8

Caveat Usor: Surveillance Capitalism as Epistemic Inequality

Shoshana Zuboff

Somebody take me home
While I still believe
While the pines are still the pines
And there's something left of me

Philip Roebuck
"Somebody Take Me Home"

The world suffers under a dictatorship of no alternatives. Although ideas all by themselves are powerless to overthrow this dictatorship we cannot overthrow it without ideas.
Roberto Unger, The Dictatorship of No Alternatives

I. WHO KNOWS?

On August 9, 2011 the *New York Times* reported that the Spanish Data Protection Agency had chosen to champion the claims of ninety ordinary citizens who were determined to preserve inherited meaning for a world bent on change at the speed of light.[1] In the name of these citizens' "right to be forgotten," the Agency ordered Google to stop indexing contested links pertaining to their pasts.

Each had a unique complaint. One had been terrorized by her former husband and didn't want him to find her address. A middle-aged woman was embarrassed by an old arrest from her days as a university student. An attorney, Mario Costejo González, had suffered the foreclosure of his home years earlier. Although the matter had long been resolved, a Google search of his name continued to deliver links to the foreclosure notice, which, he argued, damaged his reputation.

The Agency concluded that citizens had the right to request the removal of links, and ordered Google to stop indexing the information and to remove existing links to its original sources. Google had unilaterally undertaken to change the rules of the information life cycle, when it decided to crawl, index, and make accessible personal

[1] Suzanne Daley, "On Its Own, Europe Backs Web Privacy Fights," *New York Times*, August 9, 2011, http://www.nytimes.com/2011/08/10/world/europe/10spain.html.

details across the World Wide Web without asking anyone's permission. As a result, information that would normally age had been transformed into a state of perpetual youth and highlighted in the foreground of each person's digital identity. After all, the Spanish Data Protection Agency reasoned, not all information is worthy of immortality. Some information should be forgotten, because that is only human.

Unsurprisingly, Google challenged the Agency's order before the Spanish High Court, which selected Mario Costeja González's case for referral to the Court of Justice of the European Union. On May 13, 2014, after lengthy and dramatic deliberations, the Court of Justice announced its decision to assert the "right to be forgotten" as a fundamental principle of European law.[2]

From the beginning, the case was framed in a peculiar way, pitting "privacy" against an indeterminate open-ended "right to know." As one expert told the *Times*: "Europe sees the need to balance freedom of speech and the right to know against a person's right to privacy or dignity."[3] Three years later when the Court of Justice ruled in favor of Costejo González and his right to be forgotten, Google's then CEO Eric Schmidt repeated that odd juxtaposition. Speaking to his company's shareholders, he characterized the Court's decision as a "balance that was struck wrong" in the "collision between a right to be forgotten and a right to know."[4]

In fact, there was no "balance" that was "struck wrong." The Court's decision was not one of "balancing" two conflicting goods, but rather one of redistributing a single good. The conceptual problem here is that the "right to be forgotten" does not stand in opposition to a "right to know." Rather, it *is* a "right to know." The distinction is critical, because it lifts the veil on a political contest over a new domain of fundamental rights: *epistemic rights*. Such rights confer inalienable entitlements to learning and to knowing. Epistemic rights are the cause of which privacy is the effect. This political contest has been obfuscated to the point of invisibility, despite the fact that its outcome will define the moral and political milieu of our information civilization.

The distribution of epistemic rights determines the degree of epistemic inequality, defined as unequal access to learning imposed by hidden mechanisms of information capture, production, analysis, and control. It is best exemplified in the fast growing abyss between what people can know and what can be known about them. The new axis of epistemic equality/inequality does not reflect what we can earn but rather what we can learn. It represents a focal shift from ownership of "the means of production" to ownership of "the production of meaning."

[2] "Google Spain SL v. Agencia Española de Protección de Datos – (Case C-131/12 (May 13, 2014))," *Harvard Law Review* 128, no. 2 (December 10, 2014): 735.

[3] Daley, "On Its Own, Europe Backs Web Privacy Fights."

[4] James Vincent, "Google Chief Eric Schmidt Says 'Right to Be Forgotten' Ruling Has Got the Balance 'Wrong,'" *Independent*, May 15, 2014, http://www.independent.co.uk/life-style/gadgets-and-tech/google-chief-eric-schmidt-says-right-to-be-forgotten-ruling-has-got-the-balance-wrong-9377231.html.

Epistemic equality depends on epistemic justice, the scope of which is delineated by three essential questions that reflect the nested dilemmas of knowledge, authority, and power: What is the distribution of knowledge? What are the sources of authority that legitimate the distribution of knowledge? What is the power that sustains that authority? Put simply, "Who knows?" "Who decides who knows?" "Who decides who decides who knows?" The answers to these questions determine a society's progress toward epistemic equality.

From this vantage point, one may observe that the real decision faced by the Court of Justice was not one of balancing "privacy" against a "right to know," but rather about the just distribution of epistemic rights. It asked, "Who has the right to know about one's past and in what degree?" The Court judged whether an inalienable right to learn and to know about an individual's past adhered primarily to the individual or to Google. What dismayed Schmidt was that the Court rejected Google's self-authorized claim to a totality of epistemic rights and instead distributed this "right to know about one's past" in a new pattern.

The Court's decision answered the three essential questions. First, it privileged the individual with the right to learning and knowledge about one's own past. Second, it created a juridical "right to be forgotten" that stands as the source of legitimate authority. Third, it was to be Europe's democratic institutions and their power to govern through the rule of law that sustain this authority – not the private power of a corporation.

The primacy of epistemic rights as the cause of privacy was implied in Justice William O. Douglas's 1967 dissenting opinion in the Fourth Amendment case, *Warden v. Hayden*:

> Privacy involves the choice of the individual to disclose or to reveal what he believes, what he thinks, what he possesses .... 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.[5]

In Douglas's formulation, privacy is contingent on the individual's sovereign right to self/knowledge, a right that confers the ability to choose whether to disclose or withhold such knowledge, to what degree, and for what purpose. This choice has been an elemental right throughout most of human history. By "elemental," I mean to mark a distinction between, on the one hand, tacit rights that are given under the conditions of human existence, and, on the other, juridical rights codified in law.

Others have addressed this distinction, and linguistic philosopher John Searle's "pragmatic considerations of the formulation of rights" are useful here.[6] Searle argues that elemental conditions of existence are crystallized as formal human rights

[5] Justice William O. Douglas, Dissent, Warden v Hayden, 387 U.S. 294, 1967. https://www.law.cornell.edu/supremecourt/text/387/294#writing-USSC_CR_0387_0294_ZD

[6] John R. Searle, *Making the Social World: The Structure of Human Civilization* (New York: Oxford University Press, 2010), pp. 194–95.

only at that moment in history when they come under systematic threat. For example, the ability to speak is an elemental right born of an elemental 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 not 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."

As is the case with all elemental rights, many epistemic rights have not yet been codified into law for the simple reason that it has not been necessary to do so. The epistemic "right to be forgotten," for example, has always existed as an irreducible element of human experience. In a preliterate world no one needed a legal right to be forgotten when the primary record of the past was memory. One lives, one ages, and memories age too. The past is hazy, fragmented, dispersed, prismatic, and then drifts into some combination of oblivion, stories, and myth.

In traditional society, the past was preserved in ritual, and in the modern era it is technology. The printing press and widespread literacy, photography, voice recording – each made it easier to convey one's past to the next generation, chipping away at oblivion. With these inventions, elemental epistemic rights began their migration toward formal codification. For example, Justice Brandeis was moved to formalize the right to privacy, motivated in part by the invasiveness of the newspaperman's camera, as it bestowed an independent life on anyone's face, far from the elemental rights of the subject before she was framed in the camera's lens. As if in anticipation of Searle, Brandeis wrote:

> That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society.[7]

In retrospect, Brandeis's indignation aimed at the journalist's camera recalls the last stages of an infinitely long age of epistemic innocence that ended decisively over the last three decades, as the "digital tornado" abruptly transformed the conditions of existence for many twenty-first century humans. In 1986, just 1 percent of the world's capacity to store information was in digital format; 25 percent in 2000. The year 2002 was the tipping point, when more information was stored on digital than on analogue storage devices. By 2007 digitalization had exploded to 97 percent and

[7] Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," *Harvard Law Review* 4, No. 5. (December 15, 1890): 204.

by 2020 the shift was largely complete.[8] Information scholar Martin Hilbert and his colleagues observe that even the foundational elements of civilization, including "language, cultural assets, traditions, institutions, rules, and laws . . . are currently being digitized, and for the first time, explicitly put into visible code," then returned to society through the filter of "intelligent algorithms" deployed to govern a rapidly multiplying range of commercial, governmental, and social functions.[9]

Google Inc. was a product of, driving force in, and beneficiary of this sudden sweeping change. The digitalization of everything produced vast new information territories, planetary in scope, and once celebrated by Eric Schmidt as "the world's largest ungoverned space."[10] By 2002, Google was well on its way to elaborating a new economic logic that I have called *surveillance capitalism*, whose novel imperatives compelled it to hunt and capture ever more dimensions of once private experience as raw material for newly invented processes of datafication, production, and sales. Google was not alone. The vast lawless regions of the digital became the landscape in which companies and governments ruthlessly battle for information dominance, reenacting earlier epochs of invasion, conquest, and empire building in the physical world.

In order to achieve their objectives, the leading surveillance capitalists sought to establish unrivaled dominance over the totality of the world's information now rendered in digital format.[11] Their complex supply chains require hyperscale operations capable of storing and processing vast data flows. Surveillance capital has built most of the world's largest computer networks, data centers, populations of servers, undersea transmission cables, advanced microchips, and frontier machine intelligence, igniting an arms race for the 10,000 or so specialists on the planet who know how to coax knowledge from these vast new data continents.[12]

With Google in the lead, the top surveillance capitalists seek to control labor markets in critical expertise including data science and animal research, elbowing

[8] Martin Hilbert, "How Much Information Is There in the 'Information Society'?" *Significance* 9, no. 4 (August 1, 2012): 8–12, http://onlinelibrary.wiley.com/doi/10.1111/j.1740–9713.2012.00584.x/abstract; Michael R. Gillings, Martin Hilbert, and Darrell J. Kemp, "Information in the Biosphere: Biological and Digital Worlds," *Trends in Ecology & Evolution* 31, no. 3 (March 1, 2016): 180–89, http://www.sciencedirect.com/science/article/pii/S0169534715003249. Martin Hilbert, "Big Data for Development: From Information – to Knowledge Societies," *United Nations ECLAC Report*, 2013, https://doi.org/10.2139/ssrn.2205145.

[9] Gillings, Hilbert, and Kemp, "Information in the Biosphere."

[10] Eric Schmidt and Jared Cohen, *The New Digital Age: Transforming Nations, Businesses, and Our Lives* (New York: Vintage Books, A Division of Random House LLC, 2014).

[11] Hilbert, "How Much Information Is There in the 'Information Society'?"

[12] João Marques Lima, "Hyperscalers Taking over the World at an Unprecedented Scale," *Data Economy* (blog), April 11, 2017, https://data-economy.com/hyperscalers-taking-world-unprecedented-scale/; Cade Metz, "Building an AI Chip Saved Google from Building a Dozen New Data Centers," *Wired*, April 5, 2017, https://www.wired.com/2017/04/building-ai-chip-saved-google-building-dozen-new-data-centers/; Cade Metz, "Tech Giants Are Paying Huge Salaries for Scarce A.I. Talent," *New York Times*, October 22, 2017, sec. Technology, https://www.nytimes.com/2017/10/22/technology/artificial-intelligence-experts-salaries.html.

out competitors such as start-ups, universities, high schools, municipalities, state and federal government agencies, established corporations in other industries and less wealthy countries. In 2016, 57 percent of American computer science Ph.D. graduates took jobs in industry, while only 11 percent became tenure-track faculty. With so few teaching faculty, colleges and universities have had to ration computer science enrollments, which has significantly disrupted the knowledge transfer between generations. It's not just an American problem. In Britain, university administrators contemplate a "missing generation" of data scientists. A Canadian scientist laments, "the power, the expertise, the data are all concentrated in the hands of a few companies."[13]

Under these unprecedented conditions, elemental epistemic rights can no longer be taken for granted. It's not that such rights are eliminated. Rather, they fall to hidden powers – commandeered, stolen, redistributed, cornered, and hoarded.

More than 600 years ago the printing press put the written word into the hands of ordinary people, bypassing the priesthood, rescuing the prayers, and delivering spiritual communion directly into the hands of the prayerful. It was perhaps the first great event in the annals of technological disintermediation, removing the "middleman" in favor of a direct line to the end consumer.

The Internet was welcomed as an equally fearsome force of empowerment: the ultimate disintermediator, amplifying Gutenberg's revolution as it liberates information from the old institutions and distributes it directly to the people. Thanks to the mighty powers of the digital, corporations would no longer decide the music people buy, the news they read, the knowledge they access, or the goods and services they enjoy.

Celebration distracted from a parallel development that moved in stealth just beyond the sightlines as the Internet became a Trojan horse for a novel economics that would eventually infiltrate every aspect of peoples' lives. The shooting star of disintermediation quickly faded, leaving in its wake the secretive new middleman, that is, surveillance capitalism, which quietly remediated the relationship to all things digital. The result has been that the Internet is not ungoverned. Rather, it is owned and operated by this dark economic logic and wholly subject to its iron laws.

