow-up (Barry, 2020; Holmes & Langley, 2020; Yan, 2020). By July, a global analysis would ask, "What ever happened to digital contract tracing?" (Kissick et al., 2020).

One year later, a study by the US General Accounting Office (GAO) found that only 26 of 56 US states and territories had deployed the Apple-Google app, with download levels ranging from 200,000 to 2 million. Worse still, only a small fraction of the people who downloaded the app actually used it. Of six states where the GAO collected systematic data, the number of times that app users received exposure notifications ranged from a high of 31,000 and 42,000 respectively in two states, to a low of 900 to 3800 in the other four. The report concluded: "We found limited evidence that exposure notification apps are effective at enhancing the speed or reach of manual contact tracing or at reducing the spread of disease" (US Accountability Office, 2021, p. 33; see also, De Vynck & Zakrzewski, 2021). The ENP's "decentralization" secured the app as a black box. State health officials could not measure its effectiveness because there were no data to do so, and they could not improve its effectiveness because they had no measurements (US Accountability Office, 2021, pp. 34–35).

Here too the revenge of the void played a key role. On one side, US lawmakers had left citizens almost entirely unprotected from government and corporations. On the other, Americans harbored a growing sense of outrage toward the tech giants' relentless extraction and targeting. A stream of US survey data shows a complete rupture of faith in the tech companies among decisive majorities (Accountable Tech & GQR, 2021; Future of Tech Commission, 2021; Knight Foundation, 2020).

The GAO cites this "lack of trust" as the major obstacle to Americans' adoption of the Apple-Google ENP and the apps built upon it: "Mistrust of governmental health authorities and technology companies can lead people to forgo using apps ... The public may lack confidence that its privacy is being protected, in part, due to ... a lack of federal legal protections" (US Accountability Office, 2021, pp. 28, 31).

Apple-Google did not create but rather expertly exploited the rapidly escalating sense of vulnerability and disorientation engulfing whole populations. These conditions enabled them to intervene in the relationship between individuals, their societies, and governments.

The Governance Vector: The Governance of Governance

As pandemic death tolls mounted, the companies' steadfast intransigence suggests that saving lives was never their primary goal. Indeed, if their aim was to fight the pandemic effectively, then their efforts were a categorical failure. The victory Apple-Google scored is better understood in terms of the developmental urge toward systemic dominance, which now aims the great "taking" of the Robin Hood illusion at the democratic order itself. The governance threat draws on the giants' absolute control over the information and communication spaces gifted to them by the very democracies to which they laid siege. In this case, their avatars on the invisible battlefield are mobile operating systems. Disruption targets are the working elements of democratic institutions, including elected and appointed officials, their authority and power, roles, responsibilities, purpose, and public mandate. The spoils of war are measured in opportunities to alienate individuals from society, its political institutions and leaders, turning them instead toward *the system* and the propaganda that conceals its facts of private control and genuinely centralized unaccountable power.

The data scientists I interviewed each emphasized the corporations' governance

ambitions and the economies of domination upon which they depend. "*This was always a governance play*," Data Scientist I told me. "Everyone knew it, and everyone was on board with that. If they weren't, it would have been hard to speak up."

Data Scientist II explained critical digital infrastructure control as key to economies of domination. "The companies configure the operating system (OS) any way they want. They can make this protocol privacy-preserving, just as they can update the OS to make data available to them. This is the larger truth: They can do this for any data on your phone, email, messages, photos ... The owner of the OS is the Emperor, because there is no regulation that makes it illegal. You see this in the nonnegotiable requirements they set for public health apps in every country."

Half a world away, the European public officials with whom I spoke felt the effects of the "governance play" and its economies of domination, just as intended. Public Official III spontaneously described the situation as "sad ... and grotesque," adding, "This means that even in the face of so much death and disease these companies currently have the power to constrain the choices of democratically elected sovereign states. They are the gatekeepers of society."

Public Official II echoed this analysis:

> Apple can refuse to negotiate with officials of democratic governments because they are the sole gatekeeper of the iOS ... While we struggle with the notion of how to structure the platforms, the platforms are structuring our democracies. Under these conditions, what is the relevance of public power? If we are not strong enough to apply our own laws in the real world to the internet, then what is the use of the state?

From the point of view of institutional development, the governance of governance is the next necessary achievement required to protect, nourish, reproduce, and extend already conquered terrain. The possibilities of democratic contradiction are difficult to predict. More predictable is that in the absence of such contradiction, the surveillance capitalist order is likely to develop more extensive governance powers that further dissolve the distinctions between economic, political and social power in much the same way that it eliminates boundaries between sectors now reborn as information science. The words of John Donne should echo in the thoughts of every citizen and lawmaker, elected and appointed official, secretary, minister, president, prime minister and civil servant:

> Therefore, send not to know
> For whom the bell tolls,
> It tolls for thee.

The Social Harm Vector: The Desocialization of Society

The DP-3T data scientists framed "decentralization" versus "centralization" as proxies for a new contest between individuals and social solidarity. Apple and Google, sphinxlike, exploited this ideological opportunity to present themselves with mind-boggling audacity as guarantors of individual privacy, while they "take from the institution" of democracy.

In the development of systemic dominance, the taking is no longer confined to data, knowledge, or even the raw power of behavioral modification. Here the taking extends to the living bonds of trust. Society is sacrificed for the sake of individuals, this story goes, as rhetoric and action aim to transfer trust from society to "the system."

As one public official told me:

> The real problem is the decline of trust in the state. This is partially self-inflicted, but heightened and exploited by the tech companies, their false rhetoric, and their disinterest or inability to curb disinformation ... In a democracy you can effect change. You can fight authoritarianism. But with Apple, you can't change anything. It's a single massive highly centralized corporation with absolute power. So, what will remain for the people? Only the "user experience" remains. (PO I)

What is the user experience that Apple and Google's systemic dominance imposes? Trust without hope of verification. Taxation, paid in the sacrifice of society, without hope of representation. In this shadowscape, any violation of privacy is anyway invisible, unknowable, and without hope of redress. All that is sacrificed for this empty promise of empowerment is gambled on an inscrutable operating system owned and operated by vast empires and their silent emperors. The known unknown is a tweak of the OS today, and a different tweak tomorrow.

Goodbye, network. In this shadow world, economies of domination employ radical connection, now paradoxically centralized as hub and spoke, center, and node. All nodes are anonymous to all other nodes, each a single nameless atom drifting through an obscurity where everything is suspect. Connection to "the system" produces the isolation that nourishes absolute power. This isolation is mistaken for privacy. Society, or what is left of it, is only tolerable to the extent that it is drained of the social. It is not difficult to imagine the long-game calculation of a new era that begins with systemic dominance and eventually, quietly, engineers the transformation to computational governance in the name of more efficiency, less conflict, and frictionless economies of domination.

Like Clay Christensen, the senior statesmen of the surveillance capitalist institutional order and its disciplines of "disruption" do not cry for the open societies of liberal democracy. For example, in April 2020, as the Apple-Google showdown in Europe unfolded, former Google executive and all-around tech alpha Eric Schmidt was interviewed on stage at the Economic Club of New York. Speaking about the effects of the pandemic on Big Tech, the moderator posited, "We talked a lot about surveillance capitalism before this crisis, but now it seems that tracking is one of the very important elements in dealing with this" (Schmidt & Kravis, 2020, p. 7).

Schmidt's response conveys his admiration for the "simplicity" and effectiveness of authoritarian governments like China. Unencumbered by democracy, he finds them better suited to meet the crisis of the pandemic and all potential crises:

> So if you look at the state of the art in the countries that have done this well ... they've all been countries with simpler governmental systems. Ours is too complicated. We can't even decide if the President can shut down the states ... We can't decide if it's the New York Mayor or the New York Governor, who gets to decide what's going on in the schools. And because you have a problem of decision making within our country, you get confusion which leads to delay which leads to lack of action. (Schmidt & Kravis, 2020, pp. 7–8).

Schmidt has no patience for the substance of the democratic process and yearns instead for a desocialized society. All the implications of "taxation *with* representation"– voice, participation, open discussion, conflict, rights to be claimed, enacted, and protected– mean that democracy is messy, frustrating and fitful. At its best, the principles that attend to the rule of law in a liberal democracy slow things down and open things up. There is no supreme decider, no Apple or Google to tweak the OS this way or that. This slowness and mess are what protect us and ensure that democracy endures despite its perennial challenges and failures.

Economies of domination obscure the central insight upon which the very idea of democracy stands: only society can guarantee individual rights. Only a democratic society can guarantee the rights that enable self-governance to endure and sometimes to flourish, beginning with Hannah Arendt's "right to have rights" (Arendt, 2004, pp. 369–384; Ingram, 2008).

Arendt observes the Nazi machinery that first deprived Jews and other unwanted humans of their legal status as the precondition for depriving them of their humanity and then their lives. The loss of legal existence meant absolute exclusion from "the world of the living," forced into ghettos and concentration camps. She writes:

> The point is, a condition of complete rightlessness was created before the right to live was challenged ... Not the specific rights, then, but the loss of a community willing and able to guarantee any rights whatsoever, has been the calamity which has befallen ever-increasing numbers of people ... Only the loss of a polity itself expels Man [sic] from humanity. (Arendt, 2004, pp. 375, 377).

As in the case of epistemic rights discussed earlier, the existential primacy of the right to have rights is only discovered at the moment in history when it is threatened. "We became aware of the existence of a right to have rights ... and a right to belong to some kind of organized community, only when millions of people emerged who had lost and could not regain these rights" (Arendt, 2004, p. 376).

The implications of Arendt's insight should rivet our attention on the existential threat of the desocialized society into which we are propelled by surveillance capitalism. Under such conditions, rights can neither be granted nor defended. "*The system*" that was elevated above democratic society and institutions by the DP-3T data scientists cannot grant the right to have rights nor the juridical rights that are the privilege of that most basic condition of the social. There are no rights of any kind in a desocialized society because all rights issue from society. The rest is gift, as easily rescinded as given. Returning one last time to Durkheim and the conclusion to his first great opus: "Society is not, then, as has often been thought, a stranger to the moral world ... It is, on the contrary, the necessary condition of its existence" (Durkheim, 1964, p. 399).

Conclusion: The Golden Sword

Surveillance capitalism is what happened when US democracy stood down. It was always a windfall, born of an antidemocratic economic ideology and gifted by democracy-negating democratic leaders. It was always the covert quid pro quo of a fearful democratic state more inclined to control the future from the top down than to build it with trust from the bottom up. Two decades later, surveillance capitalism has failed any reasonable test of responsible global stewardship of digital information and communications.

The abdication of these information and communication spaces to surveillance capitalism has become the meta-crisis of every republic because it obstructs solutions to all other crises. It is astonishing to consider that our emergent information civilization is wholly dependent upon these "spaces," yet they remain for sale or rent by any individual, corporation, politician, billionaire, megalomaniac, or billionaire megalomaniac, with no law to constrain their action, unlike almost any other form of property. The people are left to observe, shout, or cower on the sidelines, bystanders to their own pillage and its consequences in the uniquely abstract forms of subjugation described in these pages.

While the liberal democracies have begun to engage with the challenges of regulating today's privately owned information spaces, the sober truth is that the regulation of institutionalized processes that are innately catastrophic for democracy cannot produce desired outcomes.

Our societies have faced other institutions that imposed catastrophic consequences on people and society, such as human slavery and child labor. It was understood eventually that there is no bargaining with that which is categorically catastrophic, and movements arose to abolish those institutions. In today's death match of institutional orders, the challenge again shifts from regulation to abolition as the only realistic path to reinvention.

The democratic order will not survive the contest over the politics of knowledge unless there is a reckoning with fundamental questions, starting with this: How do we organize and govern the global information and communication infrastructures of an information civilization in ways that sustain and advance democratic values, principles, aspirations, and governance? What institutions, rights, and laws are required for responsible stewardship and a free and flourishing information civilization?

The unified field analysis reveals the conflict that underlies this meta-crisis. The commodification of human behavior is the foundation of surveillance capitalism's two-decade developmental arc expressed in its rapidly evolving complexity and institutional power over four already visible stages of development. We have seen that each stage is characterized by novel economic operations, governance takeovers, and social harms. Later-stage phenomena are effects of the foundational capabilities required for commodification of the human. The operations and harms at each developmental stage are, both individually and in aggregate, categorically incompatible with democratic society. It bears repeating that this conflict produces the zero-sum dynamic in which the deepening order of surveillance capitalism propagates democratic disorder and deinstitutionalization.

The unified field analysis suggests that democratic stewardship and reinvention require contradiction strategies that first freeze surveillance capitalism's institutional development, then inhibit its reproduction and shift the global trajectory from dystopia to hope. The results must include surveillance capitalism's deinstitutionalization, but they should also clear the way for the birth of new institutional forms that draw people, law, ideas, capital, technologies, and capabilities into democracy's house. This means new zones of public governance aligned with the values, principles and aspirations of democratic societies and empowered to hold accountable both market and state to the rule of public law.

The mission here recalls Hercules' death match with the Hydra of legend and its eight monstrous heads, each able to attack swiftly from every direction. As soon as Hercules brought down his club on one head, another sprouted in its place. Eventually he perceived the ninth "Immortal Head," obscured and protected by the others. He realized that slaying the beast required hacking his way past the Hydra's most visible action to reach its hidden source of power. Hercules severed the Immortal Head with the Golden Sword, given to him by Athena for that unique purpose. The fable endures because of what it teaches: with a clear grasp of an opponent's source of power and a fit-for-purpose weapon, it is possible to succeed against a ferocious enemy that even gods believe invincible.

If the commodification of human behavior is both the foundation of surveillance capitalism and incompatible with democracy, then surveillance capitalism's hidden source of power–its Immortal Head–is the secret massive-scale extraction of human-generated data. Secret extraction operationalizes behavior commodification and turns it toward prediction, profit, and concentrations of economic, governance and social powers. It follows, then, that the *lawful abolition* of secret massive-scale extraction is democracy's Golden Sword that can interrupt the power source upon which all surveillance capitalism's destructive economic operations, governance takeovers, and social harms depend.

The abolition of the primary human extraction that I have called theft is thus the single most effective strategy of democratic contradiction. It is the most likely to inaugurate a new chapter of institutional invention drawn from all the brilliance now clamoring at the gates held shut by the surveillance dividend. Abolition of these already illegitimate operations means no annexation of epistemic rights, no wholesale destruction of privacy, and no industrialized tons of behavioral signals flowing through the blind-by-design systems required to accommodate their scale and speed. Abolition eliminates the structural causes of epistemic chaos associated with the commodification of the human. It means no antidemocratic concentrations of knowledge about people, extreme epistemic inequality, or powerful microtargeting algorithms. The absence of massive-scale extraction enhances cybersecurity by reducing the data-rich attack surface of individuals, groups, and societies, substantially eliminating vulnerabilities to remote actuation, illicit behavioral governance, the fusion of state and market powers, and the artificial construction of the public square. The abolition of extraction resets the capabilities of computational behavioral prediction and its human futures markets, eradicating

the financial incentives for surveillance capitalism, summarized as the surveillance dividend, that fund its bid for systemic dominance, governance hegemony, and the desocialized mediation of society by proprietary systems controlled by absolute instrumentarian power.

Today's discussions of content moderation and other active measures are hopeless a priori because they willfuly ignore the scale and complexity of blind-by-design information flows, while naively insisting that the giants should voluntarily handicap themselves in the death match. Doomed from the start because action is weaker than institutionalization, these contradiction strategies inadvertently create the conditions for a cynical theater of self-regulation, deflecting the emergence of genuinely effective contradiction strategies.

