HARVARD UNIVERSITY

GRADUATE SCHOOL OF BUSINESS ADMINISTRATION

GEORGE F. BAKER FOUNDATION

SHOSHANA ZUBOFF
Charles Edward Wilson Professor of Business Administration, Emeritus

PRIVACY MUST FALL
Surveillance Capitalism and the Meaning of Privacy Law After Privacy

Written testimony of
Professor Shoshana Zuboff

Before the
Committee on House Administration
U.S. House of Representatives

For the hearing on
Big Data: Privacy Risks and Needed Reforms in the Public and Private Sectors

February 16, 2022

Chair Lofgren, Ranking Member Davis, and members of the Committee, thank you for this opportunity to discuss the challenges of privacy law in a world without privacy.

I have spent forty-three years studying the rise of the digital as an economic force driving our transformation into an information civilization. Over these last two decades, I've observed the consequences as fledgling internet companies morphed into surveillance empires founded on the premise that *privacy must fall* and powered by global operations of behavioral monitoring, analysis, targeting, modification, and prediction that I have called 'surveillance capitalism'.[1]

I. A Tragedy of the Uncommons

In this written testimony, I pose the following questions to the Committee on House Administration: What kind of legislative action is required to protect privacy in the aftermath of its wholesale destruction? What is the nature and purpose of privacy law after privacy? While

these questions and their answers beg explanation, I confine myself here to the essential points necessary for meaningful deliberation.

In an information civilization, societies are defined by questions of knowledge — how it is distributed, the authority that governs its distribution, and the power that protects that authority. *Who knows? Who decides who knows? Who decides who decides who knows?* Surveillance capitalists now hold the answers to each question, though we never elected them to govern. They claim the authority to decide 'who knows' by asserting ownership rights over human-generated information, and they defend that authority with the power to control critical information spaces, systems, and infrastructures.[2] On the strength of their surveillance capabilities and for the sake of their surveillance profits, the new empires engineered an anti-democratic *epistemic coup* — a takeover of knowledge and knowing — marked by unprecedented concentrations of knowledge about individual and collective behavior along with the unaccountable power that accrues to such knowledge.

The world's liberal democracies now confront a tragedy of the 'un-commons,' as mission-critical information and communication spaces and functions have been ceded to surveillance capital. Digital territories that most people have assumed to be public are now owned, operated, and mediated by private commercial interests for maximum profit while almost entirely unconstrained by public law. All roads to economic and social participation now lead through surveillance capitalism's institutional terrain, a condition that has intensified during nearly two years of global plague. The abdication of these spaces to surveillance capitalism has become the meta-crisis of every republic because it obstructs solutions to all other crises. No democracy can survive these conditions.

This third decade demands a reckoning with the most basic questions of the digital century: how do we reinvent the operations and governance of information and communication in ways that sustain and advance democratic values, principles, and aspirations? The liberal democracies skipped this most crucial step at the dawn of the information age, leaving a void that was filled by surveillance capital.

The result is the feeling that we've stumbled into a future that we did not and would not choose, one that is increasingly ruled by the antidemocratic and unaccountable power of surveillance capitalism. A sure test of this statement is that when our young people and our artists contemplate the future, they invariably assume the overriding presence of omniscient dystopian power. This must not be our legacy.

I begin this discussion by defining surveillance capitalism as an economic logic that depends upon the destruction of privacy as a condition of its success. I then briefly discuss the historical conditions that enabled this surprising economics to root and flourish. Next, I examine the stages of surveillance capitalism's development from its origins in the destruction of individual privacy to its current status as a sweeping institutional order vying with democracy over the principles and laws that will govern society. With these elements identified, I consider the legislative and institutional challenges of this third decade and their bearing upon the renewal of privacy as a necessary condition of a democratic digital century.

II. What is Surveillance Capitalism?

Surveillance capitalism maintains core elements of traditional capitalism: private property, market exchange, growth and profit, but these cannot be realized without the technologies and social relations of surveillance. So, here is the startling new economics of surveillance capitalism: Hidden methods of observation secretly extract human experience once considered private and translate it into behavioral data. These methods operate outside of human awareness, robbing actors of the right to know and, with it, the right to combat. In an extraordinary development, these ill-gotten human data are then immediately claimed as corporate property available for manufacture and sales. The theory of surveillance capitalism challenges this property claim and redefines it as theft.

Human data thus extracted join complex supply chains and travel to computational factories, known as "machine learning" or "artificial intelligence," where they are computed into behavioral predictions and targeting algorithms. Predictions are ultimately sold to business customers in a new kind of market that trades in predictive knowledge of human behavior. These are commodity markets in human futures akin to markets in pork belly futures, or wheat, or oil. Surveillance capitalists sell certainty, which demands data extraction at a massive scale that is impossible to grasp. A leaked 2018 Facebook document provides a glimpse.[3] The company describes its "prediction engine" that "ingests trillions of data points every day," to produce thousands of "models," and its "prediction service" that churns out "more than 6 million predictions per second."