The digital century was to have been democracy's Golden Age. Instead, many societies enter the third decade of the twenty-first century marked by an extremely

[13] Madhumita Murgia, "AI Academics under Pressure to Do Commercial Research," *Financial Times*, March 13, 2019, https://www.ft.com/content/94e86cd0-44b6-11e9-a965-23d669740bfb; Sarah McBride and Ashlee Vance, "Apple, Google, and Facebook Are Raiding Animal Research Labs," *Bloomberg.com*, June 18, 2019, https://www.bloomberg.com/news/features/2019–06-18/apple-google-and-facebook-are-raiding-animal-research-labs; Committee on the Growth of Computer Science Undergraduate Enrollments et al., *Assessing and Responding to the Growth of Computer Science Undergraduate Enrollments* (Washington, DC: National Academies Press, 2018), https://doi.org/10.17226/24926; Michael Gofman and Zhao Jin, "Artificial Intelligence, Human Capital, and Innovation," August 20, 2019, 55; Ian Sample, "Big Tech Firms' AI Hiring Frenzy Leads to Brain Drain at UK Universities," *Guardian*, November 2, 2017, sec. Science, http://www.theguardian.com/science/2017/nov/02/big-tech-firms-google-ai-hiring-frenzy-brain-drain-uk-universities.

new form of social inequality that threatens to remake the social order as it unmakes democracy. A new age of epistemic inequality has dawned in which individuals' inalienable rights to learning and knowing about one's own life must be codified in law if they are to exist at all.

Unequal knowledge about us produces unequal power over us, turning epistemic inequality into a critical zone of social contest in our time. Twentieth-century industrial society was based on a division of labor, and it followed that the struggle for economic equality would shape the politics of that age. Our digital century shifts society's coordinates from a division of labor to a division of learning, and it follows that the struggle for epistemic equality will shape the politics of this age.

In redistributing the "right to be forgotten" to individuals, the European Court of Justice declared that Google's was not to be the last word on the human or the digital future. It asserted that decisive authority must rest with the people, their laws, and their democratic institutions, even in the face of a great private power. It was to be the beginning, not the end, of a bitter struggle over the fundamental rights that will define the digital future.

The remainder of this chapter explores the iron laws of this private power, their consequences for people and the democratic polis, the historical significance of this struggle, and its remedies.

II. WHAT IS SURVEILLANCE CAPITALISM?

It has long been understood that capitalism evolves by claiming things that exist outside of the market dynamic and turning them into market commodities for sale and purchase. In historian Karl Polanyi's 1944 grand narrative of the "great transformation" to a self-regulating market economy, he described the origins of this translation process in three astonishing and crucial mental inventions that he called "commodity fictions." The first was that human life could be subordinated to market dynamics and reborn as "labor" to be bought and sold. The second was that nature could be translated into the market and reborn as "land" or "real estate." The third was that exchange could be reborn as "money."[14]

Surveillance capitalism originates in an even more startling mental invention, declaring private human experience as free raw material for translation into production and sales. Once private human experience is claimed for the market, it is translated into behavioral data for computational production.

Early on, it was discovered that, unknown to users, even data freely given harbor rich predictive signals, a surplus that is more than what is required for service improvement. It isn't only what you post online, but whether you use exclamation points or the color saturation of your photos; not just where you walk but the stoop of

[14] Karl Polanyi, *The Great Transformation: The Political and Economic Origins of Our Time* (Boston, MA: Beacon Press, 2001), pp. 75–76.

your shoulders; not just the identity of your face but the emotional states conveyed by your "micro-expressions"; not just what you like but the pattern of likes across engagements. Soon this behavioral surplus was covertly hunted and captured across virtual and real worlds, accessible to the always-on ubiquitous digital architecture that I call "Big Other" and claimed as proprietary data.

Behavioral surplus is ultimately conveyed through complex supply chains of devices, tracking and monitoring software, and ecosystems of apps and companies that specialize in niche data flows captured in secret.[15] Data flows empty into surveillance capitalists' computational factories, called "artificial intelligence," where they are manufactured into behavioral predictions. A leaked 2018 Facebook document provides some insight into factory operations.[16] Facebook's "prediction engine" is built on a machine intelligence platform called "FB Learner Flow," which the company describes as its "AI backbone" and the key to "personalized experiences" that deliver "the most relevant content." The machine learning system "ingests trillions of data points every day, trains thousands of models – either offline or in real time – and then deploys them to the server fleet for live predictions." The company explains that, "since its inception, more than a million models have been trained, and our prediction service has grown to make more than 6 million predictions per second."[17]

Finally, these prediction products are rapidly swept up into the life of the market, traded in newly constituted marketplaces for behavioral predictions: human futures markets. These markets link surveillance capitalists to business customers with a keen interest in the future behavior of current and potential "users" or consumers. Certainty in human affairs is the lifeblood of these markets, where surveillance capitalists compete on the quality of their predictions, which are about individuals but are not for individuals. Surveillance capitalists have grown immensely wealthy from these trading operations, as many companies are eager to lay bets on future human behavior.

Surveillance capitalism was invented as the solution to financial emergency in the teeth of the dot.com bust when the fledgling company called Google faced the loss of investor confidence. As pressure mounted, Google's leaders decided to boost ad revenue by using their exclusive access to user data logs, in combination with their

[15] Sam Schechner and Mark Secada, "You Give Apps Sensitive Personal Information. Then They Tell Facebook.," *Wall Street Journal*, February 22, 2019, sec. Tech, https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636; "Out of Control: How Consumers Are Exploited by the Online Advertising Industry" (Forbruker Rådet, January 14, 2020), https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020–01-14-out-of-control-final-version.pdf.

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

[17] "Introducing FBLearner Flow: Facebook's AI Backbone," Facebook Code, May 9, 2016, https://code.facebook.com/posts/1072626246134461/introducing-fblearner-flow-facebook-s-ai-backbone/.

already substantial analytical capabilities and computational power, to fabricate predictions of user click-through rates, regarded as a signal of an ad's relevance.

Operationally, this meant that Google would both repurpose its growing cache of behavioral data, now put to work as a behavioral surplus, and develop methods to aggressively seek new sources of behavioral surplus. According to its own scientists' accounts, the company developed new methods of surplus hunt and capture that were prized for their ability to find data that users intentionally opted to keep private and to infer extensive personal information that users did not or would not provide. This surplus would be analyzed for predictive patterns that could match a specific ad with a specific user. These new operations institutionalized a new logic of accumulation derived from the social relations of the one-way mirror: surveillance. Its mechanisms and methods are carefully engineered to produce user ignorance through obfuscation, undetectability, indecipherability, and misdirection. Success relies on bypassing individual awareness and thus overriding the individual's rights to decide the privacy of one's experience and one's future course of action. Surveillance is essential to the DNA of this market form.

The elements of this economic logic were discovered, invented, elaborated, and deployed at Google from 2000 to 2004, while held in the strictest secrecy. Only when Google went public in 2004 did the world learn that during that period its revenues increased by 3,590%.[18] This increase represents the "surveillance dividend," which raised the bar for attracting investors to the new Internet domain. The shift in the use of behavioral surplus was an historic turning point: the game-changing zero-cost asset that could be diverted from service improvement toward a genuine market exchange. This was not an exchange with "users" but rather with other companies that learned how to profit from low risk bets on users' future behavior.

Surveillance capitalism migrated to Facebook with Google-turned-Facebook executive Sheryl Sandberg and quickly become the default model of information capitalism, attached to nearly every Internet company, start-up, and app. Like an invasive species with no natural predators, its financial prowess quickly overwhelmed the networked sphere, grossly disfiguring the earlier dream of digital technology as an empowering and emancipatory force.

While online advertisers were the dominant players in the early history of the new futures markets, surveillance capitalism is no more restricted to online ad targeting than mass production was restricted to the fabrication of the Model T. Today any actor with an interest in monetizing probabilistic information about behavior can pay to play in a range of human futures markets where behavioral predictions are told and sold.

In a world of highly commoditized products and services, companies now turn to the surveillance dividend as the source of higher margins. The result is whole new

[18] Securities and Exchange Commission, "Amendment No. 9 to Form S-1 Registration Statement under The Securities Act of 1933 for Google Inc.," Securities and Exchange Commission, August 18, 2004, https://www.sec.gov/Archives/edgar/data/1288776/000119312512025336/d260164d10k.htm.

ecosystems of behavioral surplus suppliers, as companies from every sector seek ways to participate in the unilateral dispossession of private experience. Surveillance capitalism now spreads across the "normal" economy in traditionally information intensive sectors such as insurance and finance, but also in healthcare, retail, education, real estate development, and automobiles, to name but a few.

One poignant illustration of these new facts is found in the birthplace of mass production, the Ford Motor Company. One hundred years ago, pioneer capitalists like Ford bent to the revolutionary task of making things at a price that people could afford and shaping a new century of mass consumption. Henry Ford was proud to author the definition of "mass production" for the Encyclopedia Britannica, the Google of his day, describing it as "a productive organization that delivers in quantities a useful commodity of standard material, workmanship, and design, at minimum cost."[19] Ford understood that the mass production revolution was the result, not the cause, of new era of demand in US society – farmers and shopkeepers who wanted automobiles too, but at a price they could afford. "The necessary, precedent condition of mass production is a capacity, latent or developed, of mass consumption," he wrote. "The two go together and in the latter may be traced the reasons for the former."[20] In Ford's cosmos, demand and supply were twinborn, with customers and workers forever linked in a cycle of production and sales that combined low cost goods with consumption-worthy wages immortalized by the five-dollar day.

Had Henry Ford been listening to the Freakonomics Radio podcast in November 2018, he would have learned that his authoritative rendition of supply and demand had been relegated to the dustbin of history by his own distant successor, Jim Hackett. In response to the sustained slump in global auto sales, the company is already cutting thousands of jobs and eliminating models in pursuit of a price-earnings ratio befitting a high tech data company: Hackett wants Ford to become more like Facebook and Google. In this vision, the work of making and selling cars gives way to proprietary monetizable data flows – a "transportation operating system."[21] Hackett wants Henry's company to collect data from the "100 million people . . . that are sitting in Ford blue-oval vehicles . . . . We have as much data in the future coming from vehicles, or from users in those vehicles, or from cities talking to those vehicles, as the other competitors that you and I would be talking about [like Facebook and Google] that have monetizable attraction."

[19] Henry Ford, "Mass Production," in *Encyclopedia Brittannica* (New York, NY: Encyclopedia Britannica, Inc., 1926), http://memory.loc.gov/cgi-bin/query/h?ammem/coolbib:@field(NUMBER+@band(amrlg+lg48)).

[20] Ford.

[21] William Boston, "Ford to Slash Jobs, Shut Plants in Major European Revamp," *Wall Street Journal*, January 10, 2019, sec. Business, https://www.wsj.com/articles/ford-announces-major-european-restructuring-11547117814; Greg Rosalsky, "Can an Industrial Giant Become a Tech Darling? (Ep. 357)," *Freakonomics* (blog), http://freakonomics.com/podcast/ford/.

Once customers are reinvented as data sources, it's easy for Hackett to imagine the next step in which the data that stream from vehicles in real time are combined with Ford's financing data, where, he says, "we already know . . . what people make . . . we know where they work; we know if they're married. We know how long they've lived in their house." Hackett concludes, "And that's the leverage we've got here with the data . . . I think our higher purpose is that the smart vehicle and the smart world have an interaction in the future that's much bigger than it was in the past."[22] As one industry analyst put it, Ford "could make a fortune monetizing data. They won't need engineers, factories, or dealers to do it. It's almost pure profit."[23]

This is where we live now: a world in which nearly every product or service that begins with the word "smart," "personalized," or "connected," from cars to "digital assistants," to devices, appliances, and more, is a supply-chain interface for the unobstructed flow of behavioral surplus. The growth of these connections continuously increases what military strategists call the digital "attack surface," where behavioral surplus is relentlessly tracked, hunted, coaxed, and captured. What began as a solution to financial emergency is now a burgeoning surveillance-based economic order: a surveillance economy. The dominant market form shifts under our gaze: once profits from products, then services, then profits from speculation, and now profits from surveillance.

Surveillance capitalism can no longer be defined as a specific group of corporations, neither can it be conflated with the digital technologies on which it depends. While it is impossible to imagine surveillance capitalism without the digital, it is easy to imagine the digital without surveillance capitalism. The point cannot be emphasized enough: Surveillance capitalism is not technology. Digital technologies can take many forms and have many effects, depending on the social and economic logics that bring them to life. Surveillance capitalism relies on data-gathering devices like computers, phones, sensors, microphones, and cameras. It deploys machine intelligence and platforms. It expresses itself in algorithms. But it is not the same as any of those. Just as an X-ray reveals bone and muscle, but not the soft tissue that binds them, technology is the bone and muscle here, while surveillance capitalism is the soft tissue that binds the elements and directs them into action. It is the shadow that falls over the digital, the hidden pattern that explains how this once emancipatory project transformed people and society into raw material for others' economic gain, as the Internet itself falls to the ownership and operations of surveillance capital.