Active measures directed at what is most visible, such as content moderation in all its forms, including labeling, warning, fact checking, slowdowns, takedowns, or suspensions, are each post-catastrophe, and therefore no match for the reproductive mechanisms identified in this discussion. These include automaticity and the systemic principles of blindness by design; democratic self-evisceration and the sustained absence of effective law; concealment and engineering for user ignorance; the surveillance dividend and the investment capabilities it both attracts and enables; concentrations of epistemic rights and the privacy they afford; Orwellian rhetorics of inevitability, misdirection, and disorientation; unprecedented concentrations of human data, knowledge, artificial intelligence capabilities, the epistemic inequality they produce, and the remote actuation they enable; new forms of political appeasement, declaration, colonization, and performative legitimacy; and, above all, the aura of inevitability emitted by this rogues' gallery of self-reproduction. The abolition of secret extraction would land a decisive blow on each of these mechanisms and cripple institutional reproduction as currently construed.

The abolition of secret massive-scale extraction is also a more effective form of contradiction than post-factum active measures because it is content-neutral and does not threaten genuine freedom of expression. Instead, abolition liberates social discourse and information flows from the unnatural selection of profiteering commercial operations that breed digital violence by artificially interceding to favor lucrative information corruption over integrity. The abolition of secret extraction can produce the conditions in which genuine freedom of expression, social solidarity, common sense, and the integrity of social communications are restored. Deprived of algorithmic oxygen, digital violence slithers back into the shadows at the fringe.

Yes, the abolition of secret extraction of the human promises systemic change, but there is something more here, more subtle and more powerful. Responsible democratic stewardship is drawn into being as the democratic order *stands up* to surveillance capitalism's antidemocratic counterrevolution–a Hercules for a new time. This standing up is a dedicated effort of comprehension and confrontation that speaks to every people's yearning to escape the gravitational pull of the accidental dystopia toward which we hurtle.

The work of standing up is already in motion, evidenced by recent expressions of democratic contradiction that were unimaginable only a few years ago. As this power builds, the abolition of secret massive-scale extraction, once a distant thought experiment, can and should become the subject of urgent discussion. In the dialectic of the death match, abolition draws closer to inevitability as the threats to democratic societies escalate.

Highlights of this new wave include the European Union's game-changing legislative developments. In 2022 the European Parliament's historic passage of the Digital Services Act and the Digital Markets Act broke the sound barrier of surveillance capitalism's aura of inevitability and began the work of asserting democratic governance over the tech giants and their ecosystems. The EU's proposed regulatory regime for artificial intelligence and the European Declaration on Digital Rights and Principles for the Digital Decade are powerful

new expressions of democratic contradiction that, in concert with the new legislative Acts, create the conditions for the next step function leap forward in genuinely effective contradiction: the abolition of primary extraction and its redefinition as theft (European Commission, 2022a, 2022b; European Parliament, 2022).

The global operations of human data extraction are already contested among a vanguard of lawmakers and policymakers both in the EU and the United States who have rallied to the prospect of outlawing surveillance advertising (Bryant, 2021; European Parliament, 2021; Kaye, 2021). In Europe, civil society institutions delivered their "People's Declaration" to the EU Parliament demanding an end to surveillance advertising (*The People's Declaration*, n.d.). In the United States, Accountable Tech, a civil society institution focused on the nexus of technology and democracy, submitted a petition to the US Federal Trade Commission for rulemaking that would prohibit surveillance advertising ("Accountable Tech Petitions FTC to Ban Surveillance Advertising as an 'Unfair Method of Competition' (Press Release)," 2021). Significant legislation to ban surveillance advertising and microtargeting in political advertising has been introduced in the US Congress (Davis, 2021; Eshoo, 2020, 2022), followed by historic data protection and antitrust bills in the US House and Senate (Competition and Antitrust Law Enforcement Reform Act, 2021; American Data Privacy and Protection Act, 2022).

Meanwhile, the public conversation is moving fast. In 2022, the Nobel Peace Prize Committee, led by its 2021 recipients, journalists Maria Ressa and Dmitry Muratov, published "A 10-Point Plan to Address Our Information Crisis" beginning with its demand to "Bring an end to the surveillance-for-profit business model."

> The vast machinery of corporate surveillance not only abuses our right to privacy, but allows our data to be used against us, undermining our freedoms and enabling discrimination. This unethical business model must be reined in globally, including by bringing an end to surveillance advertising that people never asked for and of which they are often unaware. (Ressa & Muratov, 2022)

In 2022, the US Federal Trade Commission solicited public comment on the prospect of "Commercial Surveillance and Data Security Rulemaking" (Federal Trade Commission, 2022). This too may augur a watershed.

These and other current expressions of democratic contradiction have the potential to ground the next critical phase of institutional reinvention. After two decades of Cook's and Kalanick's and Christensen's and Schmidt's veneration of institutional destruction, the unified field analysis suggests a different lesson. I call it Zuboff's Fourth Law: *Information is only as useful to society as the institutions, rights, and laws that govern its production and use.*[7] This is the reckoning we face, swept up in a new civilization where digital information and communications systems are owned and controlled by an economic institution that can neither value nor detect truth.

We struggle in this milieu of desocialized connection without institutional capabilities developed to failsafe rather than exploit the distance between sentience and world, a fissure that in other eras was healed by varied institutionalizations of "truth," "trust," "witness," "accountability," "responsibility," "fact," "fidelity," and "meaning." In some cases, these capabilities have been actively damaged or weakened, as in the destruction of the news industry and the democratic role of the Fourth Estate. In other cases, such capabilities, and the institutions to enact them, have not yet been developed, as illustrated in the many varieties of epistemic rights violations from location-data trafficking to the international shipping crisis of fake GPS coordinates that facilitates criminality at sea (Kurmanaev, 2022). New rights that are essential but still uncodified are mirrored by new and still nameless crimes.

The abolition of secret human extraction is a critical bridge to the reckoning with reinvention.

For example, the giants' domination of artificial intelligence and its global market structure wholly depends upon their oligopolistic advantages in the secret massive-scale extraction of human data. This dominance, as we have seen, translates into global control over knowledge production and consumption. In contrast, the abolition of secret extraction would reverse the antidemocratic capture of the division of learning that elevates the few over the many–surveillance capitalism's institutional interests over those of all people. It would tip the scales in the death match over the politics of knowledge, clearing the path for computational knowledge production that advances humanity in millions of new ways while tethered to the expansion and protection of democracy's house and its inhabitants. It frees us to begin again in the spaces sold cheap by Clinton and Gore in 1997 and sold again in 2001. We begin again and reclaim the void, finally knowing what we have lost and what is at stake.

This paper concludes on the first page of a new chapter. History is a relay race, not a sprint. The baton passes to the democratic order, not as an ideal but as lived reality, because each citizen bears responsibility for mobilization, transformation, and stewardship. It passes to a new generation of students, artists and scholars charged with the urgent demand for creative thought and vision that pulls us back from the brink of dystopia and illuminates a new direction. It passes to journalists, now under siege, but critical to the reinvention of a Fourth Estate for our information civilization. It passes to citizens and lawmakers, bent on clawing back the future. It passes to all who reject dystopia and unaccountable power.

Democracy is not a condition to be taken lightly, discarded from impatience or inconvenience. Too many have sacrificed for the sake of it. Too many have perished for the lack of it. It is not programmable. It is under siege, because at its best, democracy negates absolute power and remains a dangerous obstacle to ambitions of systemic dominance, including those nursed by a new information oligarchy sozzled on computation. Without democracy, as Wendy Brown writes, "we lose the language and frame by which we are accountable to the present and entitled to make our own future, the language and frame with which we might contest the forces otherwise claiming that future" (W. Brown, 2015, p. 210).

Hold tight to this promise in the zero-sum clash of institutional orders and a still indeterminate fate.

Declaration of conflicting interests

The author declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author received no financial support for the research, authorship, and/or publication of this article.

Note on Method

A note on my source materials: In this paper I occasionally draw upon a series of six extended interviews conducted in the months following the Apple-Google intervention in the EU. Among the six, two interviewees were seasoned Silicon Valley data scientists each employed by one of the two companies. Each had worked on various aspects of the design and launch of the Apple-Google Exposure Notification Protocol. Each was already known to me from prior interviews. I refer to them below as Data Scientist I and Data Scientist II (DSI, DSII). The other four interviewees were high-ranking public officials either in EU member states or the European Commission. I refer to these interviewees below as Public Official I, II, III, or IV (PO I-IV). Each of the four was directly involved in emergency decision-making during the course of the events described here.

The six interviewees each agreed to two extensive interview sessions, providing background and specific insights. On the promise of anonymity, each granted permission for their comments to be used at my discretion in future writing. No interviewee had knowledge of the other individuals with whom I spoke.

Most striking to me after so many decades of field interviews was the concurrence of perspectives across these many different roles and vantage points. Instead of the usual "blind man and the elephant," their unique insider experience led all six to similar conclusions, especially as regards the larger significance of the Apple-Google intervention. I include their reflections here when they offer a useful means of triangulating, contextualizing, or deepening this discussion.

Notes

1. You instruct ads not to track you, but they persist—even on an iPhone (Fowler, 2021). There's a US$16bn market for your location data (*Location Intelligence Market Size & Share Report, 2022–2030*, 2022). Cyber-mercenaries are the rage; most of their data is scraped from the giants (Bradshaw et al., 2021). Surveillance cameras are about to become truly cheap and ubiquitous, and anyone with the Bosch app can install, operate, and analyze the video data (Campbell & Jones, 2022). A "smart" light bulb tracks your heart rate (Tuohy, 2022). The new TV watches you (Fowler, 2019c). "Alexa" and all the other "assistants" retain all recordings to feed their artificial intelligence (Fowler, 2019a; Suliman, 2022). Facebook is developing brain-reading tech (Samuel, 2019). "Student Surveillance Services" "keep kids safe" by monitoring everything from biometrics to chats (Haskins, 2019). Cars are surveillance platforms (M. Anderson, 2019). General Motors has launched "behavior-based" driver insurance, with monitoring systems that track eye and head movements, and more (Bellon, 2022). Google's Chrome browser operates as surveillance software (Fowler, 2019b). The "Ring Doorbell" sees it all (Grauer, 2022). Your face travels from that graduation photo, posted in gratitude and hope, to train Chinese facial recognition systems that stand watch over Uighur families in concentration camps (Murgia, 2019b) ...
2. "Knowledge in this sense is more than what is usually described as skill, and the division of knowledge of which we here speak more than is meant by the division of labor. To put it shortly, 'skill' refers only to the knowledge of which a person makes use in his trade, while the further knowledge about which we must know something in order to be able to say anything about the processes in society is the knowledge of alternative possibilities of action of which he makes no direct use. It may be added that knowledge, in the sense in which the term is here used, is identical with foresight only in the sense in which all knowledge is capacity to predict" (Hayek, 1980, p. 273).
3. For relevant commentary and insights see W. Brown, 2015; Mirowski, 2013; Wacquant, 2012.
4. "First they came for the Socialists, and I did not speak out—Because I was not a Socialist.
   Then they came for the Trade Unionists, and I did not speak out—Because I was not a Trade Unionist.
   Then they came for the Jews, and I did not speak out—Because I was not a Jew.
   Then they came for me—and there was no one left to speak for me." (Niemöller, 1950)
5. Alphabet/Google endeavored to develop a "Google City" on the Toronto waterfront, including its own forms of governance (Cardoso & O'Kane, 2019; Goodman & Powles, 2019). In 2021 Facebook blacked out its pages in Australia rather than negotiate with Parliament over a new legislative code that would require remunerating publishers for news content (Easton, 2021; Smyth et al., 2021; Smyth, 2021b). Whistleblower documents later revealed the takedown as a highly orchestrated extortion operation planned over seven months, overseen by Zuckerberg and Sandberg, and aimed at the Australian people and their government (K. Horwitz et al., 2022; Reset Australia, 2022; Smyth, 2021a; Whistleblower Aid, 2022). Facebook established an "Oversight Board" in 2020, a private governance body that aimed to protect principles of industry self-regulation (Klonick, 2020; Lapowsky, 2020; Lewin, 2021; M. Roberts, 2019).
6. The Swiss Federal Institute of Technology in Zürich.
7. Zuboff's Fourth Law is a corollary of *Zuboff's Three Laws*. Formulated in the mid-1990s and grounded in 20 years of clinical observations of "workplace computerization," the three laws summarized and predicted behavior in the economic domain. *Zuboff's Three Laws: Assuming the dominant economic paradigm, (1) everything that can be automated will be automated; (2) everything that can be informated will be informated; (3) all digitally produced data that can be used for surveillance and control will be used for surveillance and control in the absence of countervailing rights, laws, contracts, rules, or sanctions* (Zuboff, 2013, sec. 3).

References

303 Scientists and Researchers. (2020). *Joint Statement on Contact Tracing*. https://drive.google.com/file/d/1OQg2dxPu-x-RZzETlpV-3lFa259Nrpk1J/view

Abboud, L., & Miller, J. (2020, June 23). French give cool reception to Covid-19 contact-tracing app. *Financial Times*. https://www.ft.com/content/255567d5-b7ec-4fbe-b8a9-833b3a23f665

Abboud, L., Miller, J., & Espinoza, J. (2020, May 10). How Europe splintered over contact tracing apps. *Financial Times*. https://www.ft.com/content/7416269b-0477-4a29-815d-7e4ee8100c10

Abrams et al. v. United States, 250 U.S. 616 (1919). https://www.law.cornell.edu/supremecourt/text/250/616

Accountable Tech & GQR. (2021). *America's Views on Surveillance Advertising*. Accountable Tech. https://accountabletech.org/research/surveillance-advertising/

Accountable Tech Petitions FTC to Ban Surveillance Advertising as an 'Unfair Method of Competition' (Press Release). (2021, September 28). *Accountable Tech*. https://accountabletech.org/media/accountable-tech-petitions-ftc-to-ban-surveillance-advertising-as-an-unfair-method-of-competition/

Acemoglu, D. (2021). *Harms of AI* (Working Paper No. 29247; Working Paper Series). National Bureau of Economic Research. https://doi.org/10.3386/w29247

Acemoglu, D., & Restrepo, P. (2021). *Tasks, Automation, and the Rise in US Wage Inequality* (Working Paper No. 28920; Working Paper Series). National Bureau of Economic Research. https://doi.org/10.3386/w28920

Agbehadji, I. E., Awuzie, B. O., Ngowi, A. B., & Millham, R. C. (2020). Review of Big Data Analytics, Artificial Intelligence and Nature-Inspired Computing Models towards Accurate Detection of COVID-19 Pandemic Cases and Contact Tracing. *International Journal of Environmental Research and Public Health*, *17*(15), 5330. https://doi.org/10.3390/ijerph17155330

Ahmad, N., & Salvadori, K. (2020, May 13). Building a transformative subsea cable to better connect Africa. *Engineering at Meta*. https://engineering.fb.com/2020/05/13/connectivity/2africa/

Aiello, A. E., Renson, A., & Zivich, P. (2020). Social media- and internet-based disease surveillance for public health. *Annual Review of Public Health*, *41*, 101–118. https://doi.org/10.1146/annurev-publhealth-040119-094402

Akinwotu, E. (2021, October 7). Facebook's role in Myanmar and Ethiopia under new scrutiny. *The Guardian*. https://www.theguardian.com/technology/2021/oct/07/facebooks-role-in-myanmar-and-ethiopia-under-new-scrutiny

Alegre, S. (2022). *Freedom to Think: The Long Struggle to Liberate Our Minds*. Limited Atlantic Books.