Surveillance capitalism developed into a global institutional order in only two decades, in part because of the many ways in which it learned to persuade America and the world of its inevitability. Nevertheless, this institution was and is anything but inevitable. Its success is owed to action and choice. People made it. Chance made it. Ideology, economics, and politics made it.

The year was 2000, when a mere 25% of the world's information was stored digitally, and a tiny but brilliant Silicon Valley internet startup called Google faced ruin from the financial crisis known as the dotcom bust. Even as Google's search engine was considered the best, founders Larry Page and Sergey Brin faced extreme pressure from their powerful venture capitalist investors. The company had not yet found a way to turn search into money, and their backers insisted on a fast track to monetization.

Between 2000 and 2001, the Google team stumbled into a series of discoveries that revealed the rich predictive signals embedded in the "data exhaust" left over from users' search and browsing activities, signals that could be aggregated and analyzed to predict user behavior. This leftover behavioral data was a *surplus*, more than what was required for product improvement. The founders had argued that advertising would corrupt the search experience, but financial emergency created a state of exception, and they suspended their principles.[4] Advertising became their lifeboat as they learned how to analyze behavioral surplus to predict click-through rates, the solid gold that launched their vast and lucrative online ad markets.

Surveillance is the keystone of this economic foundation. From the start, data scientists and engineers understood that these operations would have to be hidden, lest they risk user rebellion

or lawmakers' anger. Soon, its scientists were inventing ways to surveil and capture behavioral surplus across the internet without leaving a trace, proud of their ability to construct, infer, and deduce user profiles with insights that individuals never chose to disclose — personality, sexual orientation, political leanings … and much more. Later, the mobile revolution would move these secret extraction activities into the real worlds of everyday life. Such hidden-taking-without-asking is normally characterized as theft, and it is on the strength of this secret theft that 'users' once private lives are transformed into others' proprietary assets.

The discovery of behavioral surplus and the related sciences of inference, computation, modeling, algorithms, prediction and targeting known loosely as 'artificial intelligence' undermine the validity of rational choice theory or the contractual integrity of notice and consent. One may exercise rational choice in the decision to share specific information with a platform, but that information is an insignificant drop in the ocean of surplus that is hunted and captured and delivered to sophisticated machine procedures to produce more surplus. I cannot make a rational choice about what is concealed from me – the known unknown.

Google had been a technology company. Its business plan called for selling search engine licenses to large internet companies and other corporate clients. It even produced a device, the "Google Search Appliance," to help companies locate information in their own databases.[5] All of that was swept away.

Founder Larry Page laid it out in 2001, shortly after the breakthrough that would change everything. "If we did have a category," Page ruminated, "it would be personal information … The places you've seen. Communications … Sensors are really cheap … Storage is cheap. Cameras are cheap. People will generate enormous amounts of data … Everything you've ever heard or seen or experienced will become searchable. Your whole life will be searchable."[6]

Instead of selling search to users, Google would achieve revenue growth by searching its users and seizing whatever it found. Escape from financial ruin, it was decided, depended upon turning Google's search engine into a sophisticated surveillance medium for the massive-scale seizure of human-generated data.

Privacy did not disappear, exactly. Instead, it was expropriated from people and concentrated in the corporate domain. Google used its capabilities in surveillance to keep the new economic operations secret. Founders and executives were determined to hide their breakthrough from competitors, but they also feared that users would rebel against corporate mass surveillance. Worst of all was the anxiety that lawmakers might be stirred to action. According to the company's first brand manager, Douglas Edwards, Page opposed anything that might "stir the privacy pot and endanger our ability to gather data." He even questioned the prudence of the legendary electronic ticker display in the company's Mountain View lobby, and its continuous stream of search queries.[7]

Page also wanted to hide the astonishing financial implications of Google's invention. Between 2001, when the new economics of surveillance advertising were first applied, and 2004, when Google went public, its revenues increased by 3,590 percent. This 'surveillance dividend'

established the secret massive-scale extraction of human-generated data as the foundation of a new economic order.