The phrase "surveillance capitalism" is not arbitrary. Surveillance capitalism's operations are designed for the social relations of the one-way mirror. They know everything about users, but users know nothing about them. Surveillance is baked

[22] Rosalsky, "Can an Industrial Giant Become a Tech Darling?"

[23] Phoebe Wall Howard, "Data Could Be What Ford Sells Next as It Looks for New Revenue," *Detroit Free Press*, November 13, 2018, https://www.freep.com/story/money/cars/2018/11/13/ford-motor-credit-data-new-revenue/1967077002/.

into the DNA of this logic of accumulation, because without it the surveillance dividend as expressed in the revenues, profits, and market capitalization that mark the first two decades of the twenty-first century would have been impossible to achieve.

III. SURVEILLANCE CAPITALISM'S ECONOMIC IMPERATIVES

Surveillance capitalists sell certainty. They compete in human futures markets on the quality of their prediction products, which aim to guarantee outcomes or at least the ever-improving approximation to such guarantees. These guarantees have value, but in the novel logic of surveillance capitalism, their value is a function of markets that bear no organic reciprocities with their populations, now repurposed as the source of unlimited raw material supplies. The competitive dynamics thus set into motion reveal key economic imperatives, and it is these imperatives that compel epistemic inequality, setting surveillance capitalism on a collision course with democracy itself.

First, because predictions must improve in the direction of something like certainty, surplus extraction must move in the direction of something like totality. Machine learning for behavioral prediction wants data in volume and thus economies of scale in data production lay the foundation for all operations.

Once competition for prediction products intensifies, volume is not enough. Surveillance capitalists are compelled to search out ever more predictive sources of behavioral surplus. Machine learning needs volume but also variety, economies of scale but also economies of scope. This realization helped drive the "mobile revolution" sending users into the real world armed with cameras, gyroscopes, and microphones packed inside their smart new pocket-size computers, the ubiquitous interface that conveys surplus supplies to the AI hub. In the competition for scope, surveillance capitalists want your home and what you say and do within its walls.[24] They want your car, your medical conditions, and the shows you stream; your location as well as all the streets and buildings in your path and all the behavior of all the people in your city.[25] They want your voice and what you eat and what you

[24] Jingjing Ren et al., "Information Exposure From Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach," in *Proceedings of the Internet Measurement Conference* (IMC '19: ACM Internet Measurement Conference, Amsterdam Netherlands: ACM, 2019), pp. 267–79, https://doi.org/10.1145/3355369.3355577.

[25] Geoffrey A. Fowler, "What Does Your Car Know about You? We Hacked a Chevy to Find Out," *Washington Post*, December 17, 2019, https://www.washingtonpost.com/technology/2019/12/17/what-does-your-car-know-about-you-we-hacked-chevy-find-out/; Natasha Singer and Daisuke Wakabayashi, "Google to Store and Analyze Millions of Health Records," *New York Times*, November 11, 2019, sec. Business, https://www.nytimes.com/2019/11/11/business/google-ascension-health-data.html; Hooman Mohajeri Moghaddam et al., "Watching You Watch: The Tracking Ecosystem of Over-the-Top TV Streaming Devices," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (CCS '19: 2019 ACM SIGSAC

buy; your children's play time and their schooling; your brainwaves and your bloodstream.[26] Nothing is exempt.[27]

With continued competitive intensification, surveillance capitalists discovered that the most predictive data come from intervening in behavior to tune, herd, and modify action in the direction of commercial objectives. Data scientists describe this as the shift from monitoring to actuation, in which a critical mass of knowledge about a machine system enables the remote control of that system. Now people become targets for remote control, as a third imperative, *economies of action* emerges as an arena of intense experimentation. Here are the practical grounds on which unequal knowledge morphs into unequal power. Epistemic inequality widens to include the distance between what people can do and what can be done to them. "We are learning how to write the music," one data scientist explained, "and then we let the music make them dance."[28]

How shall we understand this new power "to make them dance?" Unlike twentieth-century totalitarianism, it does not employ soldiers and henchmen to threaten terror and murder. It arrives with a cappuccino, not a gun. It is a new *instrumentarian power* that works its will through Big Other's medium of ubiquitous digital instrumentation to manipulate subliminal cues, psychologically target communications, impose choice architectures, trigger social comparison dynamics, and levy rewards and punishments – all of it aimed at remotely tuning, herding, and modifying human

Conference on Computer and Communications Security, London United Kingdom: ACM, 2019), pp. 131–47, https://doi.org/10.1145/3319535.3354198; Stuart A. Thompson and Charlie Warzel, "Twelve Million Phones, One Dataset, Zero Privacy," *New York Times*, December 19, 2019, sec. Opinion, https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html; Ellen P. Goodman and Julia Powles, "Urbanism Under Google: Lessons from Sidewalk Toronto," *Fordham Law Review* 457, no. 88 (December 19, 2019): 42.

[26] Ron Amadeo, "Users Alarmed by Undisclosed Microphone in Nest Security System," *Ars Technica*, February 20, 2019, https://arstechnica.com/gadgets/2019/02/googles-nest-security-system-shipped-with-a-secret-microphone/; Gary Hawkins, "Real-Time Insights on Amazon Prime and Whole Foods Integration," *Winsight Grocery Business*, August 15, 2018, https://www.winsightgrocerybusiness.com/retailers/real-time-insights-amazon-prime-whole-foods-integration; Joel Winston, "Google Keeps an Eye on What You Buy, and It's Not Alone," *Fast Company*, August 6, 2019, https://www.fastcompany.com/90349518/google-keeps-an-eye-on-what-you-buy-and-its-not-alone; Katie Collins, "My Friend Cayla Doll Banned in Germany as 'Espionage Device,'" *CNET*, February 17, 2017, https://www.cnet.com/news/parents-told-to-destroy-connected-dolls-over-hacking-fears/; Betsy Morris, "Schools Wrestle with Privacy of Digital Data Collected on Students," *Wall Street Journal*, July 10, 2019, sec. Tech, https://www.wsj.com/articles/one-parent-is-on-a-mission-to-protect-children-from-digital-mistakes-11562762000; Sigal Samuel, "Brain-Reading Tech Is Coming. The Law Is Not Ready to Protect Us," *Vox*, August 30, 2019, https://www.vox.com/2019/8/30/20835137/facebook-zuckerberg-elon-musk-brain-mind-reading-neuroethics; Kirsten Ostherr, "You Don't Want Facebook Involved with Your Health Care," *Slate*, September 19, 2019, https://slate.com/technology/2019/09/social-determinants-health-facebook-google.html.

[27] Benjamin Romano, "Amazon Rolls Out New Devices amid Swirl of Privacy Questions," *Seattle Times*, September 25, 2019, https://www.seattletimes.com/business/amazon/amazon-rolls-out-new-devices-amid-swirl-of-privacy-questions/.

[28] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: Public Affairs, 2019), p. 295.

behavior in the direction of profitable outcomes and always engineered to preserve users' ignorance.

Although he did not name it, the visionary of ubiquitous computing, Mark Weiser, foresaw the immensity of instrumentarian power as a totalizing social project. He did so in a way that suggests both its utter lack of precedent and the danger of confounding it with what has gone before: "[H]undreds of computers in every room, all capable of sensing people near them and linked by high-speed networks, have the potential to make totalitarianism up to now seem like sheerest anarchy."[29] In fact, all those computers are not the means to a digital totalitarianism. They are, as I think Weiser sensed, the foundation of an unprecedented power that can reshape society in unprecedented ways. If instrumentarian power can make totalitarianism look like anarchy, then what might it have in store for this century?

While all power yearns toward totality, instrumentarian power's specific purposes and methods are not only distinct from totalitarianism but they are in many ways its precise opposite. Instrumentarian power has no principle to instruct, no interest the reformation of the soul. There is no aim toward spiritual salvation, no ideology against which to judge human action. Totalitarianism was a political project that converged with economics to overwhelm society. Instrumentarianism is a market project that converges with the digital to achieve its own unique brand of social domination. Totalitarianism operated through the means of violence, but instrumentarian power operates through the means of behavioral modification.

Instrumentarianism's specific "viewpoint of observation" was forged in the controversial intellectual domain of "radical behaviorism." Thanks to Big Other's capabilities, instrumentarian power reduces human experience to measurable, observable behavior, while remaining profoundly, infinitely, and radically indifferent to the meanings and motives of its targets. Radical indifference produces observation without witness. Instead of an intimate violent political religion, Big Other's way of knowing yields the remote but inescapable presence of impenetrably complex machine systems and the interests that author them, carrying individuals on a fast-moving current to the fulfilment of others' ends. Trained on measurable action, Big Other cares only about observing behavior and ensuring that it is continuously accessible to its ever-evolving operations of monitoring, datafication, calculation, actuation, and monetization.

Instrumentarianism's radical indifference is operationalized in Big Other's dehumanized methods of evaluation that produce equivalence without equality by reducing individuals to the lowest common denominator of sameness – organisms among organisms. There is no need for mass submission to social norms, no loss of self to the collective induced by terror and compulsion, no inducements of acceptance and belonging as a reward for bending to the group. All of that is superseded by a market-based digital order that thrives within things and bodies, transforming

[29] Mark Weiser, "The Computer for the 21st Century," *Scientific American*, July 1999: 104.

volition into reinforcement and action into conditioned response. Thanks to Big Other's capabilities to know and to do, instrumentarian power aims for a condition of certainty without terror in the form of guaranteed outcomes. In the execution of economies of action, Big Other transforms "natural selection" into the "unnatural selection" of variation and reinforcement authored by market players and the competition for surveillance revenues.

The paradox is that because instrumentarianism does not claim bodies for some grotesque regime of pain and murder, many are prone to undervalue its effects and lower their guard. Under the regime of instrumentarian power, the mental agency and self-possession of autonomous human action are gradually submerged beneath a new kind of automaticity: a lived routine of stimulus-response-reinforcement that operates outside of awareness and is aggregated as statistical phenomena: the comings and goings of mere organisms.

The challenges associated with successful economies of action have become a critical experimental zone for the elaboration of instrumentarian power. It is likely that much of this experimentation is invisible to the public, but at least some hides in plain sight, where one can observe how knowledge tips into power, epistemic inequality into epistemic injustice.

For example, Facebook conducted "massive-scale contagion experiments," the results of which were published in 2012 and 2014. The first aimed to subliminally induce voting in the lead-up to the 2010 US mid-term elections. The second aimed to influence users to feel "happy" or "sad." As a result of these experiments researchers concluded that, (1) it is possible to deploy subliminal cues on Facebook pages to alter real-world behaviour and emotions and (2), it is possible to accomplish such remote behavioral and affective modification with undetectable methods designed to bypass human awareness. Indeed, the very first paragraph of the 2014 research article on emotional contagion celebrates these findings: "Emotional states can be transferred to others via emotional contagion, leading people to experience the same emotions without their awareness."[30]

Facebook provides yet another observation point for the development of economies of action. In May 2017, three years after the publication of the contagion studies, The *Australian* broke the story on a confidential twenty-three-page Facebook document written by two Facebook executives and aimed at the company's Australian and New Zealand advertisers. The report depicted the corporation's systems for gathering "psychological insights" on 6.4 million high school and tertiary students as well as young Australians and New Zealanders already in the workforce. The Facebook document detailed the many ways in which the corporation uses its stores of behavioral surplus to

[30] Robert M. Bond et al., "A 61-Million-Person Experiment in Social Influence and Political Mobilization," *Nature* 489, no. 7415 (September 12, 2012): 295–98, https://doi.org/10.1038/nature11421; Adam D. I. Kramer, Jamie E. Guillory, and Jeffrey T. Hancock, "Experimental Evidence of Massive-Scale Emotional Contagion through Social Networks," *Proceedings of the National Academy of Sciences* 111, no. 24 (June 17, 2014): 8788–90, https://doi.org/10.1073/pnas.1320040111.

simulate and predict individual and group affective patterns in order to pinpoint the exact moment at which a young person needs a "confidence boost" and is therefore most vulnerable to a specific configuration of advertising cues and nudges: "By monitoring posts, pictures, interactions, and Internet activity, Facebook can work out when young people feel 'stressed,' 'defeated,' 'overwhelmed,' 'anxious,' 'nervous,' 'stupid,' 'silly,' 'useless,' and a 'failure.'"[31]

The report reveals Facebook's interest in leveraging this affective surplus for the pivot from monitoring to actuation. It boasts detailed information on "mood shifts" among young people based on "internal Facebook data," and it claims that not only can Facebook's prediction products "detect sentiment," they can also predict how emotions are communicated at different points during the week. These data are then used to match each emotional phase with appropriate ad messaging for the maximum probability of guaranteed sales. "Anticipatory emotions are more likely to be expressed early in the week," the analysis counsels, "while reflective emotions increase on the weekend. Monday–Thursday is about building confidence; the weekend is for broadcasting achievements." The young adults of Australia's and New Zealand's cities and towns had no reason to suspect that their fears and fantasies were being routinely exploited for commercial result at the precise moment of their greatest vulnerability. ("NEED A CONFIDENCE BOOST? CLICK HERE! BUY THIS BLACK LEATHER JACKET NOW! FREE OVERNIGHT DELIVERY!")