Alizada, N., Cole, R., Gastaldi, L., Grahn, S., Hellmeier, S., Kolvani, P., Lachapelle, J., Lührmann, A., Maerz, S. F., Pillai, S., & Lindberg, S. I. (2021). *Autocratization Turns Viral: Democracy Report 2021*. V-Dem Institute. https://www.v-dem.net/static/website/files/dr/dr_2021.pdf

Allam, H. (2020, December 15). Right-Wing Embrace Of Conspiracy Is "Mass Radicalization," Experts Warn. *NPR*. https://www.npr.org/2020/12/15/946381523/right-wing-embrace-of-conspiracy-is-mass-radicalization-experts-warn

Allcott, H., & Gentzkow, M. (2017). Social Media and Fake News in the 2016 Election. *Journal of Economic Perspectives*, *31*(2), 211–235.

Allen, A. L., & Rotenberg, M. (2016). *Privacy Law and Society* (3rd ed.). West Academic Publishing.

Allington, D., Duffy, B., Wessely, S., Dhavan, N., & Rubin, J. (2021). Health-protective behaviour, social media usage and conspiracy belief during the COVID-19 public health emergency. *Psychological Medicine*, *51*(10), 1763–1769. https://doi.org/10.1017/S003329172000224X

Amazon. (2022, July 21). *Amazon and One Medical Sign an Agreement for Amazon to Acquire One Medical*. Amazon Press Center. https://press.aboutamazon.com/news-releases/news-release-details/amazon-and-one-medical-sign-agreement-amazon-acquire-one-medical/

Amazon Web Services. (2019, August 12). Amazon Rekognition improves Face Analysis. *Amazon Web Services, Inc*. https://aws.amazon.com/about-aws/whats-new/2019/08/amazon-rekognition-improves-face-analysis/

American Data Privacy and Protection Act. (2022). H.R.8152, United States House of Representatives, 117. http://www.congress.gov/

Amnesty International. (2020, April 3). COVID-19, digital surveillance and the threat to your rights. *Amnesty International*. https://www.amnesty.org/en/latest/news/2020/04/covid-19-surveillance-threat-to-your-rights/

Anderson, J., & Rainie, L. (2020, February 21). Many Tech Experts Say Digital Disruption Will Hurt Democracy. *Pew Research Center*. https://www.pewresearch.org/internet/2020/02/21/many-tech-experts-say-digital-disruption-will-hurt-democracy/

Anderson, M. (2019, June 24). The Self-Driving Car Is a Surveillance Tool. *IEEE Spectrum*. https://spectrum.ieee.org/surveillance-and-the-selfdriving-car

Apple Newsroom. (2020, April 10). *Apple and Google partner on COVID-19 contact tracing technology*. Apple Newsroom. https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/

Archer, K., & Levey, I. R. (2020, March 20). Trust in Government Lacking on COVID-19's Frontlines. *Gallup Blog*. https://news.gallup.com/opinion/gallup/296594/trust-government-lacking-frontlines-covid.aspx

Arendt, H. (2004). *The Origins of Totalitarianism*. Schocken.

Atlantic Council. (2021). *Atlantic Council's DFRLab publishes new report in Just Security: #StopTheSteal: A timeline of social media and extremist activities leading up to 1/6 insurrection*. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/report/atlantic-councils-dfrlab-publishes-new-report-in-just-security-stopthesteal-a-timeline-of-social-media-and-extremist-activities-leading-up-to-1-6-insurrection/

Avaaz. (2020). *Facebook's Algorithm: A Major Threat to Public Health*. Avaaz. https://secure.avaaz.org/campaign/en/facebook_threat_health/

Bak-Coleman, J. B., Alfano, M., Barfuss, W., Bergstrom, C. T., Centeno, M. A., Couzin, I. D., Donges, J. F., Galesic, M., Gersick, A. S., Jacquet, J., Kao, A. B., Moran, R. E., Romanczuk, P., Rubenstein, D. I., Tombak, K. J., Bavel, J. J. V., & Weber, E. U. (2021). Stewardship of global collective behavior. *Proceedings of the National Academy of Sciences*, *118*(27). https://doi.org/10.1073/pnas.2025764118

Balkin, J. (2008). The Constitution in the National Surveillance State. *Minnesota Law Review*, *93*(1). https://openyls.law.yale.edu/handle/20.500.13051/1545

Balkin, J. M. (2017). *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation* (SSRN Scholarly Paper No. 3038939). https://doi.org/10.2139/ssrn.3038939

Banco, E., & Ackerman, S. (2020, April 21). Team Trump Turns to Peter Thiel's Palantir to Track Virus. *The Daily Beast*. https://www.thedailybeast.com/trump-administration-turns-to-peter-thiels-palantir-to-track-coronavirus

Barraud, E. (2020, May 25). First pilot for the Google and Apple-based decentralised tracing app. *EPFL News*. https://actu.epfl.ch/news/first-pilot-for-the-google-and-apple-based-decentr/

Barry, E. (2020, April 16). An Army of Virus Tracers Takes Shape in Massachusetts. *The New York Times*. https://www.nytimes.com/2020/04/16/us/coronavirus-massachusetts-contact-tracing.html

Bass, D., & Brustein, J. (2020, March 16). Big Tech Swallows Most of the Hot AI Startups. *Bloomberg.Com*. https://www.bloomberg.com/news/articles/2020-03-16/big-tech-swallows-most-of-the-hot-ai-startups

Bay, J. (2020, April 14). *Automated contact tracing is not a coronavirus panacea*. Medium. https://web.archive.org/web/20200419012441/https:/blog.gds-gov.tech/automated-contact-tracing-is-not-a-coronavirus-panacea-57fb3ce61d98?gi=89919a6fa2e

Bellon, T. (2022, January 24). GM set to launch behavior-based U.S. driver insurance in Q1—Executive. *Reuters*. https://www.reuters.com/business/autos-transportation/gm-set-launch-behavior-based-us-driver-insurance-q1-executive-2022-01-24/

Benesch, S. (2021, October 30). Nobody Can See Into Facebook. *The Atlantic*. https://www.theatlantic.com/ideas/archive/2021/10/facebook-oversight-data-independent-research/620557/

Berger, P. L., & Luckmann, T. (1966). *The Social Construction of Reality: A Treatise in the Sociology of Knowledge*. Random House.

Bharat, K., Lawrence, S., & Sahami, M. (2016). *Generating user information for use in targeted advertising* (United States Patent No.

US9235849B2). https://patents.google.com/patent/US9235849/en

Bhattacharyya, S. (2022, January 24). Meta Unveils New AI Supercomputer. *Wall Street Journal*. https://www.wsj.com/articles/meta-unveils-new-ai-supercomputer-11643043601

Biddle, S. (2018a, March 14). *Facebook Quietly Hid Webpages Bragging of Ability to Influence Elections*. The Intercept. https://theintercept.com/2018/03/14/facebook-election-meddling/

Biddle, S. (2018b, April 13). Facebook Uses Artificial Intelligence to Predict Your Future Actions for Advertisers, Says Confidential Document. *The Intercept*. https://theintercept.com/2018/04/13/facebook-advertising-data-artificial-intelligence-ai/

Biddle, S. (2022, July 13). *Amazon Admits Giving Ring Camera Footage to Police Without a Warrant or Consent*. The Intercept. https://theintercept.com/2022/07/13/amazon-ring-camera-footage-police-ed-markey/

Binns, R. (2022). Tracking on the Web, Mobile and the Internet of Things. *Foundations and Trends® in Web Science*, *8*(1–2), 1–113. https://doi.org/10.1561/1800000029

Birhane, A. (2020). Algorithmic Colonization of Africa. *SCRIPTed*, *17*(2), 389–409. https://doi.org/10.2966/scrip.170220.389

Bobrowsky, M. (2021, August 4). Facebook Disables Access for NYU Research Into Political-Ad Targeting. *Wall Street Journal*. https://www.wsj.com/articles/facebook-cuts-off-access-for-nyu-research-into-political-ad-targeting-11628052204

Bond, R. M., Fariss, C. J., Jones, J. J., Kramer, A. D. I., Marlow, C., Settle, J. E., & Fowler, J. H. (2012). A 61-million-person experiment in social influence and political mobilization. *Nature*, *489*(7415), 295–298. https://doi.org/10.1038/nature11421

Bradford, L. R., Aboy, M., & Liddell, K. (2020). *COVID-19 Contact Tracing Apps: A Stress Test for Privacy, the GDPR and Data Protection Regimes* (SSRN Scholarly Paper No. 3617578). https://papers.ssrn.com/abstract=3617578

Bradshaw, S., Bailey, H., & Howard, P. N. (2021). *Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation*. Project on Computational Propaganda. https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/127/2021/01/CyberTroop-Report-2020-v.2.pdf

Brown, I. (2012). Government access to private-sector data in the United Kingdom. *International Data Privacy Law*, *2*(4), 230–238. https://doi.org/10.1093/idpl/ips018

Brown, W. (2015). *Undoing the Demos: Neoliberalism's Stealth Revolution*. Zone Books.

Browning, K., & Mac, R. (2022, May 16). After Buffalo Shooting Video Spreads, Social Platforms Face Questions. *The New York Times*. https://www.nytimes.com/2022/05/15/business/buffalo-shooting-social-media.html

Bruns, A. (2018). Facebook shuts the gate after the horse has bolted, and hurts real research in the process. *Internet Policy Review*. https://policyreview.info/articles/news/facebook-shuts-gate-after-horse-has-bolted-and-hurts-real-research-process/786

Bruns, A. (2019). After the 'APIcalypse': Social media platforms and their fight against critical scholarly research. *Information, Communication & Society*, *22*(11), 1544–1566. https://doi.org/10.1080/1369118X.2019.1637447

Bryant, J. (2021, June 15). A trans-Atlantic discussion on "surveillance-based advertising." *IAPP - The Privacy Advisor*. https://iapp.org/news/a/a-transatlantic-discussion-on-surveillance-based-advertising/

Burgin, A. (2012). *The Great Persuasion: Reinventing Free Markets since the Depression*. Harvard University Press.

Burke, G., & Dearen, J. (2022, September 2). *Tech tool offers police 'mass surveillance on a budget.'* Associated Press. https://apnews.com/article/technology-police-government-surveillance-d395409ef5a8c6c3f6cdab5b1d0e27ef

Califf, R. (2022, May 7). *FDA chief explains why misinformation is leading cause of death in US - CNN* (Brown, P., Interviewer) [Interview]. https://www.cnn.com/videos/health/2022/05/07/fda-robert-califf-intv-misinformation-death-sot-vpx.cnn

Campbell, Z., & Jones, C. (2022, February 11). Kitchen Appliance Maker Wants to Revolutionize Video Surveillance. *The Intercept*. https://theintercept.com/2022/02/11/surveillance-video-ai-bosch-azena/

Cancryn, A. (2020, April 7). *Kushner's team seeks national coronavirus surveillance system*. https://www.politico.com/news/2020/04/07/kushner-coronavirus-surveillance-174165

Cardoso, T., & O'Kane, J. (2019, October 30). Sidewalk Labs document reveals company's

early vision for data collection, tax powers, criminal justice. *The Globe and Mail*. https://www.theglobeandmail.com/business/article-sidewalk-labs-document-reveals-companys-early-plans-for-data/

Cate, F. H., & Dempsey, J. X. (Eds.). (2017). *Bulk Collection: Systematic Government Access to Private-Sector Data*. Oxford University Press. https://doi.org/10.1093/oso/9780190685515.001.0001

CCDH & Anti-Vax Watch. (2021). *The Disinformation Dozen: The Sequel*. Centre for Countering Digital Hate. https://counterhate.com/research/disinformation-dozen-the-sequel/

Chafkin, M. (2021). *The Contrarian: Peter Thiel and Silicon Valley's Pursuit of Power*. Penguin Press.

Chander, A. (2014). How Law Made Silicon Valley. *Emory Law Journal*, *63*(3), 639.

Chander, A., & Le, U. P. (2014). Free Speech. *Iowa Law Review*, *100*(501). https://doi.org/10.2139/ssrn.2320124

Chen, G. J., Wiener, J. L., Iyer, S., Jaiswal, A., Lei, R., Simha, N., Wang, W., Wilfong, K., Williamson, T., & Yilmaz, S. (2016). Realtime Data Processing at Facebook. *Proceedings of the 2016 International Conference on Management of Data*, 1087–1098. https://doi.org/10.1145/2882903.2904441

Christensen, C. M., Skok, D., & Allworth, J. (2012, September 15). *Breaking News: Mastering the art of disruptive innovation in journalism*. Nieman Reports. https://niemanreports.org/articles/breaking-news/

Chung, J. (2021). *Big Tech, Big Cash: Washington's New Power Players* (p. 34). Public Citizen.

Cinelli, M., De Francisci Morales, G., Galeazzi, A., Quattrociocchi, W., & Starnini, M. (2021). The echo chamber effect on social media. *Proceedings of the National Academy of Sciences*, *118*(9), e2023301118. https://doi.org/10.1073/pnas.2023301118

Citron, D., & Franks, M. (2020). The Internet as a Speech Machine and Other Myths Confounding Section 230 Reform. *University of Chicago Legal Forum*, *2020*(1), 45–76.

Citron, D. K. (2022). *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age*. W. W. Norton & Company. https://www.daniellecitron.com/the-fight-for-privacy-protecting-dignity-identity-and-love-in-our-digital-age/

Citron, D. K., & Solove, D. J. (2022). Privacy Harms. *Boston University Law Review*, *102*. https://doi.org/10.2139/ssrn.3782222

Clammer, J. R. (1976). *Literacy and Social Change: A Case Study of Fiji*. Brill.

Clanchy, M. T. (1979). *From Memory to Written Record, England, 1066-1307*. Edward Arnold.

Clinton, P. W. J., & Gore, V. P. A, Jr.. (1997). *A Framework For Global Electronic Commerce*. The White House. https://clintonwhitehouse4.archives.gov/WH/New/Commerce/read.html

Cohen, N. (2009, October 11). Is It a Day to Be Happy? Check the Index. *The New York Times*. https://www.nytimes.com/2009/10/12/technology/internet/12link.html

Collier, K., & Burke, M. (2022, August 9). *Facebook turned over chat messages between mother and daughter now charged over abortion*. NBC News. https://www.nbcnews.com/tech/tech-news/facebook-turned-chat-messages-mother-daughter-now-charged-abortion-rcna42185

Competition and Antitrust Law Enforcement Reform Act. (2021). S.225, United States Senate, 117. http://www.congress.gov/

Constella. (2021). *Polarization as an Emerging Source of Digital Risk* (Polarization and Threat Intelligence Analysis, p. 11). Constella Intelligence. https://info.constellaintelligence.com/hubfs/PDFs/polarization-digital-risk-analysis-2109.pdf?_hsmi=159025854&_hsenc=p2ANqtz-8LUZ1uoodqx5WDbX2PXgGfgX-4tJi0zytPQiHcmCHWF9bqWdhIPXJJV3G-GM23qAWt2ACkimr1i160t5MmEAnLHTo-bzywA

Corbet, S., & Chan, K. (2020, June 2). *French virus tracing app goes live amid debate over privacy*. AP NEWS. https://apnews.com/article/understanding-the-outbreak-virus-outbreak-germany-paris-france-d67ef-2b17e287677e538fe3876a9df41

Corn, G. P., & Taylor, R. (2017). Sovereignty in the Age of Cyber. *AJIL Unbound*, *111*, 207–212. https://doi.org/10.1017/aju.2017.57

Crețu, A.-M., Monti, F., Marrone, S., Dong, X., Bronstein, M., & de Montjoye, Y.-A. (2022). Interaction data are identifiable even across long periods of time. *Nature Communications*, *13*(1), 313. https://doi.org/10.1038/s41467-021-27714-6

Cunningham-Cook, M. (2021, January 14). Arizona GOP Chair Urged Violence at the Capitol. The Mercers Spent $1.5 Million Supporting Her. *The*

Intercept. https://theintercept.com/2021/01/14/capitol-riot-mercers-election-unrest/

Davis, W. (2021, March 25). Lawmakers Ready Bill To Ban "Surveillance Advertising." *Media Post - Policy Blog*. https://www.mediapost.com/publications/article/361757/lawmakers-ready-bill-to-ban-surveillance-advertis.html

Dawson, J. (2021). Microtargeting as Information Warfare. *The Cyber Defense Review*. https://doi.org/10.31235/osf.io/5wzuq

De Vynck, G., Drozdiak, N., & Fouquet, H. (2020, May 13). Apple-Google Virus-Tracking Rules Put Apps in a Privacy Bind. *Bloomberg*. https://www.bloomberg.com/news/articles/2020-05-13/apple-google-virus-tracking-rules-put-apps-in-a-privacy-bind

De Vynck, G., & Zakrzewski, C. (2021, December 29). As omicron washes over America, much of the country still isn't using exposure notification apps. *Washington Post*. https://www.washingtonpost.com/technology/2021/12/29/omicron-exposure-notification-apple/

Dehaye, P.-O., & Reardon, J. (2020). Proximity Tracing in an Ecosystem of Surveillance Capitalism. In *Proceedings of the 19th Workshop on Privacy in the Electronic Society* (pp. 191–203). Association for Computing Machinery. https://doi.org/10.1145/3411497.3420219

Del Vicario, M., Bessi, A., Zollo, F., Petroni, F., Scala, A., Caldarelli, G., Stanley, H. E., & Quattrociocchi, W. (2016). The spreading of misinformation online. *Proceedings of the National Academy of Sciences*, *113*(3), 554–559. https://doi.org/10.1073/pnas.1517441113

Díaz, Á. (2020, December 21). Law Enforcement Access to Smart Devices. *Brennan Center for Justice*. https://www.brennancenter.org/our-work/research-reports/law-enforcement-access-smart-devices

Diaz, A., & Birnbaum, E. (2022, July 21). Amazon Breaks Lobbying Record Amid Antitrust Fight. *Bloomberg.Com*. https://www.bloomberg.com/news/articles/2022-07-21/amazon-breaks-lobbying-record-amid-antitrust-fight

Doctor Radio NYU. (2022, May 6). *Commissioner of Food and Drugs at the FDA Dr. Robert M. Califf says misinformation is the leading cause of death* [Recorded by R. M. Califf]. https://www.siriusxm.com/clips/clip/e7adfb79-ca09-4825-b8ca-1aa0c124dea0/d33de290-bbe4-48a7-8b90-a5f34f3b976b

Donovan, J. (2020). Social-media companies must flatten the curve of misinformation. *Nature*. https://doi.org/10.1038/d41586-020-01107-z

Dunn, J. (2016, May 9). Introducing FBLearner Flow: Facebook's AI backbone. *Engineering at Meta*. https://engineering.fb.com/2016/05/09/core-data/introducing-fblearner-flow-facebook-s-ai-backbone/

Durkheim, É. (1964). *The Division of Labor in Society* (G. Simpson, Trans.). The Free Press.

Dwoskin, E., Timberg, C., & Romm, T. (2020, June 28). Zuckerberg once wanted to sanction Trump. Then Facebook wrote rules that accommodated him. *Washington Post*. https://www.washingtonpost.com/technology/2020/06/28/facebook-zuckerberg-trump-hate/

Easton, W. (2021, February 17). Changes to Sharing and Viewing News on Facebook in Australia. *Meta*. https://about.fb.com/news/2021/02/changes-to-sharing-and-viewing-news-on-facebook-in-australia/

Ebenstein, L. (2012). *The Indispensable Milton Friedman: Essays on Politics and Economics*. Regnery Publishing.

Edelson, L., Nguyen, M.-K., Goldstein, I., Goga, O., Lauinger, T., & McCoy, D. (2021). Understanding engagement with U.S. (mis)information news sources on Facebook. *Proceedings of the 21st ACM Internet Measurement Conference*, 444–463. https://doi.org/10.1145/3487552.3487859

Edwards, D. (2011). *I'm Feeling Lucky: The Confessions of Google Employee Number 59*. Houghton Mifflin Harcourt.

Eshoo, A. G. (2020, May 26). Rep. Eshoo Introduces Bill to Ban Microtargeted Political Ads (Press Release). *Congresswomen Anna G. Eshoo*. https://eshoo.house.gov/media/press-releases/rep-eshoo-introduces-bill-ban-microtargeted-political-ads

Eshoo, A. G. (2022, January 18). Eshoo, Schakowsky, Booker Introduce Bill to Ban Surveillance Advertising (Press Release). *Congresswomen Anna G. Eshoo*. https://eshoo.house.gov/media/press-releases/eshoo-schakowsky-booker-introduce-bill-ban-surveillance-advertising

European Commission. (2020, April 16). Coronavirus: An EU approach for efficient contact tracing [Text]. *European Commission*. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_670

European Commission. (2022a, May 4). *European Digital Rights and Principles*. European

Commission. https://digital-strategy.ec.europa.eu/en/policies/digital-principles

European Commission. (2022b, August 11). *A European approach to artificial intelligence*. European Commission. https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

European Parliament. (2020, April 17). *Texts Adopted: EU coordinated action to combat the COVID-19 pandemic and its consequences*. European Parliament. https://www.europarl.europa.eu/doceo/document/TA-9-2020-0054_EN.pdf

European Parliament. (2021). *Opinion of the Committee on Civil Liberties, Justice and Home Affairs for the Committee on the Internal Market and Consumer Protection on the proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*. Committee on Civil Liberties, Justice and Home Affairs. https://www.europarl.europa.eu/doceo/document/LIBE-AD-692898_EN.pdf

European Parliament. (2022, May 7). Digital Services: Landmark rules adopted for a safer, open online environment | News | European Parliament. *European Parliament News*. https://www.europarl.europa.eu/news/en/press-room/20220701IPR34364/digital-services-landmark-rules-adopted-for-a-safer-open-online-environment

Evanega, S., Lynas, M., Adams, J., & Smolenyak, K. (2020). Coronavirus misinformation: Quantifying sources and themes in the COVID-19 "infodemic." *JMIR Preprints*, *19*(10), 13.

Facebook Ad and Business Product Team. (2021). *Facebook Data Lineage Internal Document: ABP Privacy Infra, Long Range Investments [A/C Priv]*. Facebook Internal Document. https://s3.documentcloud.org/documents/21716382/facebook-data-lineage-internal-document.pdf

Faife, C., & Ng, A. (2021, June 24). *After Repeatedly Promising Not to, Facebook Keeps Recommending Political Groups to Its Users*. The Markup. https://themarkup.org/citizen-browser/2021/06/24/after-repeatedly-promising-not-to-facebook-keeps-recommending-political-groups-to-its-users

Feathers, T. (2021, October 29). *Leaked Facebook Documents Reveal How Company Failed on Election Promise*. The Markup. https://themarkup.org/citizen-browser/2021/10/29/leaked-facebook-documents-reveal-how-company-failed-on-election-promise

Feathers, T., Fondrie-Teitler, S., Waller, A., & Mattu, S. (2022, June 16). Facebook Is Receiving Sensitive Medical Information from Hospital Websites – The Markup. *The Markup*. https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites

Federal Trade Commission. (2022, August 11). *Federal Register Notice: Commercial Surveillance and Data Security Rulemaking*. https://www.ftc.gov/legal-library/browse/federal-register-notices/commercial-surveillance-data-security-rulemaking

Feiner, L. (2019, January 8). *Apple CEO Tim Cook speaks with CNBC's Jim Cramer: Full transcript*. CNBC. https://www.cnbc.com/2019/01/08/apple-ceo-tim-cook-interview-cnbc-jim-cramer-transcript.html

Feuer, W. (2021, December 13). Facebook exec blames company's users for spreading misinformation. *New York Post*. https://nypost.com/2021/12/13/facebook-exec-blames-users-for-spreading-misinformation/

Fidler, M. (2021). The New Editors: Refining First Amendment Protections For Internet Platforms. *Journal on Emerging Technologies*, *2*(2). https://ndlsjet.com/fidler-the-new-editors-refining-first-amendment-protections-for-internet-platforms/

Fioretti, J. (2018, April 25). EU targets 20 billion euro investment in AI to catch up with US, Asia. *Reuters*. https://www.reuters.com/article/eu-artificialintelligence-idUSL8N1S26LG

Fitzgerald, M., & Crider, C. (2020, May 7). We need urgent answers about the massive NHS COVID data deal. *OpenDemocracy*. https://www.opendemocracy.net/en/ournhs/we-need-urgent-answers-about-massive-nhs-covid-data-deal/

Fitzpatrick, A. (2018, December 6). *An Inside Look at Apple's Biggest Step Yet in Health Care*. Time. https://time.com/5472329/apple-watch-ecg/

Fleischer, V. (2010). *Regulatory Arbitrage* (No. 1567212). SSRN Scholarly Paper. https://doi.org/10.2139/ssrn.1567212

Flichy, P. (2007). *The Internet Imaginaire*. MIT Press.

Flyverbom, M. (2022). Overlit: Digital Architectures of Visibility. *Organization Theory*, *3*(3), 26317877221090310. https://doi.org/10.1177/26317877221090314

Fowler, G. A. (2019a, May 6). Alexa has been eavesdropping on you this whole time. *The*

Washington Post. https://www.washingtonpost.com/technology/2019/05/06/alexa-has-been-eavesdropping-you-this-whole-time/

Fowler, G. A. (2019b, June 21). Goodbye, Chrome: Google's Web browser has become spy software. *The Washington Post*. https://www.washingtonpost.com/technology/2019/06/21/google-chrome-has-become-surveillance-software-its-time-switch/

Fowler, G. A. (2019c, September 18). You watch TV. Your TV watches back. *The Washington Post*. https://www.washingtonpost.com/technology/2019/09/18/you-watch-tv-your-tv-watches-back/

Fowler, G. A. (2021, September 23). When you "Ask app not to track," some iPhone apps keep snooping anyway. *The Washington Post*. https://www.washingtonpost.com/technology/2021/09/23/iphone-tracking/

Fraga, B. L., McElwee, S., Rhodes, J., & Schaffner, B. F. (2017, May 8). Why did Trump win? More whites—and fewer blacks—actually voted. *Washington Post*. https://www.washingtonpost.com/news/monkey-cage/wp/2017/05/08/why-did-trump-win-more-whites-and-fewer-blacks-than-normal-actually-voted/

Franceschi-Bicchierai, L. (2022, April 26). *Facebook Doesn't Know What It Does With Your Data, Or Where It Goes: Leaked Document*. Motherboard. https://web.archive.org/web/20220709113629/https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes

Frantz, E., Kendall-Taylor, A., & Wright, J. (2020). *Digital Repression in Autocracies* (Users Working Paper 2020:27; p. 54). The Varieties of Democracy Institute.

Frenkel, S. (2021, July 19). White House Dispute Exposes Facebook Blind Spot on Misinformation. *The New York Times*. https://www.nytimes.com/2021/07/19/technology/facebook-misinformation-blind-spot.html

Frenkel, S., Alba, D., & Zhong, R. (2020, March 8). Surge of Virus Misinformation Stumps Facebook and Twitter. *The New York Times*. https://www.nytimes.com/2020/03/08/technology/coronavirus-misinformation-social-media.html

Friedman, M. (1970, September 13). A Friedman doctrine—The Social Responsibility Of Business Is to Increase Its Profits. *The New York Times*. https://www.nytimes.com/1970/09/13/archives/a-friedman-doctrine-the-social-responsibility-of-business-is-to.html

Friedman, M. (1976). The Fragility of Freedom. *BYU Studies Quarterly*, *16*(4). https://scholarsarchive.byu.edu/byusq/vol16/iss4/12

Friedman, M. (2002). *Capitalism and Freedom* (40th anniversary edition, with a new foreword). University of Chicago Press.

Friedman, M. (2017a). *Milton Friedman on Freedom: Selections from The Collected Works of Milton Friedman* (Kindle). Hoover Institute Press.

Friedman, M. (2017b). *The Future of Capitalism*. Hoover Institution. https://www.hoover.org/research/future-capitalism

Friedman, M., Piñera, J., de Castro, S., Kaiser, A., & Bellolio, J. (2012). *Un legado de libertad: Milton Friedman en Chile* (A. Soto, Ed.). Fundación para el Progreso / Atlas Economic Research Foundation / Fundación Jaime Guzmán / Instituto Democracia y Mercado. https://www.fppchile.cl/wp-content/uploads/2014/09/Libro-Friedman-version-completa.pdf

Future of Tech Commission. (2021, September 23). Poll: Nine out of Ten Voters Support Strong Online Privacy Protections While Eight Out of Ten Strongly Support Holding Social Media Companies More Accountable for "Illegal and Harmful Content" Posted on Their Sites. *Future of Tech Commission*. https://www.futureoftechcommission.org/press-release-launch-poll

Gao, J., Zhang, Y.-C., & Zhou, T. (2019). Computational socioeconomics. *Physics Reports*, *817*, 1–104. https://doi.org/10.1016/j.physrep.2019.05.002

Gellman, B. (2020). *Dark Mirror: Edward Snowden and the American Surveillance State*. Penguin Press.

Germani, F., & Biller-Andorno, N. (2020). The anti-vaccination infodemic on social media: A behavioral analysis. *PLos One*, *16*. https://doi.org/10.1101/2020.12.07.20223370

Ghaffary, S. (2021, August 6). People do not trust that Facebook is a healthy ecosystem. *Vox*. https://www.vox.com/recode/22612151/laura-edelson-facebook-nyu-ad-observatory-social-media-researcher

Gibney, E. (2019). Privacy hurdles thwart Facebook democracy research. *Nature*, *574*(7777), 158–160.

Gilbert, B. (2020, January 8). *Facebook is the reason Trump got elected, says Facebook exec who ran advertising during the 2016 election, "but not*

for the reasons anyone thinks." Business Insider. https://www.businessinsider.com/facebook-ads-elected-trump-andrew-bosworth-says-2020-1

Gilbert, D. (2021, January 15). Steve Bannon Urged Facebook Followers to "Take Action" on Eve of Capitol Riot. *Vice*. https://www.vice.com/en/article/n7vqgb/steve-bannon-urged-facebook-followers-to-take-action-on-eve-of-capitol-riot

Gingerich, J. (2021). Is Spotify Bad for Democracy? Artificial Intelligence, Cultural Democracy, and Law. *Yale Journal of Law and Technology*, *24*(227), 90.

Global Witness. (2022a, July 28). *Facebook approves ads calling for ethnic violence in the lead up to a tense Kenyan election*. Global Witness. https:///en/press-releases/facebook-approves-ads-calling-ethnic-violence-lead-tense-kenyan-election/

Global Witness. (2022b, August 17). *Rehashing existing policies by Facebook not enough to combat election disinformation in Brazil*. Global Witness. https:///en/press-releases/rehashing-existing-policies-facebook-not-enough-combat-election-disinformation-brazil/

Gofman, M. (2021, June 23). AI Brain Drain. *Simon Business School, University of Rochester - Simon Blog: Dean's Corner*. https://simon.rochester.edu/blog/deans-corner/brain-drain

Gofman, M., & Jin, Z. (2022). *Artificial Intelligence, Education, and Entrepreneurship*. https://doi.org/10.2139/ssrn.3449440

Goldstein, A. (2021, January 27). *Social Media Engagement with Deceptive Sites Reached Record Highs in 2020*. German Marshall Fund. https://www.gmfus.org/news/social-media-engagement-deceptive-sites-reached-record-highs-2020

Goodman, E. P., & Powles, J. (2019). Urbanism under Google: Lessons from Sidewalk Toronto. *Fordham Law Review*, *88*, 457.