Facebook publicly denied these practices, but former Facebook product manager Antonio Garcia-Martinez, the author of *Chaos Monkeys*, a useful account of Silicon Valley, described in the *Guardian* the routine application of such practices and accused the corporation of "lying through their teeth." He concluded: "The hard reality is that Facebook will never try to limit such use of their data unless the public uproar reaches such a crescendo as to be un-mutable."[32] It is Facebook that knows. It decides who knows. It decides who decides.

The public's intolerable knowledge disadvantage is deepened by surveillance capitalists' perfection of mass communications as gaslighting. Indeed, these firms have long mastered the tactical arts of disinformation and fake news, paving the way for social complacency toward the crisis of truthfulness and social trust that has engulfed public communications. A few examples are illustrative. On April 30, 2019 Mark Zuckerberg made a dramatic announcement at the company's annual developer conference, declaring: "The future is private."[33] A few weeks later, a Facebook

[31] Darren Davidson, "Facebook Targets 'Insecure' to Sell Ads," *Australian*, May 1, 2017, https://www.theaustralian.com.au/business/media/facebook-targets-insecure-young-people-to-sell-ads/news-story/a89949ad016eee7d7a61c3c30c909fa6.

[32] Antonio Garcia-Martinez, "I'm an Ex-Facebook Exec: Don't Believe What They Tell You about Ads," *Guardian*, May 2, 2017, sec. Technology, https://www.theguardian.com/technology/2017/may/02/facebook-executive-advertising-data-comment.

[33] Nick Statt, "Facebook CEO Mark Zuckerberg Says the 'Future Is Private,'" *The Verge*, April 30, 2019, https://www.theverge.com/2019/4/30/18524188/facebook-f8-keynote-mark-zuckerberg-privacy-future-2019.

litigator appeared before a federal district judge in California to thwart a user lawsuit over privacy invasion, arguing that the very act of using Facebook negates any reasonable expectation of privacy "as a matter of law."[34] While leaked internal documents describe the firm's sophisticated methods for accruing granular psychological insights for targeting and triggering individuals, in early 2020 its Vice President of Public Policy told a public forum: "We don't do surveillance capitalism, that by definition is surreptitious; we work hard to be transparent."[35] In May 2019, Google CEO Sundar Pichai wrote in the *New York Times* of his corporation's commitment to the principle that "privacy cannot be a luxury good."[36] Five months later Google contractors were observed offering $5 gift cards to homeless people of color in an Atlanta park in return for a facial scan.[37] While Amazon cracked down on employees for violating the company's privacy by publicly discussing its policies and practices, the corporation aggressively strengthens the one-way mirror, marketing its collection of surveillance-as-a-service connected devices and appliances based on the Alexa voice recognition system. Its latest suite of Internet-enabled devices was characterized by the *Seattle Times* as "a sweeping vision of automation, entertainment, ubiquitous surveillance and commerce permeating nearly every aspect of life."[38]

Facebook's denial of psychological targeting practices invites even more scrutiny in light of the leaked 2018 company document, which described its "AI Hub."[39] That report also indicated that the company's extraordinary data flows and computational production are dedicated to meeting its corporate customers' "core business challenges" with procedures that link prediction, microtargeting, intervention, and behavior modification. For example, a Facebook service called "loyalty prediction" was touted for its ability to plumb proprietary behavioral surplus in order to predict which individuals are "at risk" of shifting their brand allegiance. This knowledge

[34] Sam Biddle, "In Court, Facebook Blames Users for Destroying Their Own Right to Privacy," *The Intercept* (blog), June 14, 2019, https://theintercept.com/2019/06/14/facebook-privacy-policy-court/.

[35] Tekla S. Perry, "CES 2020 News: Tech Executives Answer Tough Questions about Privacy," *IEEE Spectrum*, January 8, 2020, https://spectrum.ieee.org/view-from-the-valley/telecom/internet/ces-2020-news-tech-executives-answer-tough-questions-about-privacy; Biddle, "Facebook Uses Artificial Intelligence to Predict Your Future Actions for Advertisers, Says Confidential Document"; Darren Davidson, "Facebook Targets 'Insecure' to Sell Ads."

[36] Sundar Pichai, "Google's Sundar Pichai: Privacy Should Not Be a Luxury Good | Opinion," *New York Times*, May 22, 2019, sec. Opinion, https://www.nytimes.com/2019/05/07/opinion/google-sundar-pichai-privacy.html.

[37] Ginger Adams Otis and Nancy Dillon, "City Worker Saw Homeless People Lined Up to Get $5 Gift Card for Face Scan Uploaded to Google," *Nydailynews.com*, October 3, 2019, https://www.nydailynews.com/news/national/ny-witness-saw-homeless-people-selling-face-scans-google-five-dollars-20191004-j6z2vonllnerpiuakt6wrp6l44-story.html.

[38] Shirin Ghaffary, "Amazon Threatened to Fire Employees Who Spoke Out against Its Environmental Policies," *Vox*, January 2, 2020, https://www.vox.com/recode/2020/1/2/21046886/amazon-climate-change-fired-activists-sustainability-walkout-pledge-carbon-emissions-activism; Benjamin Romano, "Amazon Rolls out New Devices amid Swirl of Privacy Questions."

[39] Biddle, "Facebook Uses Artificial Intelligence to Predict Your Future Actions for Advertisers, Says Confidential Document."

alerts advertisers to intervene promptly with targeted messages designed to stabilize loyalty just in time to alter the course of the future.

Google's experimentation with economies of action moved boldly into the real world with the augmented reality game Pokémon Go. The project had been incubated at Google for many years, led by John Hanke, an early inventor of satellite mapping and leader of Google's mapping operations including Google Earth and Street View, both critical sources of surplus data supplies. Later Hanke headed up his own augmented reality shop inside Google, Niantic Labs, where Pokémon Go was developed and spun off from the company just in time to go to market with Hanke as its head and Goggle its principal investor.[40]

Pokémon Go brought the emerging science of remote population tuning and herding to the real world: real streets, real towns, real cities. It added the rewards and punishments of gamification to the methods of subliminal cueing and the manipulation of social comparison dynamics in order to bypass users' awareness of the situational facts: families and friends were engaged in a search game without knowing that it was they who were being searched and gamed. Players were, in fact, unwitting pawns in a hidden higher-order game that aimed to provide "footfall" to fee-paying establishments as they vied for real-world consumer visits in exactly the same way that online advertisers pay for the virtual visits of clicks and engagement. Niantic used immense caches of data collected from game players' devices in order to apply the incentives and reinforcements of gamification for the sake of herding players to the real-world business customers in its futures markets, from McDonald's and Starbucks to Joe's Pizza.[41]

These escalating zones of experimentation and their practical success suggest a disturbing conclusion: the competitive necessity of economies of action means that surveillance capitalists must use all means available to supplant autonomous action with heteronomous behavior. Human awareness is a threat to surveillance revenues because the mobilization of awareness endangers the larger project of behavior modification. Philosophers recognize "self-regulation," "self-determination," and "autonomy" as expressions of "freedom of will," and a flourishing research literature illuminates the antecedents, conditions, consequences, and challenges of human self-regulation as a universal need. The capacity for self-determination is understood as an essential foundation for behaviors associated with critical human capabilities such as empathy, volition, reflection, personal development, authenticity, integrity, learning, goal accomplishment, impulse control, creativity, and the sustenance of intimate relationships. "Implicit in this process is a self that sets goals and standards, is aware of its own thoughts and behaviors, and has the capacity to change them. Indeed, some theorists have

[40] Dyani Sabin, "The Secret History of 'Pokemon GO' as Told by the Game's Creator," *Inverse*, February 28, 2017, https://www.inverse.com/article/28485-pokemon-go-secret-history-google-maps-ingress-john-hanke-updates.

[41] For a full discussion of John Hanke, Pokémon Go and Niantic Labs, see Zuboff, *The Age of Surveillance Capitalism*, pp. 309–19.

suggested that the primary purpose of self-awareness is to enable self-regulation." Every threat to human autonomy begins with an assault on awareness, "tearing down our capacity to regulate our thoughts, emotions, and desires."[42]

The salience of self-awareness as a bulwark against self-regulatory failure is also highlighted in recent research on "susceptibility to persuasion," which concludes that "the ability to premeditate" is the single-most-important determinant of one's ability to resist persuasion.[43] People who harness self-awareness to think through the consequences of their actions are more disposed to chart their own course and are thus significantly less vulnerable to persuasion techniques. Self-awareness also figures in the second highest-ranking protection from susceptibility to persuasion: commitment. Those who consciously commit to a course of action or set of principles are less likely to be persuaded to do something that violates their commitment.

In one sense, there is nothing remarkable in observing that capitalists would prefer individuals who submit to arrangements that advantage capital. It would be incorrect, however, to conclude that today's surveillance capitalists simply represent more of the same. The structural requirements of economies of action turn the means of behavioral modification into an engine of growth. At no other time in history have the wealthiest private corporations had at their disposal a pervasive global architecture of ubiquitous computation able unilaterally to amass unparalleled concentrations of information about individuals, groups, and populations sufficient to mobilize the pivot from knowledge about behavior to the actuation of commercially desirable behavior. In other words, when we climb the mountain of the division of learning and peek into the fortress, we see a frontier operation run by geniuses and funded by vast capital outlays that is furiously dedicated to knowing everything about us and pivoting that knowledge to the remote control of people. These are unprecedented conditions that bestow an unprecedented instrumentarian power on private capital.

IV. INFORMATION WARFARE

While democracy slept, epistemic inequality was produced, institutionalized, and protected by an unequal power that annuls the possibility of conflict by denying the

[42] Dylan D. Wagner and Todd F. Heatherton, "Self-Regulation and Its Failure: The Seven Deadly Threats to Self-Regulation," in *APA Handbook of Personality and Social Psychology* (Washington, DC: American Psychological Association,2015), pp. 805–42, https://pdfs.semanticscholar.org/2e62/15047e3a296184c3698f3553255ffabd46c7.pdf; William M. Kelley, Dylan D. Wagner, and Todd F. Heatherton, "In Search of a Human Self-Regulation System," *Annual Review of Neuroscience* 38, no. 1 (2015): 389–411, https://doi.org/10.1146/annurev-neuro-071013–014243.

[43] David Modic and Ross J. Anderson, "We Will Make You Like Our Research: The Development of a Susceptibility-to-Persuasion Scale," *SSRN* (Rochester, NY: Social Science Research Network, April 28, 2014), https://papers.ssrn.com/abstract=2446971; Mahesh Gopinath and Prashanth U. Nyer, "The Influence of Public Commitment on the Attitude Change Process: The Effects of Attitude Certainty, PFC and SNI," *SSRN*, 2007, https://doi.org/10.2139/ssrn.1010562.

right of combat. In this case, denial is achieved through Big Other's hidden techno-economic systems that steal, know, and shape human behavior for the sake of others' gain. These capabilities depend on the evasion of human awareness. This entails the denial of the epistemic rights that confer individual sovereignty over self/knowledge. Instrumentarian power is the guarantor of epistemic inequality, the hammer of epistemic injustice, and the usurper of epistemic rights.

Because one's self and all the selves are meant to sleepwalk peacefully through this known unknown, sudden news from behind the veil can have an electrifying effect, if only for a while. This helps to explain the force with which the story of Cambridge Analytica broke on the world in March 2018, when Chris Wylie, the young mastermind-turned-whistleblower, unleashed a torrent of information on that company's secret efforts to predict and influence individual voting behavior, quickly riveting the world on the small political analytics firm and the giant source of its data: Facebook. There are many unanswered questions about the legality of Cambridge Analytica's complex subterfuge, its actual political impact, and its relationship with Facebook. My interest here is restricted to how it replicated surveillance capitalism's ordinary practices, and the implications of that fact.[44]

Academic researchers had already demonstrated the predictive power of behavioral surplus culled from Facebook pages, the insights into human personality that it can yield, the resulting opportunities for behavioral manipulation and modification, and the commercial value of such methods. Wylie recounted his fascination with these studies, especially as they might be pivoted from commercial to political outcomes.[45] Through a complicated chain of events, it was Wylie who persuaded Cambridge Analytica's owner, the secretive software billionaire and active enemy of democracy Robert Mercer, and his operatives, including anti-democracy's dark theorist Steve Bannon, to use Facebook data to advance Mercer's political aims.

Cambridge Analytica's operations followed the surveillance capitalist playbook. They were designed to produce ignorance through secrecy and the careful evasion of individual awareness: "We exploited Facebook to harvest millions of people's profiles," Wylie admitted, "and built models to exploit what we knew about them and target their inner demons."[46] The objective was "behavioral micro-targeting . . . influencing voters based not on their demographics but on their personalities."[47] "I think it's worse than bullying, because people don't necessarily know it's being done to them," Wylie reflects. "At least bullying respects the agency of people because they know . . . if you do not respect the agency of people, anything that you're doing

[44] For a full account of the Cambridge Analytica story, see Zuboff, *The Age of Surveillance Capitalism.*, pp. 278–82, 482–3.

[45] Zuboff, *The Age of Surveillance Capitalism*, pp. 272–78.

[46] Andy Kroll, "Cloak and Data: The Real Story behind Cambridge Analytica's Rise and Fall," *Mother Jones* (blog), March 2018, https://www.motherjones.com/politics/2018/03/cloak-and-data-cambridge-analytica-robert-mercer/.

[47] Kroll.

after that point is not conducive to a democracy. And fundamentally, information warfare is not conducive to democracy."[48]

Wylie describes Cambridge Analytica's operations as "information warfare," correctly acknowledging that this form of shadow warfare originates in significant asymmetries of knowledge and the power produced by such knowledge. In other words, information warfare exploits epistemic inequality, while its effects intensify epistemic injustice.

However, the Cambridge Analytica narrative suggests an even more disturbing conclusion. The political firm was only able to operate as an information warrior because the conditions for successful warfare and its weapons had already been developed by surveillance capital. Surveillance capitalist operations like Facebook, Google, Amazon, Microsoft, and countless others are best understood as examples of information-warfare-for-profit. These firms are information mercenaries that leverage unprecedented asymmetries of knowledge/power for the sake of revenues, which, in turn, fund their continued dominance and the intensification of epistemic inequality.

Consider how a small firm such as Cambridge Analytica was able to enter the fray of information war. The so-called political consultancy functioned as a parasite buried into the host of Facebook's vast behavioral data supply chains, while adapting its host's foundational mechanisms and methods: secret data capture, extraction of behavioral surplus, predictive computational analysis, behavioral microtargeting in the service of economies of action.

Cambridge Analytica channeled these methods and mechanisms, merely pivoting the surveillance capitalist machinery from commercial markets in human futures toward guaranteed outcomes in the political sphere. Its strategies of secret invasion and hidden conquest were the same standard operating procedures to which billions of innocent "users" are subjected each day. What better description of the unsavory treatment of 6.6 million young people in Australia and New Zealand whose social anxieties were extracted and manipulated for profit than to say that we "built models to exploit what we knew about them and target their inner demons"? What more apt reflection on "loyalty prediction" interventions based on trillions of data points, or Pokémon Go's manipulative game within the game than, "I think it's worse than bullying, because people don't necessarily know it's being done to them"?

It is worthwhile noting that it was Google's Eric Schmidt who first pried open this Pandora's box, transferring surveillance capitalism's core mechanisms of behavioral microtargeting to the Obama presidential campaigns, where Wylie enjoyed some of his early training under Obama's Director of Targeting.[49] In little over a decade,

[48] Carole Cadwalladr, "'I Made Steve Bannon's Psychological Warfare Tool': Meet the Data War Whistleblower," *Guardian*, March 18, 2018, sec. News, http://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump.

[49] Kroll, "Cloak and Data."

Schmidt's innovations have become the envy of every enemy of democracy, well within reach of the plutocrat's wallet or the more modest budgets of other non-state actors. Indeed, information warfare is widely assumed to originate in the State for the purposes of political, cultural, and, or, military destabilization, just as we once considered behavioral modification or surveillance as projects of the State. But recent theories of information warfare have begun to recognize the growing ease with which non-state actors, such as Robert Mercer or ISIS, can undertake information warfare.[50]

What has not yet been adequately recognized is that surveillance capitalism has already institutionalized information warfare as a market project. It is only on the strength of this construction that states and non-state actors alike can succeed as information warriors. Such operations exist as parasites on the host of the larger surveillance capitalist body. A simple set of distinctions framed by US Naval Academy professor and cyber-security expert Martin Libicki are useful here as they help to describe the contributions of the surveillance capitalist host that deliver triple nourishment by providing what Libicki identifies as (1) the conditions, (2) the weapons, and (3) the opportunity to wage information war.[51]

Conditions

Surveillance capitalism's economic imperatives increase the range of societal vulnerabilities for parasitic exploitation. Libicki observes that US companies lead the world in the collection and processing of personal information. Pervasive datafication and connectivity, largely driven by surveillance capital, substantially increases society's "attack surface" leaving it more vulnerable to a range of assault capabilities. Libicki asks: "[W]hy collect what can be stolen?"[52]

Weapons

The surveillance capitalism host also provides the "weapons" (data, methods, and mechanisms) necessary to exploit the vulnerabilities that it creates. "Ultimately it has been the evolution of the information economy that has provided the means by which hostile others can run a pervasive harassment campaign," Libicki

[50] Frederik Zuiderveen Borgesius et al., "Online Political Microtargeting: Promises and Threats for Democracy," *SSRN* (Rochester, NY: Social Science Research Network, February 9, 2018), https://papers.ssrn.com/abstract=3128787.

[51] Martin C. Libicki, "The Convergence of Information Warfare," *Strategic Studies Quarterly*, 2017: 49–65; For other relevant discussions, see Gary P. Corn and Robert Taylor, "Sovereignty in the Age of Cyber," *AJIL Unbound* 111 (2017): 207–12, https://doi.org/10.1017/aju.2017.57; Duncan Hollis, "The Influence of War; The War for Influence," *Temple International & Comparative Law Journal* 32, no. 1 (2018): 31–46; Herbert Lin, "The Existential Threat from Cyber-Enabled Information Warfare," *Bulletin of the Atomic Scientists* 75, no. 4 (July 4, 2019): 187–96, https://doi.org/10.1080/00963402.2019.1629574.

[52] Martin C. Libicki, "The Convergence of Information Warfare," 51.

acknowledges.[53] He cites "data-mining techniques" that construct "realistic simulations of individuals, indeed perhaps of most of a population … integrating data streams with enormous cloud-based storage, powerful processing, and a dash of artificial intelligence." Such simulations, he notes, "may be used to test every individual's reaction to events," including "advertising, political campaigns, and psychological operations, and even to guess what might go viral through person-to-person interactions," just as we saw in the case of Facebook's contagion experiments.[54]

Libicki catalogues some of these weapons, which are already essential methods in surveillance capitalism's arsenal: "exquisite psychological operations," "messages tailored to one person at a time," and data-mining able to characterize individuals precisely enough for "crafting the message most likely to resonate with them." These achievements permit the "optimization" of "psychological operations," "new conduits for persuasion," and "the manipulation of fear," all of which are amply on display in surveillance capital's expanding zones of experimentation as it learns to translate knowledge into power.[55]

Opportunity

Libicki notes that information warfare unfolds in an atmosphere of "deep secrets" protected by "a dense fog of ambiguity."[56] These conditions are structurally enabled. First, they reproduce and extend the asymmetries of knowledge and power already compelled by economic imperatives. Second, as long as the surveillance capitalist host operates from the perspective of radical indifference, it is like a Cyclops whose single line of sight leaves it blind to everything but its prey. Parasitic operations succeed because they fall on the blind sides of radical indifference. This means that parasites can persist unchallenged for long periods. It is difficult to find them, disable them, and to confirm their destruction. Such was the case with Cambridge Analytica, which fed off illegitimately collected Facebook data that were illegitimately sold for nefarious purpose – all of it secreted in the shadow of Facebook's single eye. Radical indifference creates a void where social reciprocities once thrived. Surveillance capitalists cannot fill this void because doing so would violate the logic of accumulation on which everything depends. The rogue forces of disinformation grasp this fact more crisply than anyone else, as they cleverly exploit the Cyclops of radical indifference and escalate the perversion of information in an open society.[57]

[53] Libicki, 63.
[54] Libicki, 51–52.
[55] Libicki, 53–54.
[56] Libicki, 55–56.
[57] For a detailed discussion, see Zuboff, *The Age of Surveillance Capitalism*, pp. 504–12.

Surveillance capitalism's antidemocratic and antiegalitarian consequences are best described as a market-driven coup from above. It is not a coup d'état in the classic sense but rather a coup de gens: an overthrow of the people concealed in the technological Trojan horse that is Big Other. On the strength of its audacious annexation of human experience, this coup achieves exclusive concentrations of knowledge and power that undermine democracy at root and crown. It poisons democracy at its roots by usurping the epistemic rights that confer individual sovereignty over self/knowledge, thus weakening self-determination and undermining human autonomy without which democratic society is unimaginable. It poisons democracy from above by imposing a new axis of epistemic inequality that now threatens to remake society while unmaking the structure and function of democratic institutions. Surveillance capital wages a quiet information war for epistemic hegemony and the power over human behavior that it promises, thus channeling capitalism's adversarial bloodline not toward groups like workers or consumers who are defined by their economic function, but rather toward the widest possible category of people: "users." This broad target of all people engaged in all forms of life is as all-encompassing as the economic imperatives that compel surveillance capitalism toward societal domination. It bears a single message: CAVEAT USOR.

V. THE POISONED CROWN: THE DIVISION OF LEARNING IN SOCIETY

When the young Emile Durkheim wrote *The Division of Labor in Society*, a treatise that would become a foundational text of modern sociology, the title itself was controversial. Why this was the case is relevant to our predicament today. Because the transformation that we witness in our time echoes many of the century-old observations in Durkheim's seminal work, a few key points are reviewed here.

The division of labor had been understood as a critical means of achieving labor productivity through the specialization of tasks. Adam Smith memorably wrote about this new principle of industrial organization in his description of a pin factory, and the division of labor remained a topic of economic discourse and controversy throughout the nineteenth century. Durkheim recognized labor productivity as an economic imperative of industrial capitalism that would drive the division of labor to its most extreme application, but that was not what held his fascination.

Instead, Durkheim trained his sights on the social transformation already gathering around him, observing that "specialization" was gaining "influence" in politics, administration, the judiciary, science, and the arts. He concluded that the division of labor was no longer quarantined in the industrial workplace. Instead it had burst through those factory walls to becoming the central organizing principle of industrial society: "Whatever opinion one has about the division of labor," Durkheim

wrote, "everyone knows that it exists, and is more and more becoming one of the fundamental bases of the social order."[58]

Economic imperatives predictably mandated the division of labor in production, but what was the purpose of the division of labor in society? This was the question that motivated Durkheim's analysis, and his century-old conclusions are relevant for us now. He argued that the division of labor accounts for the interdependencies and reciprocities that link the many diverse members of a modern industrial society in a larger prospect of solidarity. This new principle of social order was an essential response to the breakdown of traditional communities as the old sources of meaning that had reliably bonded people across space and time melted away. What would hold society together in the absence of the rules and rituals of place, clan, and kin? Durkheim's answer was "the division of labor." Society's need for a coherent new source of meaning and structure was the cause, and the effect was an ordering principle that enabled and sustained a healthy modern community. The reciprocities of the division of labor would breed mutual need, interdependence, and respect, all of which imbue this new ordering principle with moral force. As the young social theorist explained:

> The most remarkable effect of the division of labor is not that it increases output of functions divided, but that it renders them solidary. Its role ... is not simply to embellish or ameliorate existing societies, but to render societies possible which, without it, would not exist .... It passes far beyond purely economic interests, for it consists in the establishment of a social and moral order sui generis.[59]

Durkheim's vision was neither sterile nor naive. He recognized that things can take a dark turn and often do, resulting in what he called an "abnormal division of labor" (sometimes translated as "pathological") that produces social distance, injustice, and discord in place of reciprocity and interdependence. In this context, Durkheim singled out the destructive effects of inequality on the division of labor in society, especially what he viewed as the most dangerous source of inequality: extreme asymmetries of power that make "conflict itself impossible" by "refusing to admit the right of combat." Such pathologies can only be cured by a politics that asserts the people's right to contest, confront, and prevail in the face of unequal and illegitimate power over society. In the late nineteenth and most of the twentieth centuries, that contest was defined by economic inequality and led by labor and other social movements that asserted rights to economic justice through new institutional constructions: unions, collective bargaining, public education.

But now it is a division of learning that follows the same migratory path from the economic to the social domain once traveled by the division of labor. The progress of digitalization and information intensification began in the offices and factories of the 1980s, when workplaces mobilized around the new questions concerning

[58] Emile Durkheim, *The Division of Labor in Society* (New York, NY: Free Press, 1964), p. 41.
[59] Durkheim, pp. 60–61.

knowledge, authority, and power, thus drawing labor and capital into a novel and poorly understood crisis of epistemic equality.[60]

Forty years later it is possible to see that the labor crisis of the late twentieth century was an early phase of a longer struggle over the division of learning in society that would engulf twenty-first century societies as the dilemmas of knowledge, authority, and power broke through the boundaries of the economic sphere to overwhelm and finally saturate everyday life. Now the division of learning "passes far beyond purely economic interests," as it establishes the basis for a new social order and its moral content. But scientists warn that the world's capacity to produce information has substantially exceeded its ability to process and store information.[61] Information is digital, but its volume exceeds our ability to discern its meaning.

As the solution to this problem, Martin Hilbert counsels, "The only option we have left to make sense of all the data 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."[62] The rise of surveillance capitalism, however, necessarily turns Hilbert's advice into a damning vision of social pathology. Although he does not mean to, Hilbert's suggestion merely confirms the self-authorized epistemic dominance of the surveillance capitalists and the institutionalization of epistemic inequality as the division of learning in society is bent to the commercial interests of private surveillance capital.

Surveillance capitalism's command of the division of learning in society begins with the problem of what may be called "the two texts." The first is the public-facing text, familiar and celebrated for the universe of information and connection that it brings to our fingertips. We are its authors and its readers. Google Search codifies the informational content of the World Wide Web. Facebook's News Feed binds the social network. Much of this public-facing text is composed of what we inscribe on its pages: posts, blogs, videos, photos, conversations, music, stories, observations, "likes," tweets, and all the great massing hubbub of lives captured and communicated.