Goody, J. (1986). *The Logic of Writing and the Organization of Society*. Cambridge University Press. http://hdl.handle.net/2027/heb.05702

Google Inc. (2004). *Form 10-K 2004*. https://content.edgar-online.com/ExternalLink/EDGAR/0001193125-05-065298.html?hash=52891c0ad117912f1ca1079cbd630a820a2f65e9db0cfcd50e8d855a989fc2fb&dest=DEX100801_HTM#D10K_HTM_TOC10062_9

Grafton, A., Blair, A., Duguid, P., & Goeing, A.-S. (Eds.). (2021). Communication, Computation and Information. In *Information: A Historical Companion*. Princeton University Press.

Grand View Research. (2022). *Location Intelligence Market Size, Share & Trends Analysis Report By Application (Sales & Marketing Optimization, Remote Monitoring), By Service, By Vertical, By Region, And Segment Forecasts, 2022—2030*. Grand View Research. https://www.grandviewresearch.com/industry-analysis/location-intelligence-market

Grauer, Y. (2022, April 15). Video Doorbell Cameras Record Audio, Too. *Consumer Reports*. https://www.consumerreports.org/video-doorbells/video-doorbell-cameras-record-audio-too-a4636115889/

Green, J., & Issenberg, S. (2016, October 27). Inside the Trump Bunker, With Days to Go. *Bloomberg.Com*. https://www.bloomberg.com/news/articles/2016-10-27/inside-the-trump-bunker-with-12-days-to-go

Grind, K., McMillan, R., & Mathews, A. W. (2020, March 17). To Track Virus, Governments Weigh Surveillance Tools That Push Privacy Limits. *The Wall Street Journal*. https://www.wsj.com/articles/to-track-virus-governments-weigh-surveillance-tools-that-push-privacy-limits-11584479841

Grunwald, M. (2020, April 25). Biden wants a new stimulus "a hell of a lot bigger" than $2 trillion. *POLITICO*. https://www.politico.com/news/2020/04/25/joe-biden-green-stimulus-207848

Gursky, J., & Woolley, S. (2020, June 21). The Trump 2020 app is a voter surveillance tool of extraordinary power. *MIT Technology Review*. https://www.technologyreview.com/2020/06/21/1004228/trumps-data-hungry-invasive-app-is-a-voter-surveillance-tool-of-extraordinary-scope/

Guthrie, S., & Benjamin, M. (2022, March 4). Microsoft + Nuance: Better together to transform business and healthcare outcomes with AI. *Official Microsoft Blog*. https://blogs.microsoft.com/blog/2022/03/04/microsoft-nuance-better-together-to-transform-business-and-healthcare-outcomes-with-ai/

Gvili, Y. (2020). Security Analysis of the COVID-19 Contact Tracing Specifications by Apple Inc. And Google Inc. *Cryptology EPrint Archive*. https://eprint.iacr.org/2020/428

Hagey, K., & Horwitz, J. (2021, September 15). Facebook Tried to Make Its Platform a Healthier Place. It Got Angrier Instead. *Wall Street Journal*. https://www.wsj.com

/articles/facebook-algorithm-change-zuckerberg-11631654215

Hao, K. (2021a, March 11). How Facebook got addicted to spreading misinformation. *MIT Technology Review*. https://www.technologyreview.com/2021/03/11/1020600/facebook-responsible-ai-misinformation/

Hao, K. (2021b, November 20). How Facebook and Google fund global misinformation. *MIT Technology Review*. https://www.technologyreview.com/2021/11/20/1039076/facebook-google-disinformation-clickbait/

Hao, K. (2022, April 19). *Artificial intelligence is creating a new colonial world order*. MIT Technology Review. https://www.technologyreview.com/2022/04/19/1049592/artificial-intelligence-colonialism/

Hao, K., & Hernández, A. P. (2022, April 20). *How the AI industry profits from catastrophe*. MIT Technology Review. https://www.technologyreview.com/2022/04/20/1050392/ai-industry-appen-scale-data-labels/

Harwell, D., & Oremus, W. (2022, May 16). Only 22 saw the Buffalo shooting live. Millions have seen it since. *The Washington Post*. https://www.washingtonpost.com/technology/2022/05/16/buffalo-shooting-live-stream/

Haskins, C. (2019, November 1). Gaggle Knows Everything About Teens And Kids In School. *BuzzFeed News*. https://www.buzzfeednews.com/article/carolinehaskins1/gaggle-school-surveillance-technology-education

Hayek, F. A. (1945). The Use of Knowledge in Society. In F. A. Hayek (Ed.), *Individualism and Economic Order*. University of Chicago Press.

Hayek, F. A. (1980). *Individualism and Economic Order*. University of Chicago Press.

Hayek, F. A. (1988). *The Fatal Conceit: The Errors of Socialism* (W. W. Bartley III, Ed.). The University of Chicago Press. https://press.uchicago.edu/ucp/books/book/chicago/F/bo3643985.html

Hayek, F. A. (2007). *The Road to Serfdom: Text and Documents–The Definitive Edition* (B. Caldwell, Ed.; Kindle). The University of Chicago Press. https://press.uchicago.edu/ucp/books/book/chicago/R/bo4138549.html

Hazelwood, K., Bird, S., Brooks, D., Chintala, S., Diril, U., Dzhulgakov, D., Fawzy, M., Jia, B., Jia, Y., Kalro, A., Law, J., Lee, K., Lu, J., Noordhuis, P., Smelyanskiy, M., Xiong, L., & Wang, X. (2018). Applied Machine Learning at Facebook: A Datacenter Infrastructure Perspective. *2018 IEEE International Symposium on High Performance Computer Architecture (HPCA)*, 620–629. https://doi.org/10.1109/HPCA.2018.00059

Heller, B. (2021). Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law. *Vand. J. Ent. & Tech. L.*, *23*(1). https://www.vanderbilt.edu/jetlaw/2021/04/09/watching-androids-dream-of-electric-sheep-immersive-technology-biometric-psychography-and-the-law/

Hellewell, J., Abbott, S., Gimma, A., Bosse, N. I., Jarvis, C. I., Russell, T. W., Munday, J. D., Kucharski, A. J., Edmunds, W. J., Sun, F., Flasche, S., Quilty, B. J., Davies, N., Liu, Y., Clifford, S., Klepac, P., Jit, M., Diamond, C., Gibbs, H., ... Eggo, R. M. (2020). Feasibility of controlling COVID-19 outbreaks by isolation of cases and contacts. *The Lancet Global Health*, *8*(4), e488–e496. https://doi.org/10.1016/S2214-109X(20)30074-7

Hempel, J. (2008, April 11). Sheryl Sandberg: Facebook's new number two. *CNN Money*. https://money.cnn.com/2008/04/11/technology/facebook_sandberg.fortune/

Hern, A. (2020a, April 16). NHS in standoff with Apple and Google over coronavirus tracing. *The Guardian*. https://www.theguardian.com/technology/2020/apr/16/nhs-in-standoff-with-apple-and-google-over-coronavirus-tracing

Hern, A. (2020b, April 21). France urges Apple and Google to ease privacy rules on contact tracing. *The Guardian*. https://www.theguardian.com/world/2020/apr/21/france-apple-google-privacy-contact-tracing-coronavirus

Hilbert, M. (2012). How much information is there in the "information society"? *Significance*, *9*(4), 8–12. https://doi.org/10.1111/j.1740-9713.2012.00584.x

Hilbert, M., & López, P. (2011). The World's Technological Capacity to Store, Communicate, and Compute Information. *Science*, *332*(6025), 60–65. https://doi.org/10.1126/science.1200970

Hinds, J., & Joinson, A. (2019). Human and Computer Personality Prediction From Digital Footprints. *Current Directions in Psychological Science*, *28*(2), 204–211. https://doi.org/10.1177/0963721419827849

Hoffman, S. (2022). China's Tech-Enhanced Authoritarianism. *Journal of Democracy*, *33*(2), 76–89. https://doi.org/10.1353/jod.2022.0019

Hollis, D. (2018). The Influence of War; The War for Influence. *Temple International & Comparative Law Journal*, *32*(1), 31–46.

Holmes, A., & Langley, H. (2020, June 10). Apple and Google's ambitious COVID-19 contact-tracing tech can help contain the pandemic if used widely. But so far only 3 states have agreed—And none has started to use it. *Business Insider*. https://www.businessinsider.com/apple-google-coronavirus-contact-tracing-tech-states-dont-plan-using-2020-6

Holt, J. (2021). *#StopTheSteal: Timeline of Social Media and Extremist Activities Leading to 1/6 Insurrection*. Atlantic Council - DFRLab. https://www.justsecurity.org/74622/stopthesteal-timeline-of-social-media-and-extremist-activities-leading-to-1-6-insurrection/

Horder, J. (2021). Online Free Speech and the Suppression of False Political Claims. *ILSA Journal of International and Comparative Law*. https://doi.org/10.2139/ssrn.3827192

Horwitz, J. (2020, October 23). Facebook Seeks Shutdown of NYU Research Project Into Political Ad Targeting. *Wall Street Journal*. https://www.wsj.com/articles/facebook-seeks-shutdown-of-nyu-research-project-into-political-ad-targeting-11603488533

Horwitz, J., & Seetharaman, D. (2020, May 26). Facebook Executives Shut Down Efforts to Make the Site Less Divisive. *The Wall Street Journal*. https://www.wsj.com/articles/facebook-knows-it-encourages-division-top-executives-nixed-solutions-11590507499

Horwitz, K., Cherney, M., & Horwitz, J. (2022, May 5). *Facebook Deliberately Caused Havoc in Australia to Influence New Law, Whistleblowers Say*. The Wall Street Journal. https://www.wsj.com/articles/facebook-deliberately-caused-havoc-in-australia-to-influence-new-law-whistleblowers-say-11651768302

Hunt, G. (Director). (2013, April 18). *Gus Hunt (CTO, CIA) Mentions Actitracker @ GigaOm's Structure:Data 2013*. https://www.youtube.com/watch?v=edP95iJWVBI

IAB Tech Lab. (2016). *OpenRTB API Specification Version 2.5*. https://www.iab.com/wp-content/uploads/2016/03/OpenRTB-API-Specification-Version-2-5-FINAL.pdf

Ingram, J. D. (2008). What Is a "Right to Have Rights"? Three Images of the Politics of Human Rights. *The American Political Science Review*, *102*(4), 401–416.

Iqbal, U., Bahrami, P. N., Trimananda, R., Cui, H., Gamero-Garrido, A., Dubois, D., Choffnes, D., Markopoulou, A., Roesner, F., & Shafiq, Z. (2022). *Your Echos are Heard: Tracking, Profiling, and Ad Targeting in the Amazon Smart Speaker Ecosystem* (arXiv:2204.10920). arXiv. https://doi.org/10.48550/arXiv.2204.10920

Isaacson, W. (2014). *The Innovators*. Simon & Schuster.

ISD. (2020). *Far-right Exploitation of Covid-19: ISD and BBC Click Investigation* (No. 3; Covid Disinformation Briefing, pp. 1–8). Insitute for Strategic Dialogue. https://www.isdglobal.org/wp-content/uploads/2020/06/COVID-19-Briefing-03-Institute-for-Strategic-Dialogue-12th-May-2020.pdf#page=1&zoom=auto,-251,848

Jacobides, M. G., Brusoni, S., & Candelon, F. (2021). The Evolutionary Dynamics of the Artificial Intelligence Ecosystem. *Strategy Science*, *6*(4), 412–435. https://doi.org/10.1287/stsc.2021.0148

Jepperson, R. L. (2021). Institutions, Institutional Effects, and Institutionalism (1991). In J. W. Meyer & R. L. Jepperson (Eds.), *Institutional Theory: The Cultural Construction of Organizations, States, and Identities* (pp. 37–66). Cambridge University Press. https://doi.org/10.1017/9781139939744.004

Jepperson, R. L., & Meyer, J. W. (2021). *Institutional Theory: The Cultural Construction of Organizations, States, and Identities* (1st ed.). Cambridge University Press. https://doi.org/10.1017/9781139939744

Johnson, B. (2010, January 10). Privacy no longer a social norm, says Facebook founder. *Guardian*. https://www.theguardian.com/technology/2010/jan/11/facebook-privacy

Johnson, M., Abboud, L., Warrell, H., & Bradshaw, T. (2020, May 1). Europe split over approach to virus contact tracing apps. *Financial Times*. https://www.ft.com/content/10f87eb3-87f9-46ea-88ab-8706adefe72d

Karanicolas, M. (2021). A FOIA for Facebook: Meaningful Transparency for Online Platforms. *St. Louis University Law Journal*, *66*(49). https://doi.org/10.2139/ssrn.3964235

Kaye, K. (2021, July 20). When the White House invoked the s-word, it gave new legitimacy to "surveillance" advertising. *Digiday*. https://digiday.com/marketing/when-the-white-house-invoked-the-s-word-it-gave-new-legitimacy-to-surveillance-advertising/

Kaziukėnas, J. (2021, March 24). *Amazon Tops Six Million Third-Party Sellers*. Marketplace Pulse. https://www.marketplacepulse.com/articles/amazon-reaches-six-million-third-party-sellers

Kelion, L. (2020, April 27). NHS rejects Apple-Google coronavirus app plan. *BBC News*. https://www.bbc.com/news/technology-52441428

Kelly, H., Hunter, T., & Abril, D. (2022, August 12). Seeking an abortion? Here's how to avoid leaving a digital trail. *Washington Post*. https://www.washingtonpost.com/technology/2022/06/26/abortion-online-privacy/

Kerner, C., & Risse, M. (2021). Beyond Porn and Discreditation: Epistemic Promises and Perils of Deepfake Technology in Digital Lifeworlds. *Moral Philosophy and Politics*, *8*(1), 81–108. https://doi.org/10.1515/mopp-2020-0024

Kim, N. S. (2013). *Wrap Contracts: Foundations and Ramifications*. Oxford University Press. https://papers.ssrn.com/abstract=2322255

Kincaid, J. (2009, December 9). The Facebook Privacy Fiasco Begins. *TechCrunch*. https://techcrunch.com/2009/12/09/facebook-privacy/

Kirkpatrick, D. (2011). *The Facebook effect: The inside story of the company that is connecting the world*. Simon & Schuster Paperbacks.

Kissick, C., Setzer, E., & Schulz, J. (2020, July 21). What Ever Happened to Digital Contact Tracing? *Lawfare*. https://www.lawfareblog.com/what-ever-happened-digital-contact-tracing

Klonick, K. (2020). The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression. *Yale Law Journal*, *129*(8), 2418.

Knight Foundation. (2020). *American Views 2020: Trust, Media and Democracy*. Gallup and Knight Foundation. https://knightfoundation.org/reports/american-views-2020-trust-media-and-democracy/

Korb, L. J., & Evans, C. (2017). The Third Offset Strategy: A misleading slogan. *Bulletin of the Atomic Scientists*, *73*(2), 92–95. https://doi.org/10.1080/00963402.2017.1288443

Kouzy, R., Abi Jaoude, J., Kraitem, A., El Alam, M., Karam, B., Adib, E., Zarka, J., Traboulsi, C., Akl, E., & Baddour, K. (2020). Coronavirus Goes Viral: Quantifying the COVID-19 Misinformation Epidemic on Twitter. *Cureus*, *12*. https://doi.org/10.7759/cureus.7255

Kramer, A. D. I., Guillory, J. E., & Hancock, J. T. (2014). Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National Academy of Sciences*, *111*(24), 8788–8790. https://doi.org/10.1073/pnas.1320040111

Kreiss, D., & McGregor, S. C. (2018). Technology Firms Shape Political Communication: The Work of Microsoft, Facebook, Twitter, and Google With Campaigns During the 2016 U.S. Presidential Cycle. *Political Communication*, *35*(2), 155–177. https://doi.org/10.1080/10584609.2017.1364814

Kröger J. L., Lutz O. HM., Müller F. (2020). What Does Your Gaze Reveal About You? On the Privacy Implications of Eye Tracking. In: Friedewald M. et al. (Eds.) *Privacy and Identity Management. Data for Better Living: AI and Privacy* (pp. 226–241). Springer, Cham. https://doi.org/10.1007/978-3-030-42504-3_15

Krogstad, J. M., & Lopez, M. H. (2017, May 12). Black voter turnout fell in 2016, even as a record number of Americans cast ballots. *Pew Research Center*. https://www.pewresearch.org/fact-tank/2017/05/12/black-voter-turnout-fell-in-2016-even-as-a-record-number-of-americans-cast-ballots/

Kurmanaev, A. (2022, September 3). How fake GPS coordinates are leading to lawlessness on the high seas. *The New York Times*. https://www.nytimes.com/2022/09/03/world/americas/ships-gps-international-law.html

Lapowsky, I. (2020, May 6). *How Facebook's oversight board could rewrite the rules of the entire internet*. Protocol. https://www.protocol.com/facebook-oversight-board-rules-of-the-internet

Leibowitz, J. (2022, February 14). How Congress Can Protect Your Data Privacy. *Wall Street Journal*. https://www.wsj.com/articles/congress-can-protect-our-data-consumer-privacy-bipartisan-personal-information-regulations-online-security-ftc-cybersecurity-11644871937

Levy, R. (2021). Social Media, News Consumption, and Polarization: Evidence from a Field Experiment. *American Economic Review*, *111*(3), 831–870. https://doi.org/10.1257/aer.20191777

Levy, S. (2011). *In The Plex: How Google Thinks, Works, and Shapes Our Lives*. Simon & Schuster.

Lewin, J. (2021, March 17). Facebook's long-awaited content "supreme court" has arrived. It's a clever sham. *The Guardian*. https://www.theguardian.com/commentisfree/2021/mar/17/facebook-content-supreme-court-network

Li, T. C. (2022, June 26). Why you should delete your period-tracking app right now. *MSNBC*.

https://www.msnbc.com/opinion/msnbc-opinion/states-abortion-bans-can-weaponize-your-own-data-against-you-n1296591

Libicki, M. C. (2017). The Convergence of Information Warfare. *Strategic Studies Quarterly*, 49–65.

Lima, C. (2021, December 14). Facebook's latest defense: Social media doesn't hurt people. People hurt people. *The Washington Post*. https://www.washingtonpost.com/politics/2021/12/14/facebooks-latest-defense-social-media-doesnt-hurt-people-people-hurt-people/

Lima, J. M. (2017, April 11). Hyperscalers taking over the world at an unprecedented scale. *Data Economy*. https://web.archive.org/web/20170615104605/https://data-economy.com/hyperscalers-taking-world-unprecedented-scale/

Lin, H. (2019). The existential threat from cyber-enabled information warfare. *Bulletin of the Atomic Scientists*, *75*(4), 187–196. https://doi.org/10.1080/00963402.2019.1629574

Linebaugh, C. D. (2022). *Abortion, Data Privacy, and Law Enforcement Access: A Legal Overview* (No. LSB10786). Congressional Research Service. https://crsreports.congress.gov/product/pdf/LSB/LSB10786

Location Intelligence Market Size Share Report, 2022–2030 (GVR-2-68038-401-7; p. 153). (2022). Grand View Research. https://web.archive.org/web/20220525210808/https://www.grandviewresearch.com/industry-analysis/location-intelligence-market

Lohr, S. (2019, September 26). At Tech's Leading Edge, Worry About a Concentration of Power. *The New York Times*. https://www.nytimes.com/2019/09/26/technology/ai-computer-expense.html

Lomas, N. (2020a, April 6). EU privacy experts push a decentralized approach to COVID-19 contacts tracing. *TechCrunch*. https://techcrunch.com/2020/04/06/eu-privacy-experts-push-a-decentralized-approach-to-covid-19-contacts-tracing/

Lomas, N. (2020b, April 16). EU lawmakers set out guidance for coronavirus contacts tracing apps. *TechCrunch*. https://techcrunch.com/2020/04/16/eu-lawmakers-set-out-guidance-for-coronavirus-contacts-tracing-apps/

Loomba, S., de Figueiredo, A., Piatek, S. J., de Graaf, K., & Larson, H. J. (2021). Measuring the impact of COVID-19 vaccine misinformation on vaccination intent in the UK and USA. *Nature Human Behaviour*, *5*(3), 337–348. https://doi.org/10.1038/s41562-021-01056-1

Lyon, D. (2022). *Pandemic Surveillance*. Polity Press. https://www.wiley.com/en-us/Pandemic+Surveillance-p-9781509550319

Ma, L., & Sun, B. (2020). Machine learning and AI in marketing – Connecting computing power to human insights. *International Journal of Research in Marketing*, *37*(3), 481–504. https://doi.org/10.1016/j.ijresmar.2020.04.005

Mac, R., & Silverman, C. (2020, November 5). *Facebook Has A Metric For "Violence And Incitement Trends." It's Rising*. BuzzFeed News. https://www.buzzfeednews.com/article/ryanmac/facebook-internal-metric-violence-incitement-rising-vote

Mac, R., Warzel, C., & Kantrowitz, A. (2018, March 29). Growth At Any Cost: Top Facebook Executive Defended Data Collection In 2016 Memo—And Warned That Facebook Could Get People Killed. *BuzzFeed News*. https://www.buzzfeednews.com/article/ryanmac/growth-at-any-cost-top-facebook-executive-defended-data

MacMillan, D., Kelly, H., Dwoskin, E., & Dawsey, J. (2020, March 16). Trump announced Google was building a virus screening tool. Then someone had to build it. *Washington Post*. https://www.washingtonpost.com/technology/2020/03/16/google-verily-coronavirus-website-trump/

Manns, J. (2020). *The Case for Preemptive Oligopoly Regulation* (SSRN Scholarly Paper No. 3665651). https://papers.ssrn.com/abstract=3665651

Markoff, J. (2005). *What the Dormouse Said*. Viking Penguin.

Martin, N. (2021). *Noelle Martin—Fighting for Online Safety, Justice, and Accountability*. Noelle Martin. https://www.noellemartin.org/

McBride, S., & Vance, A. (2019, June 18). Apple, Google, and Facebook Are Raiding Animal Research Labs. *Bloomberg Businessweek*. https://www.bloomberg.com/news/features/2019-06-18/apple-google-and-facebook-are-raiding-animal-research-labs

McConnell, M. (2010, February 28). Mike McConnell on how to win the cyber-war we're losing. *The Washington Post*. http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html

McCorkindale, T., & Henry, A. (2022). *2022 Institute for Public Relations Disinformation in Society*

Report. Institute for Public Relations. https://instituteforpr.org/2022-disinformation-report/

McGuinness, T. (2022, March 15). Microsoft Cloud for Healthcare: Reshaping the future of healthcare. *Microsoft Industry Blogs*. https://cloudblogs.microsoft.com/industry-blog/health/2022/03/15/microsoft-cloud-for-healthcare-reshaping-the-future-of-healthcare/

Menendez, R. (2020). *The new big brother–China and digital authoritarianism: A minority staff report*. U.S. Government Publishing Office.

Merrill, J. B., & Oremus, W. (2021, October 26). *Five points for anger, one for a 'like': How Facebook's formula fostered rage and misinformation*. Washington Post. https://www.washingtonpost.com/technology/2021/10/26/facebook-angry-emoji-algorithm/

Metz, C. (2017a, April 5). Building an AI Chip Saved Google From Building a Dozen New Data Centers. *Wired*. https://www.wired.com/2017/04/building-ai-chip-saved-google-building-dozen-new-data-centers/

Metz, C. (2017b, October 22). Tech Giants Are Paying Huge Salaries for Scarce A.I. Talent. *The New York Times*. https://www.nytimes.com/2017/10/22/technology/artificial-intelligence-experts-salaries.html

Metz, R. (2021, October 27). *Likes, anger emojis and RSVPs: The math behind Facebook's News Feed—and how it backfired | CNN Business*. CNN. https://www.cnn.com/2021/10/27/tech/facebook-papers-meaningful-social-interaction-news-feed-math/index.html

Mirowski, P. (2013). *Never let a serious crisis go to waste: How neoliberalism survived the financial meltdown*. Verso.

MIT Sloan School of Management. (2013, November 6). Uber CEO talks regulatory disruption, maintaining startup culture. *MIT Management Sloan School Newsroom*. https://perma.cc/NG3C-XWC7

Mosco, V. (2004). *The Digital Sublime: Myth, Power, and Cyberspace*. MIT Press.

Moses, D. A., Leonard, M. K., Makin, J. G., & Chang, E. F. (2019). Real-time decoding of question-and-answer speech dialogue using human cortical activity. *Nature Communications*, *10*(1), 3096. https://doi.org/10.1038/s41467-019-10994-4

Mosseri, A. (2018, January 11). News Feed FYI: Bringing People Closer Together. *Facebook Newsroom*. https://newsroom.fb.com/news/2018/01/news-feed-fyi-bringing-people-closer-together/

Mozur, P., Kessel, J. M., & Chan, M. (2019, April 24). Made in China, Exported to the World: The Surveillance State. *The New York Times*. https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html

Mozur, P., & Scott, M. (2016, November 17). Fake News in U.S. Election? Elsewhere, That's Nothing New. *The New York Times*. https://www.nytimes.com/2016/11/18/technology/fake-news-on-facebook-in-foreign-elections-thats-not-new.html

Murgia, M. (2019a, March 13). AI academics under pressure to do commercial research. *Financial Times*. https://www.ft.com/content/94e86cd0-44b6-11e9-a965-23d669740bfb

Murgia, M. (2019b, June 6). Microsoft quietly deletes largest public face recognition data set. *Financial Times*.

Murgia, M., Criddle, C., & Murphy, H. (2021, December 6). Investigating Facebook: A fractious relationship with academia. *Financial Times*.

Murgia, M., & Gross, A. (2020, March 27). Inside China's controversial mission to reinvent the internet. *Financial Times*. https://www.ft.com/content/ba94c2bc-6e27-11ea-9bca-bf503995cd6f

Murphy, H. (2022, January 18). Facebook patents reveal how it intends to cash in on metaverse. *Financial Times*. https://www.ft.com/content/76d40aac-034e-4e0b-95eb-c5d34146f647

Murphy, L. W., & Cacace, M. (2020). *Facebook's Civil Rights Audit—Final Report*. Relman Colfax. https://www.relmanlaw.com/cases-377

Murphy, M. (2019, March 10). Dr Google will see you now: Search giant wants to cash in on your medical queries. *The Telegraph*. https://www.telegraph.co.uk/technology/2019/03/10/google-sifting-one-billion-health-questions-day/

Narayanan, A., & Reisman, D. (2017). The Princeton Web Transparency and Accountability Project. In T. Cerquitelli, D. Quercia, & F. Pasquale (Eds.), *Transparent Data Mining for Big and Small Data* (*Vol. 32*, pp. 45–67). Springer, Cham. https://doi.org/10.1007/978-3-319-54024-5_3

National Academies of Sciences, Engineering, Medicine. (2018). *Assessing and Responding to the Growth of Computer Science Undergraduate Enrollments* (p. 24926). The National Academies Press. https://doi.org/10.17226/24926

Naughton, J. (1999). *A Brief History of the Future: The Origins of the Internet*. Phoenix.

NewsWhip. (2019). *2019 Guide to Publishing on Facebook*. NewsWhip. https://web.archive.org/web/20190319160555if_/http://go.newswhip.com/rs/647-QQK-704/images/Facebook%20Publishing%202019_Final.pdf

Ng, A. (2021, April 27). *Google Promised Its Contact Tracing App Was Completely Private—But It Wasn't*. https://themarkup.org/privacy/2021/04/27/google-promised-its-contact-tracing-app-was-completely-private-but-it-wasnt

Niemöller, M. (1950). *First They Came...*. CommonLit. https://www.commonlit.org/en/texts/first-they-came

Nix, N., & Dwoskin, E. (2022, August 12). Search warrants for abortion data leave tech companies few options. *Washington Post*. https://www.washingtonpost.com/technology/2022/08/12/nebraska-abortion-case-facebook/

Ohlheiser, A., & Kiros, H. (2022, June 28). *Big Tech remains silent on questions about data privacy in a post-Roe US*. MIT Technology Review. https://www.technologyreview.com/2022/06/28/1055044/big-tech-data-privacy-supreme-court-dobbs-abortion/

Ong, W. J. (1982). *Orality and Literacy: The Technologizing of the Word*. Methuen. http://www.gbv.de/dms/bowker/toc/9780416713701.pdf

Oremus, W. (2021, November 13). *Why Facebook won't let you control your own news feed*. Washington Post. https://www.washingtonpost.com/technology/2021/11/13/facebook-news-feed-algorithm-how-to-turn-it-off/

Owen, M. (2020, June 7). Profile of Apple-Google contact tracing API reveals how project started. *AppleInsider*. https://appleinsider.com/articles/20/06/07/profile-of-apple-google-contact-tracing-api-reveals-how-project-started

Pasquale, F. (2013). Privacy, Antitrust, and Power. *George Mason Law Review*, *20*(4), 1009–1024.

Pasquale, F. (2017a). The Automated Public Sphere. *U of Maryland Legal Studies Research Paper No. 2017-31*. https://papers.ssrn.com/abstract=3067552

Pasquale, F. (2017b, December 6). From Territorial to Functional Sovereignty: The Case of Amazon. *Law and Political Economy Project*. https://lpeproject.org/blog/from-territorial-to-functional-sovereignty-the-case-of-amazon/

PEPP-PT. (2020). *Pan European Privacy Protecting Proximity Tracing: Context and Mission*. https://404a7c52-a26b-421d-a6c6-96c63f2a159a.filesusr.com/ugd/159fc3_878909ad0691448695346b128c6c9302.pdf

Perigo, B. (2022, February 17). *Inside Facebook's African Sweatshop*. Time. https://time.com/6147458/facebook-africa-content-moderation-employee-treatment/

Perri et al. v. Robinhood Markets, Inc. et al., 8:21-cv-00234 (Florida Southern District April 6, 2021). https://unicourt.com/case/pc-db5-perri-et-al-v-robinhood-markets-inc-et-al-867511

Peterson, B. (2020, July 30). Now we know exactly what Jeff Bezos, Mark Zuckerberg, Sundar Pichai and Tim Cook think about before they make a giant startup acquisitions. *Business Insider*. https://www.businessinsider.com/amazon-facebook-google-ceos-mergers-antitrust-documents-acquisitions-2020-7

Pifer, R. (2022, July 25). *Amazon will see you now: Reading between the lines of the One Medical acquisition*. Healthcare Dive. https://www.healthcaredive.com/news/amazon-why-one-medical-acquisition-primary-care/627822/

Piketty, T. (2014). Capital in the Twenty-First Century. In *Capital in the Twenty-First Century*. Belknap Press of Harvard University Press. https://doi.org/10.4159/9780674982918

Pitofsky, R., Anthony, S. F., Thompson, M. W., Swindle, O., & Leary, T. B. (2000). Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress. *Federal Trade Commission*, *35*.