Under the regime of surveillance capitalism, however, the first text does not stand alone; it trails a shadow close behind. The first text, full of promise, actually functions as the supply operation for this second shadow text. Everything that is contributed to the first text, no matter how trivial or fleeting, becomes a target for surplus extraction. That surplus fills the pages of the shadow text, hidden from view and "read only" for surveillance capitalists.[63] In this text, private experience is

[60] Zuboff, *In the Age of the Smart Machine*.

[61] Hilbert (2012).

[62] Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (Boston, MA: Houghton Mifflin Harcourt, 2013), p. 9.

[63] Harvard legal scholar John Palfrey observed the "read only" nature of electronic surveillance in his wonderful 2008 essay, John Palfrey, "The Public and the Private at the United States Border with Cyberspace," *Mississippi Law Journal* 78 (2008): 241–94, see especially p. 249.

dragooned as raw material to be accumulated and analyzed as means to others' market ends. The shadow text conceals more about us than we can know about ourselves, exemplified in Facebook's ingestion and calculation of trillions of behavioral data points each day. Worse still, it is nearly impossible to refrain from contributing to this vast concentration of shadow knowledge, as Big Other feeds on the normal and necessary routines of daily life.

Finally, shadow knowledge ricochets back into lives, morphing into the instrumentarian power to shape what is seen, learned, and done. As Frank Pasquale describes Google: "The decisions at the Googleplex are made behind closed doors ... the power to include, exclude, and rank is the power to ensure which public impressions become permanent and which remain fleeting ... Despite their claims of objectivity and neutrality, they are constantly making value-laden, controversial decisions. They help create the world they claim to merely 'show' us."[64] When it comes to the shadow text, we are the objects of its narratives from whose lessons we are excluded. As the source from which all the treasure flows, the shadow text is about us, but it is not for us. Instead it is created, maintained, and exploited outside our awareness for others' profit.

Just as Durkheim warned his society a century ago of an abnormal division of labor, we now enter the third decade of the twenty-first century with our societies already disfigured by a division of learning that drifts into pathology marked by epistemic inequality and injustice at the hands of the unprecedented asymmetries of knowledge institutionalized in the shadow text. The pathology does not stop here. Asymmetries of knowledge feed the progress of instrumentarian power as exclusive knowledge is translated through the networked layer of digital instrumentation to produce new capabilities of actuation at scale – influencing, tuning, herding, and modifying human behavior toward others' commercial ends. The division of learning is thus both the ascendant principle of social order in the twenty-first century and already hostage to surveillance capital's privileged position, empowered by its ownership of the texts and its exclusive command of analysis and prediction capabilities.

More than thirty years ago, the legal scholar Spiros Simitis published a remarkable essay on the theme of privacy in an information society. Simitis grasped early on that the already visible trends in public and private "information processing" harbored threats to society that transcended narrow conceptions of privacy and data ownership. "[P]ersonal information is increasingly used to enforce standards of behavior," he wrote. "Information processing is developing, therefore, into an essential element of long-term strategies of manipulation intended to mold and adjust individual conduct."[65] Simitis argued that these trends were incompatible not only with privacy but with the very possibility of democracy, which depends

[64] Frank Pasquale, *The Black Box Society* (Cambridge, MA: Harvard University Press, 2015), pp. 60–61.
[65] Spiros Simitis, "Reviewing Privacy in an Information Society," *University of Pennsylvania Law Review* 135, no. 3 (1987): 710, https://doi.org/10.2307/3312079.

on a reservoir of individual proficiencies associated with autonomous moral judgment and self-determination.

Building on Simitis's work, Paul Schwartz warned in 1989 that computerization would transform the delicate balance of rights and obligations upon which privacy law depends: "Today the enormous amounts of personal data available in computers threaten the individual in a way that renders obsolete much of the previous legal protection." Most important, Schwartz foresaw that the scale of the still emerging epistemic crisis would impose risks that exceed the scope of privacy law. "The danger that the computer poses is to human autonomy," he warned. "The more that is known about a person, the easier it is to control him. Insuring the liberty that nourishes democracy requires a structuring of societal use of information and even permitting some concealment of information."[66]

Both Simitis and Schwartz sensed the ascent of the division of learning as the axial principle of a new computational societal milieu, but they could not have anticipated the rise of surveillance capitalism and its consequences. While the explosive growth of information territories shifts a crucial axis of the social order from a twentieth-century division of labor to a twenty-first century division of learning, it is surveillance capitalists who command the field and unilaterally lay claim to a disproportionate share of the epistemic rights that shape the division of learning in society.

Instead of the long anticipated explosion of democratization, the competitive struggle over surveillance revenues has dragged our societies into a regressive "pre-Gutenberg" pattern, in which a pathological division of learning is captured by private capital, presided over by a narrow priesthood of privately employed computational specialists, their privately owned machines, and the economic interests for whose sake they learn. This epistemic violence runs free of law, of market restraints, and of organic reciprocities with its communities, which are no longer required as sources of customers or employees but rather as a passive unwitting cornucopia of raw material for production and sales.

The result is best understood as *the unauthorized privatization of the division of learning in society*. Just as Durkheim warned of the subversion of the division of labor by the powerful forces of industrial capital a century ago, today's successful prosecution of information warfare aimed at citizen-users by surveillance capital now exerts private power over the definitive principle of social order in our time. Epistemic inequality is enshrined as the signature deformation of this epoch as the pathologies of the division of learning infect the societal superstructure.

Here is democracy's poisoned crown: As things currently stand, it is the surveillance capitalist corporations that know. It is the market form that decides. It is surveillance capital that decides who decides. Experts in the disciplines associated

[66] Paul M. Schwartz, "The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination," *American Journal of Comparative Law* 37 (1989): 676.

with machine intelligence know this, although they have little grasp of its implications as the signal of the defining axis of social inequality in our time. One data scientist writes: "Whoever has the best algorithms and the most data wins . . .. Google with its head start and larger market share, knows better what you want . . . whoever learns fastest wins."[67] In 2018, the *New York Times* reported that Google CEO Sundar Pichai had located his office on the same floor as the company's AI research lab, noting it as a trend among many CEOs – a literal take on the concentration of knowledge and power.[68]

Here is the paradox in which citizens are caught: *Democracy is the target of this epistemic poison, and its only antidote.*

VI. REMEDIES

Despite the variation of motives among the ninety Spanish citizens, their collective assertion of a "right to be forgotten" announced a new twenty-first-century contest over once elemental epistemic rights now under global assault from private surveillance capital. The European Court of Justice's decision on the "right to be forgotten" so often reduced to the legal and technical considerations related to the deletion or delinking of personal data, was in fact a key inflection point at which elemental epistemic rights successfully sought the protection of democratic institutions as they undertook the long migration toward law. It was the Court of Justice that wrote an early chapter in what is now an epoch-defining struggle to claw back epistemic rights from the powerful forces of surveillance capital and its determination to assert authority over what can be learned and known. There is evidence that citizens and lawmakers around the world are finally picking up the pen, as a new wave of public "techlash," legislative initiatives, and regulatory actions begins to take shape.

The past offers good counsel at this key juncture. In his Pulitzer prize-winning history, *Prophets of Regulation*, Thomas McCraw recounts the phases and distinct purposes of regulatory regimes in the US: the 1870s and the initial period of industrialization; the early twentieth century, especially 1900–1916; the 1930s and the New Deal; and the onset of deindustrialization during the 1970s and 1980s. The challenges of each era brought distinct forms of law and regulatory leadership. At the dawn of the twentieth century it was the muckrakers and progressives who defined the regulatory paradigm. Later, the lawyers dominated. It was only the past few decades that saw the economists as framers of the regulatory vision.

McCraw observes that this "economists' hour" will certainly end and wonders what will follow. In considering the arc of this history, he finds clues, noting that

[67] Pedro Domingos, *The Master Algorithm: How the Quest for the Ultimate Learning Machine Will Remake Our World* (New York, NY: Basic Books, 2015), pp. 12–13.

[68] Cade Metz, "Why A.I. Researchers at Google Got Desks Next to the Boss," *New York Times*, February 19, 2018, sec. Technology, https://www.nytimes.com/2018/02/19/technology/ai-researchers-desks-boss.html.

concerns for justice and fairness have generally overshadowed the more narrow aims of economic growth in the construction of regulatory regimes. "Regulation," he writes, "is best understood as a political settlement."[69]

This perspective suggests that the chartering frameworks of a digital future compatible with the principles of a democratic society are most likely to be defined and led by champions of democracy. The key principles here must be: (1) the redistribution of epistemic rights to the sovereign individual, (2) under the authority of the rule of law, and (3) sustained by the power of democratic institutions and their governance. Elected officials, citizens, and specialists can seize this opportunity, allied in the knowledge that despite its failures and shortcomings, democracy is the one idea to emerge from the long human story that enshrines the peoples' right to govern themselves and asserts the ideal of the sovereign individual as the single most powerful bulwark against tyranny.

McCraw delivers a warning with his observations, however, and it is significant for us now. The historical record shows that regulators failed when they were unable "to frame strategies appropriate to the particular industries they were regulating."[70] The lesson is that today's new legislative and regulatory challenges will not be met effectively without a clear grasp of surveillance capitalism as a novel economic logic defined by distinct economic imperatives and the specific practices and consequences that they compel. Twenty-first century solutions to our twenty-first century challenges may build on existing paradigms of privacy and antitrust but will also have to move beyond and even transform those paradigms, as we learn how to interrupt and outlaw surveillance capitalism's key mechanisms, methods, and markets. As the European Commissioner for Competition Margrethe Vestager recently put it: "One of the things I have learned from surveillance capitalism . . . is [that] it's not you searching Google, it is Google searching you. And that gives a very good idea about not only what you want to buy but also what you think. So we have indeed a lot to do."[71]

The prospects of a new regulatory paradigm are improved with a clear grasp of the forces that have impeded its emergence during the first two decades of the twenty-first century. Lawmakers have been reluctant to challenge surveillance capitalism for many reasons.[72] Among these was an unwritten policy of "surveillance exceptionalism" forged in the aftermath of the September 11 terrorist attacks, when the government's concerns shifted from online privacy protections to a new zeal for "total information awareness." In that political environment, the fledgling surveillance

[69] Thomas K. McCraw, *Prophets of Regulation: Charles Francis Adams; Louis D. Brandeis; James M. Landis; Alfred E. Kahn* (Cambridge, MA: Belknap Press: An Imprint of Harvard University Press, 1986), l. 3990.

[70] McCraw, l. 4037.

[71] Natasha Lomas, "Europe's Recharged Antitrust Chief Makes Her Five-Year Pitch to Be Digital EVP," *TechCrunch* (blog), October 8, 2019, http://social.techcrunch.com/2019/10/08/europes-recharged-antitrust-chief-makes-her-five-year-pitch-to-be-digital-evp/.

[72] Zuboff, *The Age of Surveillance Capitalism*, chapter 4.

capabilities emerging from Silicon Valley appeared to hold great promise. Another reason has been the unparalleled lobbying infrastructure pioneered by Google and later joined by Facebook and others. A third is the value of behavioral microtargeting to political campaigns.[73]

As a new wave of public mobilization and lawmaking gathers force, doing "a lot" will require overcoming these old impediments. It also means confronting surveillance capitalism's strategic propaganda campaigns and its mass communications tactics based on gaslighting and mendacity. Strategies and tactics have been designed as defensive fortifications intended to undermine and intimidate lawmakers and citizens alike, confounding judgment and freezing action. What follows are three examples of strategic propaganda that have received relatively little scrutiny compared to the damage they do.

The Innovation Defense

Surveillance capitalist leaders vigorously portray democracy as the enemy of innovation. Facebook's Head of Global Policy and Communications, Sir Nick Clegg, warned in 2019 that any restrictions resulting from "tech-lash" risked making it "almost impossible for tech to innovate properly," invoking the threat of Chinese ascendance as the price the West would pay for law. "I can predict that . . . we will have tech domination from a country with wholly different sets of values," he insisted.[74]

Clegg was only repeating what surveillance capitalist leaders had been proselytizing for years. In 2010, Mark Zuckerberg announced that privacy was no longer a "social norm," celebrating Facebook's explosive new "privacy policies" that publicly displayed personal information by default as evidence of his determination to innovate rather than "be trapped" by conventions or law. "We decided that these would be the social norms now and we just went for it."[75] In 2011, former Google CEO Eric Schmidt warned that government overreach would foolishly constrain innovation: "We'll move much faster than any government."[76] That year Google founder Larry Page complained that "old institutions like the law" impede the firm's freedom to "build really great things."[77] All of this rhetoric is actually a hand-me-down from another era when Gilded Age barons, whom we now call "robbers,"

[73] See, ibid., pp. 112–27.

[74] Natasha Lomas, "Facebook Makes Another Push to Shape and Define Its Own Oversight," *TechCrunch* (blog), June 24, 2019, http://social.techcrunch.com/2019/06/24/facebook-makes-another-push-to-shape-and-define-its-own-oversight/.