Power, M. (2022). Theorizing the Economy of Traces: From Audit Society to Surveillance Capitalism. *Organization Theory*, *3*(3), 26317877211052296. https://doi.org/10.1177/26317877211052296

Prodhan, G., & Nienaber, M. (2015, June 9). Merkel urges Germans to put aside fear of big data. *Reuters*. https://www.reuters.com/article/us-germany-technology-merkel-idUSKBN0OP2EM20150609

Purcher, J. (2020, April 23). European Commissioner urges Apple's CEO on a Video Conference call to support Europe's "StopCovid" App on the iPhone. *Patently Apple*. https://www.patentlyapple.com/2020/04/european-commissioner-urges-apples-ceo-on-a-video-conference-call-to-support-europes-stopcovid-app-on-the-iphone.html

Puschmann, C. (2019). An end to the wild west of social media research: A response to Axel

Bruns. *Information, Communication & Society*, *22*(11), 1582–1589. https://doi.org/10.1080/1369118X.2019.1646300

Quaker, D. (2022, March 31). *Amazon Stats*. Amazon Selling Partner Blog. https://sell.amazon.com/blog/grow-your-business/amazon-stats-growth-and-sales

Rabkin, J., Basnett, G., Howker, E., Eastham, J., & Pett, H. (2020, September 28). Revealed: Trump campaign strategy to deter millions of Black Americans from voting in 2016. *Channel 4 News*. https://www.channel4.com/news/revealed-trump-campaign-strategy-to-deter-millions-of-black-americans-from-voting-in-2016

Radin, M. J. (1987). Market-Inalienability. *Harvard Law Review*, *100*(8), 1849–1937. https://doi.org/10.2307/1341192

Radin, M. J. (2012). *Boilerplate: The Fine Print, Vanishing Rights, and the Rule of Law*. Princeton University Press. https://doi.org/10.23943/princeton/9780691155333.001.0001

Radjenovic, A., Mańko, R., & Eckert, G. (2020). Coronavirus and elections in selected Member States. *European Parliamentary Research Service*, *11*.

Rahbar, D. H. (2022). Laundering Data: How the Government's Purchase of Commercial Location Data Violates Carpenter and Evades the Fourth Amendment. *Columbia Law Review*, *122*(3), 713–754.

Rahman-Shepherd, A., Clift, C., Ross, E., Hollman, L., Van Der Mark, N., Wakefield, B., Patel, C., & Yates, R. (2021). *Solidarity in Response to the COVID-19 pandemic* (pp. 1–10). Chatham House. https://www.chathamhouse.org/sites/default/files/2021-07/2021-07-14-solidarity-response-covid-19-pandemic-summary-rahman-shepherd-et-al_0_0.pdf

Ramjee, D., Sanderson, P., & Malek, I. (2021). *COVID-19 and Digital Contact Tracing: Regulating the Future of Public Health Surveillance* (SSRN Scholarly Paper No. 3733071). https://doi.org/10.2139/ssrn.3733071

Raskin, R. (2020, July 2). Why Americans Hate Contact Tracing. *Techonomy*. https://techonomy.com/why-americans-hate-contact-tracing/

Rathje, S., Van Bavel, J. J., & van der Linden, S. (2021). Out-group animosity drives engagement on social media. *Proceedings of the National Academy of Sciences*, *118*(26), e2024292118. https://doi.org/10.1073/pnas.2024292118

Reardon, J., Dehaye, P.-O., & Richter, B. (2020, December 4). Proximity Tracing in an Ecosystem of Surveillance Capitalism. *AppCensus Blog*. https://blog.appcensus.io/2020/12/04/proximity-tracing-in-an-ecosystem-of-surveillance-capitalism/

Redlener, I., Sachs, J. D., Hansen, S., & Hupert, N. (2020). *130,000—210,000 Avoidable COVID-19 Deaths—And Counting—In the U.S.* National Center for Disaster Preparedness - Columbia University Earth Institute. https://ncdp.columbia.edu/custom-content/uploads/2020/10/Avoidable-COVID-19-Deaths-US-NCDP.pdf

Reed, J. (2019, August 9). Maria Ressa: 'It would be great if we didn't have to fight our government.' *Financial Times*.

Reed, J. (2022, May 10). Marcos myths lift dictator's son to power in Philippines. *Financial Times*. https://www.ft.com/content/adc60586-9267-43b5-be3b-f44ad4506d2d

Reset Australia. (2022, May 11). *Briefing: How Meta Extorted Australia*. Reset Australia. https://au.reset.tech/news/how-meta-extorted-australia/

Ressa, M., & Muratov, D. (2022). *A 10-point plan to address our information crisis*. People vs. Big Tech. https://peoplevsbig.tech/10-point-plan

Richter, F. (2020, July 9). *Infographic: Apple Leads the Race for AI Domination*. Statista Infographics. https://www.statista.com/chart/9443/ai-acquisitions/

Riemer, K., & Peter, S. (2021). Algorithmic audiencing: Why we need to rethink free speech on social media. *Journal of Information Technology*, *36*(4), 409–426. https://doi.org/10.1177/02683962211013358

Riles, A. (2014). Managing Regulatory Arbitrage: A Conflict of Laws Approach. *Cornell International Law Journal*, *47*, 63–117.

Risse, M. (2021). *The Fourth Generation of Human Rights: Epistemic Rights in Digital Lifeworlds* (HKS Working Paper No. RWP21-027). https://doi.org/10.2139/ssrn.3973946

Roberts, M. (2019, January 31). Opinion | Facebook has declared sovereignty. *Washington Post*. https://www.washingtonpost.com/opinions/2019/01/31/facebook-has-declared-sovereignty/

Roberts, P. (2012, October 4). *FTC Releases Google Privacy Report—Minus The Juicy Details*. The Security Ledger. https://securityledger.com/2012/10/ftc-releases-google-privacy-report-minus-the-juicy-details/

Romm, T. (2020, March 11). White House asks Silicon Valley for help to combat coronavirus, track its spread and stop misinformation. *Washington Post*. https://www.washingtonpost.com/technology/2020/03/11/white-house-tech-meeting-coronavirus/

Romm, T., Dwoskin, E., & Timberg, C. (2020, March 17). U.S. government, tech industry discussing ways to use smartphone location data to combat coronavirus. *Washington Post*. https://www.washingtonpost.com/technology/2020/03/17/white-house-location-data-coronavirus/

Roose, K., & Isaac, M. (2021, February 10). Facebook Dials Down the Politics for Users. *The New York Times*. https://www.nytimes.com/2021/02/10/technology/facebook-reduces-politics-feeds.html

Rosen, J. (2012). The Right to Be Forgotten. *Stanford Law Review Online*, *64*, 88.

Rosenbush, S. (2022, March 8). Big Tech Is Spending Billions on AI Research. Investors Should Keep an Eye Out. *Wall Street Journal*. https://www.wsj.com/articles/big-tech-is-spending-billions-on-ai-research-investors-should-keep-an-eye-out-11646740800

Rozenshtein, A. Z. (2021). Silicon Valley's Speech: Technology Giants and the Deregulatory First Amendment. *Journal of Free Speech Law*, *337*. https://papers.ssrn.com/abstract=3911460

Rubin, A. J. (2015, May 5). Lawmakers in France Move to Vastly Expand Surveillance. *The New York Times*. https://www.nytimes.com/2015/05/06/world/europe/french-legislators-approve-sweeping-intelligence-bill.html

Ryan, J. (2022). *The Biggest Data Breach: ICCL report on scale of Real-Time Bidding data broadcasts in the U.S. and Europe*. Irish Council for Civil Liberties. https://www.iccl.ie/wp-content/uploads/2022/05/Mass-data-breach-of-Europe-and-US-data-1.pdf

Sample, I. (2017, November 2). Big tech firms' AI hiring frenzy leads to brain drain at UK universities. *The Guardian*. https://www.theguardian.com/science/2017/nov/02/big-tech-firms-google-ai-hiring-frenzy-brain-drain-uk-universities

Samuel, S. (2019, August 5). Facebook is building tech to read your mind. The ethical implications are staggering. *Vox*. https://www.vox.com/future-perfect/2019/8/5/20750259/facebook-ai-mind-reading-brain-computer-interface

Santos, F. P., Lelkes, Y., & Levin, S. A. (2021). Link recommendation algorithms and dynamics of polarization in online social networks. *Proceedings of the National Academy of Sciences*, *118*(50). https://doi.org/10.1073/pnas.2102141118

Scheck, J., Purnell, N., & Horwitz, J. (2021, September 16). Facebook Employees Flag Drug Cartels and Human Traffickers. The Company's Response Is Weak, Documents Show. *Wall Street Journal*. https://www.wsj.com/articles/facebook-drug-cartels-human-traffickers-response-is-weak-documents-11631812953

Schmidt, E. (Director). (2018, March 16). *Eric Schmidt HIMSS18 Opening Keynote*. Healthcare Information and Management Systems Society, Inc. https://www.youtube.com/watch?v=ACQes9erfsw

Schmidt, E., & Cohen, J. (2014). *The New Digital Age: Transforming Nations, Businesses, and Our Lives*. Vintage Books.

Schmidt, E., & Kravis, M.-J. (2020). *The Technological Response to COVID-19—Video Conference Transcript*. The Economic Club of New York. https://www.econclubny.org/documents/10184/109144/2020SchmidtTranscript.pdf

Schmidt, E., Work, R. O., Catz, S., Chien, S., Clyburn, M., Darby, C., Ford, K., Griffiths, J.-M., Horvitz, E., Jassy, A., Louie, G., Mark, W., Matheny, J., McFarland, K., & Moore, A. (2019). *NSCAI Interim Report for Congress*. National Security Commission on Artificial Intelligence. https://www.nscai.gov/wp-content/uploads/2021/01/NSCAI-Interim-Report-for-Congress_201911.pdf

Schwartz, P. M. (2012). Systematic government access to private-sector data in Germany. *International Data Privacy Law*, *2*(4), 289–301. https://doi.org/10.1093/idpl/ips026

Scola, N. (2017, October 26). *How Facebook, Google and Twitter "embeds" helped Trump in 2016*. Politico. https://www.politico.com/story/2017/10/26/facebook-google-twitter-trump-244191

Scola, N. (2019, October 17). Zuckerberg defends Facebook's "free expression" in face of Washington hostility. *POLITICO*. https://www.politico.com/news/2019/10/17/mark-zuckerberg-facebook-georgetown-address-050181

Scott, M. (2015, November 18). Europe, Shaken by Paris Attacks, Weighs Security With

Privacy Rights—The New York Times. *New York Times - Bits Blog*. https://web.archive.org/web/20151119015821/https://bits.blogs.nytimes.com/2015/11/18/europe-shaken-by-paris-attacks-weighs-security-with-privacy-rights/

Scott, M., Braun, E., Delcker, J., & Manancourt, V. (2020, May 15). How Google and Apple outflanked governments in the race to build coronavirus apps. *Politico*. https://www.politico.eu/article/google-apple-coronavirus-app-privacy-uk-france-germany/

Searle, J. R. (2010). *Making the Social World: The Structure of Human Civilization*. Oxford University Press.

Sekalala, S., Dagron, S., Forman, L., & Meier, B. M. (2020). Analyzing the Human Rights Impact of Increased Digital Public Health Surveillance during the COVID-19 Crisis. *Health and Human Rights Journal*, *22*(2), 7–20.

Selinger, E., & Durant, D. (2022). Amazon's Ring: Surveillance as a Slippery Slope Service. *Science as Culture*, *31*(1), 92–106. https://doi.org/10.1080/09505431.2021.1983797

Shannon, C. E., & Weaver, W. (1963). *The Mathematical Theory of Communication (first published in 1949)*. University of Illinois Press.

Shapiro, J. (2021, January 27). *Free Speech Fundamentalism*. Inside Higher Ed. https://www.insidehighered.com/views/2021/01/27/academics-should-put-freedom-speech-context-other-values-opinion

Shattuck, J., & Risse, M. (2021). *Reimagining Rights & Responsibilities in the United States: Freedom of Speech and Media* (No. RWP21-004). https://doi.org/10.2139/ssrn.3801268

Shenkman, C., Franklin, S. B., Nojeim, G., & Thakur, D. (2021). *Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers*. Center for Democracy & Technology. https://cdt.org/wp-content/uploads/2021/12/2021-12-08-Legal-Loopholes-and-Data-for-Dollars-Report-final.pdf

Sherman, J., & Morgus, R. (2018, December 5). Authoritarians Are Exporting Surveillance Tech, And With it Their Vision for the Internet. *Council on Foreign Relations - Net Politics*. https://www.cfr.org/blog/authoritarians-are-exporting-surveillance-tech-and-it-their-vision-internet

Siganos, A., Vagenas-Nanos, E., & Verwijmeren, P. (2014). Facebook's daily sentiment and international stock markets. *Journal of Economic Behavior & Organization*, *107*, 730–743. https://doi.org/10.1016/j.jebo.2014.06.004

Silverman, C., & Mac, R. (2020, November 3). Facebook Reduced Traffic To Leading Liberal Pages Just Before The Election. *BuzzFeed News*. https://www.buzzfeednews.com/article/craigsilverman/facebook-cut-traffic-liberal-pages-before-election

Silverman, C., Timberg, C., Kao, J., & Merrill, J. B. (2022, January 4). Facebook groups topped 10,000 daily attacks on election before Jan. 6, analysis shows. *Washington Post*. https://www.washingtonpost.com/technology/2022/01/04/facebook-election-misinformation-capitol-riot/

Simon, F., Howard, P. N., & Nielsen, R. K. (2020, April 7). *Types, sources, and claims of COVID-19 misinformation*. Reuters Institute for the Study of Journalism. https://reutersinstitute.politics.ox.ac.uk/types-sources-and-claims-covid-19-misinformation

Singer, N. (2020, July 8). Virus-Tracing Apps Are Rife With Problems. Governments Are Rushing to Fix Them. *The New York Times*. https://www.nytimes.com/2020/07/08/technology/virus-tracing-apps-privacy.html

Smyth, J. (2021a, February 14). Nine Entertainment urges Australian MPs to ignore Big Tech threats over news code. *Financial Times*. https://www.ft.com/content/7505a222-30d9-4ba3-b2fb-48ff4daafe80

Smyth, J. (2021b, February 19). Facebook 'behaving like North Korea' as Australia wakes up to news ban. *Financial Times*. https://www.ft.com/content/9e519b57-4e48-4221-9622-facd83cd0e42

Smyth, J., Murphy, H., & Barker, A. (2021, February 18). Facebook ban on news in Australia provokes fierce backlash. *Financial Times*. https://www.ft.com/content/cac1ff54-b976-4ae4-b810-46c29ab26096

Snowden, E. (2019). *Permanent Record*. Henry Holt and Company.

Soni, J., & Goodman, R. (2018). *A Mind at Play: How Claude Shannon Invented the Information Age*. Simon & Schuster. https://www.simonandschuster.com/books/A-Mind-at-Play/Jimmy-Soni/9781476766690

Sontani, A., Calo, R., & Bergstrom, C. (2020, April 27). Contact-tracing apps are not a solution to the COVID-19 crisis. *Brookings*. https://www.brookings.edu/techstream/inaccurate-and-insecure-why-contact-tracing-apps-could-be-a-disaster/

Srinivasan, D. (2019). The Antitrust Case against Facebook: A Monopolist's Journey towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy. *Berkeley Business Law Journal*, *16*(1), 39–101.