[75] Bobbie Johnson, "Privacy No Longer a Social Norm, Says Facebook Founder," *Guardian*, January 10, 2010, sec. Technology, https://www.theguardian.com/technology/2010/jan/11/facebook-privacy.

[76] Pascal-Emmanuel Gobry, "Eric Schmidt to World Leaders at EG8: Don't Regulate Us, or Else," *Business Insider*, May 24, 2011, http://www.businessinsider.com/eric-schmidt-google-eg8-2011–5.

[77] Jay Yarow, "Google CEO Larry Page Wants a Totally Separate World Where Tech Companies Can Conduct Experiments on People," *Business Insider*, May 16, 2013, http://www.businessinsider.com/google-ceo-larry-page-wants-a-place-for-experiments-2013–5.

insisted that there was no need for law when one had the "law of evolution," the "laws of capital," and the "laws of industrial society." As historian David Nasaw put it, the millionaires preached "democracy had its limits, beyond which voters and their elected representatives dared not trespass lest economic calamity befall the nation."[78]

George Orwell observed that the rhetorical silences and blatant contradictions of power are designed so that "to see what is in front of one's nose needs a constant struggle."[79] The tech companies' innovation rhetoric helped to suppress criticism from users and their lawmakers for many years, despite what was in front of their noses. Facebook and Google were regarded as innovative companies that sometimes make dreadful mistakes at the expense of privacy. Since then the picture has sharpened and we are getting better at seeing what's in front of our collective nose. It is now possible to recognize that what were once regarded as mistakes – Google Glass, Gmail scanning, Street View's theft of private data, Facebook's Beacon program, its sale of private information to developers, and more – were, in fact, the innovations.

The Freedom Defense

Lawmakers also have been held back in their work by confusion about the relationship between knowledge and freedom. Surveillance capitalists are no different from other capitalists in demanding freedom from any sort of constraint. They insist on the "freedom to" launch every novel practice while aggressively asserting the necessity of their "freedom from" law and regulation. This classic pattern reflects two bedrock assumptions about capitalism made by its own theorists: The first is that markets are intrinsically unknowable. The second is that the ignorance produced by this lack of knowledge requires wide-ranging freedom of action for market actors.

The notion that ignorance and freedom are twinborn characteristics of capitalism is rooted in the conditions of life before the advent of modern systems of communication and transportation, let alone global digital networks, the Internet, or the ubiquitous architectures of Big Other. Until the last few moments of the human story, life was necessarily local, and the "whole" was necessarily invisible to the "part."

Adam Smith's famous metaphor of the "invisible hand" drew on these enduring realities of human life. Each individual, Smith reasoned, employs his capital locally in pursuit of immediate comforts and necessities. Each one attends to "his own security . . . his own gain . . . led by an invisible hand to promote an end which was

[78] David Nasaw, "Gilded Age Gospels," in *Ruling America: A History of Wealth and Power in a Democracy*, eds. Steve Fraser and Gary Gerstle (Cambridge, MA: Harvard University Press, 2005), pp. 124–5, 148.

[79] Sonia Orwell and Ian Angus, *In Front of Your Nose 1945–1940: The Collected Essays, Journalism, and Letters of George Orwell*, vol. 4 (New York, NY: Harcourt, Brace & World, Inc., 1968), p. 125.

no part of his intention." That end is the efficient employ of capital in the broader market: the wealth of nations. The individual actions that produce efficient markets add up to a staggeringly complex pattern, a mystery that no one person or entity could hope to know or understand, let alone to direct: "The statesman, who should attempt to direct private people in what manner they ought to employ their capitals, would . . . assume an authority which could safely be trusted, not only to no single person, but to no council or senate whatever."[80]

The neoliberal economist Friedrich Hayek, whose work laid the foundation for the market-privileging economic policies of the past half century, drew the most basic tenets of his arguments from Smith's assumptions about the whole and the part. "Adam Smith," Hayek wrote, "was the first to perceive that we have stumbled upon methods of ordering human economic cooperation that exceed the limits of our knowledge and perception. His 'invisible hand' had perhaps better have been described as an invisible or unsurveyable pattern."[81]

In Hayek's framing, the mystery of the market is that a great many people can behave effectively while remaining ignorant of the whole. Individuals not only can choose freely, but they must freely choose their own pursuits because there is no alternative, no source of total knowledge or conscious control to guide them. "Human design" is impossible, Hayek says, because the relevant information flows are "beyond the span of the control of any one mind." The market dynamic makes it possible for people to operate in ignorance without "anyone having to tell them what to do."[82]

When it comes to surveillance capitalist operations, the classic quid pro quo of freedom for ignorance is shattered. The "market" is no longer invisible, certainly not in the way that Smith or Hayek imagined. The competitive struggle among surveillance capitalists produces the compulsion toward totality. Total information tends toward certainty and the promise of guaranteed outcomes. These operations mean that the supply and demand of human futures markets are rendered in infinite detail. Surveillance capitalism aims to replace mystery with certainty as it substitutes datafication, behavioral modification, and prediction for the old "unsurveyable pattern."

The result is a fundamental reversal of the classic ideal of the "market" as intrinsically unknowable. Now the market is visible. As the head of Facebook's data science team once reflected: "This is the first time the world has seen this scale and quality of data about human communication. For the first time, we have a microscope that . . . lets us examine social behavior at a very fine level that we've never been able to see before."[83] A top Facebook engineer put it more succinctly:

[80] Adam Smith, *The Wealth of Nations*, ed. Edwin Cannan (New York, NY: Modern Library, 1994), p. 485.

[81] Friedrich August von Hayek, *The Collected Works of Friedrich August Hayek*, ed. William Warren Bartley (Chicago, IL: University of Chicago Press, 1988), p. 14.

[82] Friedrich Hayek, "The Use of Knowledge in Society," in *Individualism and Economic Order* (Chicago, IL: University of Chicago Press, 1980). See the discussion on pp. 85–89.

[83] Tom Simonite, "What Facebook Knows," *MIT Technology Review*, June 13, 2012, https://www.technologyreview.com/s/428150/what-facebook-knows/.

"We are trying to map out the graph of everything in the world and how it relates to each other."[84] The same objectives are echoed in the other leading surveillance capitalist firms. As Google's Eric Schmidt observed in 2010: "You give us more information about you, about your friends, and we can improve the quality of our searches. We don't need you to type at all. We know where you are. We know where you've been. We can more or less know what you're thinking about."[85] Microsoft's Satya Nadella understands all physical and institutional spaces, people, and social relationships as indexable and searchable: all of it subject to machine reasoning, pattern recognition, prediction, preemption, interruption, and modification.[86]

Although there is nothing unusual about the prospect of capitalist enterprises seeking every kind of knowledge advantage in a competitive marketplace, the surveillance capitalist capabilities that translate ignorance into knowledge are unprecedented because they rely on the one resource that distinguishes the surveillance capitalists from traditional utopianists: the financial and intellectual capital that permits the actual transformation of the world, materialized in the continuously expanding architectures of Big Other. More astonishing still is that surveillance capital derives from the dispossession of human experience, operationalized in its unilateral and pervasive programs of rendering private experience as computational data.

This new condition unravels the economic justification for the triumph of raw capitalism: its free markets, free-market actors, and self-regulating enterprises. It suggests that surveillance capitalists mastered the rhetoric and political genius of the neoliberal ideological defense while pursuing a novel logic of accumulation that belies the most fundamental postulates of the capitalist worldview. It's not just that the cards have been reshuffled; the rules of the game have been transformed into something that is both unprecedented and unimaginable outside the digital milieu and the vast resources of wealth and scientific prowess that the surveillance capitalists bring to the table. Surveillance capitalism's command and control of the division of learning in society is the signature feature that breaks with the old justifications of the invisible hand and its entitlements. The combination of knowledge and freedom works to accelerate the asymmetry of power between surveillance capitalists and the societies in which they operate. This cycle will be broken only when we acknowledge as citizens, as lawmakers, as societies, and indeed as a civilization that surveillance capitalists know too much to qualify for freedom.

[84] Ashlee Vance, "Facebook: The Making of 1 Billion Users," *Bloomberg.com*, October 4, 2012, http://www.bloomberg.com/news/articles/2012–10-04/facebook-the-making-of-1-billion-users.

[85] Derek Thompson, "Google's CEO: 'The Laws Are Written by Lobbyists,'" *Atlantic*, October 1, 2010, https://www.theatlantic.com/technology/archive/2010/10/googles-ceo-the-laws-are-written-by-lobbyists/63908/.

[86] Shoshana Zuboff, "The Road to Digital Serfdom? The Visible Hand of Surveillance Capitalism," *Promarket*, February 22, 2019, https://promarket.org/road-to-digital-serfdom-surveillance-capitalism-visible-hand/.

The Success Defense

A third propaganda strategy is the argument that the financial success of the leading surveillance capitalist firms reflects the real value they bring to people. In this view, financial success is prima facie evidence that no laws are required. But data from the demand side evident in a range of research conducted over the last decade and a half suggest a more disturbing picture. In forty-six of the most prominent forty-eight opinion surveys on the subject of privacy administered in the US and Europe between 2008 and 2016, substantial majorities support measures for enhanced privacy and user control over personal data. (Only two early surveys were somewhat less conclusive, because so many participants said they did not understand how or what personal information was being gathered.)

By 2008 it was well established that the more information people have about "Internet privacy practices," the more they are "very concerned" about privacy.[87] A major 2009 survey found that when people were informed of the ways that companies gather data for targeted online ads, more than 73 percent rejected such advertising.[88] A substantial 2015 survey found 91 percent of respondents disagreed that the collection of personal information "without my knowing" was a fair trade-off for a price discount.[89] Fifty-five percent disagreed that it was even a fair exchange for improved services. By late 2019 the disjuncture was even more pronounced: An important survey from PEW Research reported that 81 percent of Americans believe the potential risks of companies' data collection outweigh the benefits, compared to 66 percent who felt that way about government data collection.[90] A similar Swedish study in 2020 found that 55 percent of Swedes were most concerned about data collection by private companies, compared to 11 percent concerned about government data collection.[91]

The surveillance capitalist firms typically dismiss these results, pointing instead to users' actual behavior and the spectacular revenues it produces as justification for

[87] Chris Jay Hoofnagle and Jennifer King, "Research Report: What Californians Understand About Privacy Offline," *SSRN*, May 15, 2008 (Rochester, NY: Social Science Research Network), http://papers.ssrn.com/abstract=1133075.

[88] Joseph Turow et al., "Americans Reject Tailored Advertising and Three Activities That Enable It" (Annenberg School for Communication, September 29, 2009), http://papers.ssrn.com/abstract=1478214.

[89] Joseph Turow, Michael Hennessy, and Nora Draper, "The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them Up to Exploitation," Survey Results (Pennsylvania, PA: Annenberg School for Communication, June 2015), https://www.asc.upenn.edu/news-events/publications/tradeoff-fallacy-how-marketers-are-misrepresenting-american-consumers-and.

[90] Brooke Auxier et al., "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information," *Pew Research Center: Internet, Science & Tech* (blog), November 15, 2019, https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[91] Markus Lahtinen, "Big Tech Greater Threat to Privacy than Big Brother," Lund University School of Economics and Management, January 23, 2020, https://lusem.lu.se/news/big-tech-greater-threat-to-privacy-than-big-brother.

the status quo. Recall former Google CEO Eric Schmidt's infamous 2009 privacy brushoff: "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place."[92] Scholars have called the gap between attitudes and behavior "the privacy paradox," but there really is no paradox here, only the predictable consequence of the pitched battle between supply and demand expressed in the difference between what surveillance capitalism imposes on people and what they really want.[93]

The data suggest that surveillance capitalism is best understood as a market failure that would not survive a genuinely competitive commercial environment. Few people who get a glimpse of surveillance capitalism's hidden operations actually want to be their target. Most want an alternative path to the digital future, one that will fulfill their needs without compromising privacy and usurping epistemic rights. This is one of those disjunctures in economic history, when nearly everyone wants something that they cannot have, just as early twentieth-century farmers and shopkeepers wanted automobiles too, but at a price they could afford. Instead of a close alignment of supply and demand, people use surveillance capitalism's services because they have no comparable alternatives and because they are ignorant of its shadow operations and their consequences. Corporate success is best understood as the result of coercion and obfuscation, practices that are only sustainable when they are conducted in secret.

Surveillance capitalism has thrived in the absence of law and regulation. Rather than mourning this state of affairs, the lack of prior action may be regarded as a positive. Democracy has not failed to reign in this rogue capitalism, it has simply not yet tried. And further, democratic societies have successfully confronted destructive forms of raw capitalism in the past, asserting new laws that tethered capitalism to the needs of people and democratic values. Democracy moderated some of the excesses of early industrialization. It ended the Gilded Age. It mitigated the destruction of the Great Depression. It built a strong post-War society. It protected earth, creatures, water, air, consumers, and workers.

According to Lawrence Friedman's history of American law in the twentieth century, the appetite for new law and regulation in the 1930s came from decades of anger, frustration, outrage, and helplessness at the growing scale and complexity of the industrial behemoths.[94] Only law was up to the task of tethering the giant industrial corporations to the needs of a democratic society. The swell of survey data,

[92] Richard Esguerra, "Google CEO Eric Schmidt Dismisses the Importance of Privacy," *Electronic Frontier Foundation*, 10 December 2009, https://www.eff.org/deeplinks/2009/12/google-ceo-eric-schmidt-dismisses-privacy.

[93] Susanne Barth and Menno D. T. de Jong, "The Privacy Paradox—Investigating Discrepancies between Expressed Privacy Concerns and Actual Online Behavior: A Systematic Literature Review," *Telematics and Informatics* 34, no. 7 (November 2017): 1038–58, https://doi.org/10.1016/j.tele.2017.04.013.

[94] Lawrence M. Friedman, *American Law in the 20th Century* (New Haven, CT: Yale University Press, 2004).

the gradual awakening to surveillance capitalism's mass communication tactics, and the drumbeat of novel legislative and regulatory discussions and initiatives appears to point in a similar direction. The question remains: What is to be done? What kinds of new law and regulation are likely to be effective? Will it be comprehensive privacy legislation? Will it be an antitrust approach, as many counsel? McCraw's warning suggests that we need new economic, legal, and collective action paradigms born of a close understanding of surveillance capitalism's economic imperatives and foundational mechanisms.

Privacy and antitrust law are vital, but there is reason to believe that neither will be wholly adequate to this new challenge. An example is privacy law's call for "data ownership" and related data rights. Such formulations legitimate the original sin that is the theft of human experience for rendition into data in the first instance. All discussions that begin with existing data flows serve to institutionalize that theft. Negotiating data ownership is like negotiating how many hours a day a seven-year-old should be allowed to work in a factory, rather than contesting the fundamental legitimacy of child labor. Data rights also fail to reckon with the realities of behavioral surplus. Even if "users" achieve "ownership" of the data that they provided to a company, they will not achieve "ownership" of the behavioral surplus that floods the shadow text, the predictions gleaned from it, or the fate of those predictions in markets that trade in human futures. Finally, data ownership is a recipe for a new epistemic underclass, in which economically disadvantaged individuals, families, and groups sell their data in the same way that one might sell one's organs in an illicit market. The Google contractors who induced homeless people of color to "sell" their faces for $5 offered a portent of that bleak future.

The prospect of "breaking up" the largest surveillance capitalist firms also fails to reckon with the actual mechanisms of this economic logic. Surveillance capitalists achieve scale by cornering behavioral surplus supplies and driving up the value chain for more predictive forms of surplus. If there are monopolies here, they are monopolies of behavioral surplus supplies, of scientific labor, and of material infrastructures for predictive analytics. These features do not correspond neatly to conventional monopoly criteria, neither do they reflect the conventional categories of "consumer harms" that most antitrust laws are designed to combat.

It is necessary to rethink the meaning of "size" and "monopoly" when a company with relatively few employees but huge capital reserves can corner data flows from large domains of human experience (e.g., "search" or "social networking") while simultaneously cornering the capabilities to compute those data flows. Assistant Attorney General Makan Delrahim offered an initial analysis of such distinctions in 2019 noting: "Broadly speaking, in some digital markets, the competition is for user attention or clicks. If we see the commercial dynamics of Internet search, for example, in terms of the Yellow Pages that were delivered to our doors a generation ago, we cannot properly assess practices and transactions that create, enhance, or entrench market power – and in some cases monopoly

power."[95] Breaking up the largest surveillance capitalists – Google, Facebook, Microsoft, and Amazon – can address important anti-competitive problems, but without measures tailored to the actual mechanisms of surveillance capitalism, it will not prevent the emergence of smaller and more efficient surveillance capitalist firms, while opening the field for new surveillance capitalist competitors.

The most efficient legislative and regulatory strategies would be aimed at disrupting the surveillance dividend by disrupting the raw material supplies and financial incentives that sustain it. In other words, it means legislative and regulatory strategies that interrupt and in some cases outlaw surveillance capitalism's mechanisms of supply and demand. Such measures would create space for alternative citizen-based and commercial action, building ecosystems that realign with individual needs and democratic practice.

***Supply*:** The relentless expansion of extractive supply chain operations is only likely to be constrained when the legal and regulatory focus shifts from data ownership and management to the originating processes of datafication: the secret theft of private human experience as free raw material for rendition into data. The boundary in dispute must move upstream, from contest over data as property to the codification of epistemic rights that link individual sovereignty to inalienable rights of self/knowledge and establish a rights-based moat around private experience.

This codification of epistemic rights to self/knowledge would interrupt data supply chains by safeguarding the boundaries of human experience before they come under assault from the forces of datafication. It assigns the choice to turn any aspect of one's life into data as a right that adheres to individuals and communities by virtue of law sustained by democratic governance and as an extension of elemental rights now explicated and translated into juridical rights. This means, for example, that companies cannot claim the right to your face as you walk down the street, or use your face as free raw material for analysis, or fabricate, own, or sell any computational products that derive from your face and its depths of personal information. Such epistemic rights can be understood as the cornerstone of individual freedom under twenty-first-century conditions of existence.

The conversation on epistemic rights has already begun. In the absence of a comprehensive epistemic right to self/knowledge, for example, legal scholars, practitioners, and neural scientists have begun to frame epistemic rights claims to "freedom of thought." They cite the sanctity of the "forum internum," the interior space of human awareness and thought, and the need for codified individual rights that protect this domain of human experience from unwanted intrusion, theft, and

[95] Makan Delrahim, "Assistant Attorney General Makan Delrahim Delivers Remarks for the Antitrust New Frontiers Conference," United States Department of Justice, June 11, 2019, https://www.justice.gov/opa/speech/assistant-attorney-general-makan-delrahim-delivers-remarks-antitrust-new-frontiers.

manipulation.[96] Some of this work is a direct response to surveillance capitalism's unrelenting drive to eliminate every barrier to the datafication of human experience, including recent breakthroughs in translating brain signals into speech.[97] Columbia University is home to a "neurorights initiative,"[98] the OECD issued formal recommendations for "responsible innovation in neurotechnology,[99] and Amnesty International issued a path-breaking report on the human rights implications of the "surveillance business model."[100] As contests over epistemic rights multiply, there is a strong likelihood that surveillance assets will be reinterpreted as toxic "fruit of the poisonous tree" that can only be acquired at the price of fundamental epistemic rights.

Demand: The opportunity on the demand side is to disrupt or eliminate the financial incentives that sustain the surveillance dividend. This can be accomplished with sanctions that outlaw the trade in human futures. This is not a radical prospect. For example, societies outlaw markets that trade in human

[96] Examples include, Susie Alegre, "Using Freedom of Thought to Limit 'Surveillance Capitalism'?" Doughty Street Chambers (blog), July 3, 2019, https://insights.doughtystreet.co.uk/post/102fn86/using-freedom-of-thought-to-limit-surveillance-capitalism; Susie Alegre, "Time to Think about Freedom of Thought," *International Law Bulletin*, November 2017, https://doughty-street-chambers.newsweaver.com/International/rn8wy1p800g?a=1&p=2047237&t=174031; Marcello Ienca and Roberto Andorno, "Towards New Human Rights in the Age of Neuroscience and Neurotechnology," *Life Sciences, Society and Policy* 13 (April 26, 2017), https://doi.org/10.1186/s40504-017–0050-1.

[97] Antonio Regalado, "Facebook Is Funding Brain Experiments to Create a Device That Reads Your Mind," *MIT TechnologyReview*, July 30, 2019, https://www.technologyreview.com/s/614034/facebook-is-funding-brain-experiments-to-create-a-device-that-reads-your-mind/; Sigal Samuel, "Facebook Is Building Tech to Read Your Mind. The Ethical Implications Are Staggering.," *Vox*, August 5, 2019, https://www.vox.com/future-perfect/2019/8/5/20750259/facebook-ai-mind-reading-brain-computer-interface; David A. Moses et al., "Real-Time Decoding of Question-and-Answer Speech Dialogue Using Human Cortical Activity," *Nature Communications* 10, no. 1 (July 30, 2019): 1–14, https://doi.org/10.1038/s41467-019–10994-4; Sigal Samuel, "Brain-Reading Tech Is Coming. The Law Is Not Ready to Protect Us," *Vox*, August 30, 2019, https://www.vox.com/2019/8/30/20835137/facebook-zuckerberg-elon-musk-brain-mind-reading-neuroethics; "Surge in US 'Brain-Reading' Patents," *BBC News*, May 7, 2015, sec. Technology, http://www.bbc.com/news/technology-32623063; Anderson Cooper, "What Is 'Brain Hacking'? Tech Insiders on Why You Should Care," *CBS News*, April 9, 2017, https://www.cbsnews.com/news/brain-hacking-tech-insiders-60-minutes/; Christopher N. Cascio, Christin Scholz, and Emily B. Falk, "Social Influence and the Brain: Persuasion, Susceptibility to Influence and Retransmission," *Current Opinion in Behavioral Sciences* 3 (June 2015): 51–57, https://doi.org/10.1016/j.cobeha.2015.01.007; Kiyoto Kasai et al., "The Future of Real-World Neuroscience: Imaging Techniques to Assess Active Brains in Social Environments," *Neuroscience Research* 90 (January 2015): 65–71, https://doi.org/10.1016/j.neures.2014.11.007; "Brain-Connected Computers," *Week*, July 28, 2017.

[98] "NeuroRights Initiative," accessed February 23, 2020, https://nri.ntc.columbia.edu/.

[99] "New Frontiers of the Mind: Enabling Responsible Innovation in Neurotechnology," The OECD Forum Network, December 19, 2019, http://www.oecd-forum.org/users/338762-david-winickoff/posts/57641-new-frontiers-of-the-mind-enabling-responsible-innovation-in-neurotechnology.

[100] Amnesty International, "Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights" (2019), https://amnestyusa.org/wp-content/uploads/2019/11/Surveillance-Giants-Embargo-21-Nov-0001-GMT-FINAL-report.pdf.

organs, babies, and slaves. In each case, such markets are recognized as morally repugnant operations that produce predictably violent consequences and violate democratic principles. Human futures markets can be shown to produce equally predictable outcomes that challenge human freedoms, violate epistemic rights, and undermine democracy.

****

Consider the Aware Home, a collaboration between computer scientists and engineers in the year 2000, intended as a "living laboratory" for the study of "ubiquitous computing."[101] The project envisioned a "human-home symbiosis" in which animate and inanimate processes would be captured by an elaborate network of "context aware sensors" embedded in the house and by wearable computers worn by the home's occupants. The Aware Home information system was designed as a simple closed-loop controlled entirely by the home's occupants. Because the house would be "constantly monitoring the occupants' whereabouts and activities . . . even tracing its inhabitants' medical conditions," the engineers concluded, "there is a clear need to give the occupants knowledge and control of the distribution of this information." All the information was to be stored on the occupants' wearable computers "to insure the privacy of an individual's information."

In 2017 University of London scholars published a detailed analysis of a single "smart home" device, the Google-owned Nest thermostat.[102] They determined that the purchase of a single Nest thermostat entails the need to review nearly 1,000 so-called "contracts," each with its own burdensome and audacious terms of service for third-party data sharing.[103] Should the customer refuse to agree to Nest's stipulations, the Terms of Service indicate that the functionality and security of the thermostat may be deeply compromised, no longer supported by the necessary updates meant to ensure its reliability and safety. The consequences can range from frozen pipes to failed smoke alarms to an easily hacked internal home system.[104]

Today we might mourn the innocence of the Aware Home but, like a message in a bottle from a bygone age, it tells us something important. Once we were the

[101] Cory D. Kidd et al., "The Aware Home: A Living Laboratory for Ubiquitous Computing Research," in *Proceedings of the Second International Workshop on Cooperative Buildings, Integrating Information, Organization, and Architecture*, CoBuild '99 (London: Springer-Verlag, 1999), pp. 191–98, http://dl.acm.org/citation.cfm?id=645969.674887.

[102] Ron Amadeo, "Nest Is Done as a Standalone Alphabet Company, Merges with Google," *Ars Technica*, February 7, 2018, https://arstechnica.com/gadgets/2018/02/nest-is-done-as-a-standalone-alphabet-company-merges-with-google/; Leo Kelion, "Google-Nest Merger Raises Privacy Issues," *BBC News*, February 8, 2018, sec. Technology, http://www.bbc.com/news/technology-42989073.

[103] Guido Noto La Diega, "Contracting for the 'Internet of Things': Looking into the Nest," Research Paper (London: Queen Mary University of London, School of Law, 2016); Robin Kar and Margaret Radin, "Pseudo-Contract & Shared Meaning Analysis," *SSRN* (November 16, 2017), https://papers.ssrn.com/abstract=3083129.

[104] Grant Hernandez, Orlando Arias, Daniel Buentello, and Yier Jin, "Smart Nest Thermostat: A Smart Spy in Your Home," *Black Hat USA* (2014), https://www.blackhat.com/docs/us-14/materials/us-14-Jin-Smart-Nest-Thermostat-A-Smart-Spy-In-Your-Home-WP.pdf.

subjects of our lives, now we are its objects. We once looked to the digital future as a human future – a place we could call home. The Aware Home is testimony to what we have lost and what we can find again: the rights to know and decide who knows and decide who decides who knows about our lives: Individual epistemic sovereignty, law, and democracy. Such rights and principles have been and remain the only possible grounds for human freedom, a functional democratic society, and an information civilization founded on equality and justice.