Statt, N. (2019, April 30). Facebook CEO Mark Zuckerberg says the "future is private." *The Verge*. https://www.theverge.com/2019/4/30/18524188/facebook-f8-keynote-mark-zuckerberg-privacy-future-2019

Stock, B. (1983). *The Implications of Literacy: Written Language and Models of Interpretation in the Eleventh and Twelfth Centuries*. Princeton University Press. http://hdl.handle.net/2027/heb.01528

Stoto, M. A. (2008). Public Health Surveillance in the Twenty-First Century: Achieving Population Health Goals While Protecting Individuals' Privacy and Confidentiality. *Georgetown Law Journal*, *96*(703). https://heinonline.org/HOL/Page?handle=hein.journals/glj96&id=706&div=&collection=

Stowell, J., & Ramos, C. (2019, November 15). Curie subsea cable set to transmit to Chile, with a pit stop to Panama. *Google Cloud [blog]*. https://cloud.google.com/blog/products/infrastructure/curie-subsea-cable-set-to-transmit-to-chile-with-a-pit-stop-to-panama

Stroud, N. J., Scacco, J., & Curry, A. (2014). *Analysis of News Sites*. Center for Media Engagement. https://mediaengagement.org/research/news-site-analysis/

Suliman, A. (2022, January 29). Joni Mitchell pulls music from Spotify in stand with Neil Young against covid misinformation. *The Washington Post*. https://www.washingtonpost.com/arts-entertainment/2022/01/29/joni-mitchell-spotify-covid-rogan/

Summers, L. H. (2006, November 19). The Great Liberator. *The New York Times*. https://www.nytimes.com/2006/11/19/opinion/19summers.html

Swire, P. (2013). The Second Wave of Global Privacy Protection: Symposium Introduction. *Ohio State Law Journal*, *74*(6). https://kb.osu.edu/handle/1811/71601

Tech Transparency Project. (2022, May 25). Eric Schmidt's Hidden Influence Over US Defense Spending. *Tech Transparency Project*. https://www.techtransparencyproject.org/articles/eric-schmidts-unseen-influence-over-us-defense-spending

Terry, N. P. (2016). *Big Data and Regulatory Arbitrage in Health Care* (No. 2821964). SSRN Scholarly Paper. https://papers.ssrn.com/abstract=2821964

Terry, N. P. (2017). Regulatory Disruption and Arbitrage in Health-Care Data Protection. *Yale Journal of Health Policy, Law and Ethics*, *17*, 143.

The People's Declaration. (n.d.). The People's Declaration. https://www.peoplesdeclaration.net

The White House. (2019, February 11). *Artificial Intelligence for the American People*. The White House. https://web.archive.org/web/20190321000750/https://www.whitehouse.gov/ai/executive-order-ai/

Thompson, N. (2018, February 12). Inside Facebook's Two Years of Hell. *Wired*. https://www.wired.com/story/inside-facebook-mark-zuckerberg-2-years-of-hell/

Timberg, C. (2020, February 20). How conservatives learned to wield power inside Facebook. *Washington Post*. https://www.washingtonpost.com/technology/2020/02/20/facebook-republican-shift/

Timberg, C., & Harwell, D. (2020, March 19). Government efforts to track virus through phone location data complicated by privacy concerns. *Washington Post*. https://www.washingtonpost.com/technology/2020/03/19/privacy-coronavirus-phone-data/

Tobin, B. (2022, June 9). A top Walmart exec shares why it's outperforming Amazon in selling customer data while turning the business into a key revenue stream for the retailer. *Business Insider*. https://www.businessinsider.com/walmart-thinks-it's-beating-amazon-in-monetizing-customer-data-2022-6

Tokita, C. K., Guess, A. M., & Tarnita, C. E. (2021). Polarized information ecosystems can reorganize social networks via information cascades. *Proceedings of the National Academy of Sciences*, *118*(50), e2102147118. https://doi.org/10.1073/pnas.2102147118

Tribe, L. (2021, May 11). First Amendment fantasies in the social media debate. *The Hill*. https://thehill.com/opinion/technology/552735

-laurence-tribe-first-amendment-fantasies-in-the-social-media-debate

Tromble, R. (2021). Where Have All the Data Gone? A Critical Reflection on Academic Digital Research in the Post-API Age. *Social Media + Society*, *7*(1), 2056305121988929. https://doi.org/10.1177/2056305121988929

Troncoso, C. (2021). *Contact Tracing Apps: Engineering Privacy in Quicksand*. EPFL. https://www.usenix.org/sites/default/files/conference/protected-files/enigma2021_slides_troncoso.pdf

Troncoso, C., Payer, M., Hubaux, J.-P., Salathé, M., Larus, J., Bugnion, E., Lueks, W., Stadler, T., Pyrgelis, A., Antonioli, D., Barman, L., Chatel, S., Paterson, K., Capkun, S., Basin, D., Beutel, J., Jackson, D., Preneel, B., Smart, N., ... Boneh, D. (2020a). *DP3T - Decentralized Privacy-Preserving Proximity Tracing: Overview of Data Protection and Security*. Github. https://github.com/DP-3T/documents/blob/08e9c145dabfe26907afd66e0973aceb4e4b44f7/DP3T%20-%20Data%20Protection%20and%20Security.pdf

Troncoso, C., Payer, M., Hubaux, J.-P., Salathé, M., Larus, J., Bugnion, E., Lueks, W., Stadler, T., Pyrgelis, A., Antonioli, D., Barman, L., Chatel, S., Paterson, K., Capkun, S., Basin, D., Beutel, J., Jackson, D., Preneel, B., Smart, N., ... Boneh, D. (2020b). *DP3T - Decentralized Privacy-Preserving Proximity Tracing: README*. Github. https://github.com/DP-3T/documents/blob/08e9c145dabfe26907afd66e0973aceb4e4b44f7/README.md

Troncoso, C., Payer, M., Hubaux, J.-P., Salathé, M., Larus, J., Bugnion, E., Lueks, W., Stadler, T., Pyrgelis, A., Antonioli, D., Barman, L., Chatel, S., Paterson, K., Capkun, S., Basin, D., Beutel, J., Jackson, D., Preneel, B., Smart, N., ... Boneh, D. (2020c). *DP3T - Decentralized Privacy-Preserving Proximity Tracing: Simplified Overview*. Github. https://raw.githubusercontent.com/DP-3T/documents/master/DP3T%20-%20Simplified%20Three%20Page%20Brief.pdf

Troncoso, C., Payer, M., Hubaux, J.-P., Salathé, M., Larus, J., Bugnion, E., Lueks, W., Stadler, T., Pyrgelis, A., Antonioli, D., Barman, L., Chatel, S., Paterson, K., Capkun, S., Basin, D., Beutel, J., Jackson, D., Preneel, B., Smart, N., ... Boneh, D. (2020d). *DP3T - Decentralized Privacy-Preserving Proximity Tracing—Overview of Data Protection and Security*. Github. https://github.com/DP-3T/documents/blob/master/DP3T%20-%20Data%20Protection%20and%20Security.pdf

Tuohy, J. P. (2022, January 3). This new light bulb from Sengled can tell if you are sleeping. *The Verge*. https://www.theverge.com/2022/1/3/22864783/sengled-smart-health-monitoring-smart-bulb-ces2022

Turner, F. (2006). *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism*. University of Chicago Press.

Tutt, A. (2014). The Revisability Principle. *Hastings Law Journal*, *66*(1113). http://dx.doi.org/10.2139/ssrn.2489718

US Accountability Office. (2021, September 9). *Exposure Notification: Benefits and Challenges of Smartphone Applications to Augment Contact Tracing - Full Report*. US Government Accountability Office. https://www.gao.gov/assets/gao-21-104622.pdf

US District Court—San Francisco. (2019). *Facebook, Inc Consumer Privacy Litigation NO. 18-MD-02843 VC - Transcript of Proceedings*. https://www.documentcloud.org/documents/6153329-05-29-2019-Facebook-Inc-Consumer-Privacy.html

US Senate Committee on Commerce, Science, & Transportation. (2016, May 10). Thune Seeks Answers from Facebook on Political Manipulation Allegations. *US Senate Committee on Commerce, Science, & Transportation*. https://www.commerce.senate.gov/2016/5/thune-seeks-answers-from-facebook-on-political-manipulation-allegations

US Supreme Court. (1967, May 29). *WARDEN, MARYLAND PENITENTIARY, Petitioner, v. Bennie Joe HAYDEN*. Cornell Law School - Legal Information Institute. https://www.law.cornell.edu/supremecourt/text/387/294

Vasconcelos, V. V., Constantino, S. M., Dannenberg, A., Lumkowsky, M., Weber, E., & Levin, S. (2021). Segregation and clustering of preferences erode socially beneficial coordination. *Proceedings of the National Academy of Sciences*, *118*(50), e2102153118. https://doi.org/10.1073/pnas.2102153118

Vaudenay, S. (2020). *Centralized or Decentralized? The Contact Tracing Dilemma* (No. 2020/531; Cryptology EPrint Archive). EPFL. https://infoscience.epfl.ch/record/277809

Vaudenay, S., & Vuagnoux, M. (2022, February 22). *The Dark Side of SwissCovid*. EPFL - Serge Vaudenay's Staff Page. https://lasec.epfl.ch/people/vaudenay/swisscovid.html

Vincent, E. M., Théro, H., & Shabayek, S. (2022). Measuring the effect of Facebook's downranking interventions against groups and websites that repeatedly share misinformation. *Harvard Kennedy School Misinformation Review*. https://doi.org/10.37016/mr-2020-100

VIScon (Director). (2020, October 9). *Building a Contact Tracing App for Switzerland | Kenny Paterson | ETH Zürich*. VIScon. https://www.youtube.com/watch?v=20kHvbsej-w

Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science*, *359*(6380), 1146–1151. https://doi.org/10.1126/science.aap9559

Voss, W. G. (2016). After Google Spain and Charlie Hebdo: The Continuing Evolution of European Union Data Privacy Law in a Time of Change. *Business Lawyer*, *71*(1). https://papers.ssrn.com/abstract=2711996

Vought, R. T. (2020). *Guidance for Regulation of Artificial Intelligence Applications*. The White House. https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/11/M-21-06.pdf

Wacquant, L. (2012). Three steps to a historical anthropology of actually existing neoliberalism. *Social Anthropology/Anthropologie Sociale*, *20*(1), 66–79. https://doi.org/10.1111/j.1469-8676.2011.00189.x

Waddell, K. (2018, September 6). A feud atop AI's commanding heights. *Axios*. https://www.axios.com/academia-corporate-research-ai-9d525070-303d-47fd-b822-0fbffcac6740.html

Wall Street Journal (Director). (2021a, September 18). The Facebook Files, Part 4: The Outrage Algorithm. In *The Journal*. WSJ Podcasts. https://www.wsj.com/podcasts/the-journal/the-facebook-files-part-4-the-outrage-algorithm/e619fbb7-43b0-485b-877f-18a98ffa773f

Wall Street Journal. (2021b, October 1). The Facebook Files. *Wall Street Journal*. https://www.wsj.com/articles/the-facebook-files-11631713039

Waller, A., & Lecher, C. (2022, May 12). *Facebook Promised to Remove "Sensitive" Ads. Here's What It Left Behind*. The Markup. https://themarkup.org/citizen-browser/2022/05/12/facebook-promised-to-remove-sensitive-ads-heres-what-it-left-behind

Ward, P. A. (2022). When the Soapbox Talks: Platforms as Public Utilities. *Wisconsin Law Review*, *2022*(1). https://wlr.law.wisc.edu/volume-2022-no-1/

Warrell, H., Neville, S., & Bradshaw, T. (2020, June 18). UK to replace contact-tracing app with Apple and Google model. *Financial Times*. https://www.ft.com/content/819ff491-0ae9-4359-b3db-ed8de48330d7

Waters, R. (2022, May 19). Microsoft woos Brussels as battle over the cloud intensifies. *Financial Times*.

Wellcome. (2019). *Wellcome Global Monitor—First Wave Findings 2018*. Gallup. https://wellcome.org/sites/default/files/wellcome-global-monitor-2018.pdf

Whistleblower Aid. (2022, May 5). *New Disclosure Exposes Facebook's Dangerous Campaign to Exert Leverage over Lawmaking Process*. Whistleblower Aid. https://whistleboweraid.org/blog/australia-facebook-press-release/

Wiewiórowski, W. R. (2020, March 25). *Monitoring spread of COVID-19* [Letter to Roberto Viola]. https://edps.europa.eu/sites/edp/files/publication/20-03-25_edps_comments_concerning_covid-19_monitoring_of_spread_en.pdf

Wilson, S. L., & Wiysonge, C. (2020). Social media and vaccine hesitancy. *BMJ Global Health*, *5*(10), e004206. https://doi.org/10.1136/bmjgh-2020-004206

Wong, J. C. (2021, April 12). How Facebook let fake engagement distort global politics: A whistleblower's account. *The Guardian*. https://www.theguardian.com/technology/2021/apr/12/facebook-fake-engagement-whistleblower-sophie-zhang

Work, B. (2015, January 28). *The Third U.S. Offset Strategy and its Implications for Partners and Allies*. https://www.defense.gov/News/Speeches/Speech/Article/606641/the-third-us-offset-strategy-and-its-implications-for-partners-and-allies/

World Health Organization. (2020). *Novel Coronavirus (2019-nCoV)* (Situation Report-13). World Health Organization. https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200202-sitrep-13-ncov-v3.pdf?sfvrsn=195f4010_6

Wu, T. (2017, September 1). *Is the First Amendment Obsolete?* Knight First Amendment Institute at Columbia University. http://knightcolumbia.org/content/tim-wu-first-amendment-obsolete

Wuerthele, M. (2020, April 10). *Apple, Google team on "contact tracing" smartphone software to combat spread of COVID-19*. AppleInsider. https://appleinsider.com/articles/20/04/10/apple-google-partner-on-contact-tracing-to-combat-covid-19-spread

Yan, W. (2020, May 17). The U.S. Is Building A Contact-Tracer Army. *HuffPost*. https://www.huffpost.com/entry/coronavirus-contact-tracers_n_5ebd9dc1c5b66e2790db1035

Zakrzewski, C., Verma, P., & Parker, C. (2022, July 3). Texts, web searches about abortion have been used to prosecute women. *Washington Post*. https://www.washingtonpost.com/technology/2022/07/03/abortion-data-privacy-prosecution/

Zekavat, S. (Reza), Buehrer, R. M., Durgin, G. D., Lovisolo, L., Wang, Z., Goh, S. T., & Ghasemi, A. (2021). An Overview on Position Location: Past, Present, Future. *International Journal of Wireless Information Networks*, *28*, 45–76. https://doi.org/10.1007/s10776-021-00504-z

Zhang, D., Maslej, N., Brynjolfsson, E., Etchemendy, J., Lyons, T., Manyika, J., Ngo, H., Niebles, J. C., Sellitto, M., Sakhaee, E., Shoham, Y., Clark, J., & Perrault, R. (2022). *The AI Index 2022 Annual Report*. AI Index Steering Committee, Stanford Institute for Human-Centered AI, Stanford University. https://aiindex.stanford.edu/wp-content/uploads/2022/03/2022-AI-Index-Report_Master.pdf

Zoltán, K. (2020, March 24). Hungary's Coronavirus Bill—Orbán's bid for absolute power? *Index*. https://index.hu/english/2020/03/24/hungary_coronavirus_bill_viktor_orban_fidesz_sweeping_powers_indefinite_term/

Zuboff, S. (1988). *In the age of the smart machine: The future of work and power*. Basic Books.

Zuboff, S. (2013, June 25). The Surveillance Paradigm: Be the friction - Our Response to the New Lords of the Ring. *FAZ.NET*. https://www.faz.net/aktuell/feuilleton/the-surveillance-paradigm-be-the-friction-our-response-to-the-new-lords-of-the-ring-12241996.html

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*(1), 75–89. https://doi.org/10.1057/jit.2015.5

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.

Author biography

Shoshana Zuboff's most recent book is The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. She is the Charles Edward Wilson Professor Emeritus at the Harvard Business School, a Faculty Associate at the Harvard Kennedy School's Carr Center for Human Rights, and the Co-chair of the Prefiguration Committee of the International Observatory on Information and Democracy.