Facebook was Google's first follower. Like Google a few years earlier, its founder Mark Zuckerberg had not found a way to turn popularity into profit. He changed his destiny in 2008 by hiring Sheryl Sandberg as his second in command. Sandberg had joined Google in the breakthrough year of 2001 and became a key leader of the surveillance capitalism advertising revolution. She led the build-out of Google's advertising engine, AdWords, and its AdSense program, which together accounted for most of the company's $16.6 billion revenues in 2007.[8]

By the mid-2010s, surveillance economics had become the default economic model in the tech sector. Success drew surveillance economics inexorably into the 'normal' economy, where it has continued to migrate and reorder diverse sectors from insurance, retail, banking and finance to agriculture, automobiles, education, healthcare and more. Every product called "smart," and every service called "personalized" are loss leaders for the human data that flow through them. Today every 'app,' no matter how apparently benign, is designed as a data mule, shuttling personal information from devices to the servers at Google, Facebook, and ad tech companies. As one Silicon Valley executive recently described it to me, "The underlying norm of virtually all software and apps design now is data collection. All software design assumes that all data should be collected, and most of this occurs without the user's knowledge." Extraction operations and their supply chains range far beyond their original settings on computers, laptops, and smartphones to cities and villages, buildings and roads, homes and cars — every form of activity in every domain of daily life.

Among the five leading surveillance capitalist corporations — Google, Facebook, Amazon, Apple, and Microsoft — each participates in surveillance advertising and surveillance economics, though the specifics of their business models vary. Google and Facebook are data companies and surveillance-advertising "pure plays" whose revenues derive almost entirely from surveillance advertising markets.[9] The others have multiple lines of business that include varying configurations of data, services, software, and-or physical products. Despite these distinctions, all five contribute to, benefit from, and build upon surveillance capitalism's institutional strategies, operations, and revenues in conjunction with their complex ecosystems, the ad tech behemoths, the telcos, the internet service providers, and a growing majority of market-based organizations across the commercial universe. It is therefore not surprising that in 2021 the five giants were also five of the six largest publicly traded companies by market capitalization in the world.[10]

III. Windfall

Nothing was inevitable. Ours is an accidental dystopia.

Surveillance capitalism is neither a technology nor a corporation nor an executive. It is a political-economic institution that owes its existence to a windfall of unique economic, political, ideological, and material conditions that permitted this extractive economic logic to root and

flourish. I have documented these conditions in detail in other work, and here I shall mention only a few highlights.[11]

In 1970, three years before Larry Page's birth, the *New York Times Magazine* lent its prestigious pages to "A Friedman Doctrine," the libertarian call to arms giving popular voice to a radical free market world view that would be essential to Page's, and surveillance capitalism's, astounding success.[12] "There is one and only one social responsibility of business," the University of Chicago economist thundered, "to use its resources and engage in activities designed to increase its profits …"

Friedman was a self-described "extremist" partial to sharp dualisms, absolutes, and unequivocal policy positions that frequently triggered public controversy.[13] His ideology was forged in the aftermath of World War II as a response to the collectivist nightmares of German and Soviet totalitarianism. As the old central planning enemies receded, new ones took their place: the regulatory powers of the democratic state, its social legislation and welfare policies, labor unions and the institutions of collective bargaining, and principles of equality and justice. These were replaced by the market's version of truth. Growth would be accelerated by unimpeded market competition sustained by supply-side reforms, including comprehensive deregulation, privatization, and lower taxes.

By mid-decade, as the Nixon and then the Ford White House searched for a way out of the stagflation crisis, Professor Friedman advised both Presidents. By 1979 he was economic advisor to Presidential candidate Ronald Reagan, a relationship that endured throughout Regan's presidency. President Reagan and British Prime Minister Margaret Thatcher famously established Friedman's radical free market doctrine as governmental policy. The market must rule. Democratic institutions must recede.

From the start, the internet and its commerce were claimed for Friedman's radical freedom, and the overarching theme of internet-related governmental policy was "self-regulation" for the sake of Friedman-style profit maximization. This ideological zeitgeist dominated those crucial post-World Wide Web years of the mid to late 1990s finding iconic expression in a 1997 Clinton-Gore whitepaper.[14] The Administration's policy vision for "Global Electronic Commerce" begins with its primary principle: "The private sector should lead." The Google founders became the unwitting heirs apparent of the Friedman Doctrine.

The report denigrated to the point of caricature government's role and capabilities in the governance of digital information and communication spaces, insisting on "minimal government involvement or intervention … Existing laws and regulations that may hinder electronic commerce should be reviewed and revised or eliminated ..." The Administration's approach was not only to get out of the way, but to proactively cede whole governance functions to the internet companies. When it came to privacy protections, the whitepaper's prescriptions rested on formulations that even in 1997 were not easily defensible. This shortfall became more dangerous once the science of behavioral surplus extraction, inference, and computation was invented. The Clinton-Gore framework left 'users' naked at the altar of the rational choice theory assumed in the whitepaper's advocacy of privacy protections such as, "market resolution of privacy concerns by empowering individuals to obtain relevant knowledge," "self-regulatory privacy regimes,"

"industry-developed solutions to privacy problems," and "market driven mechanisms to assure customer satisfaction about how private data is handled."

By 2000, however, a majority of FTC commissioners, including Chair Robert Pitofsky, concluded that self-regulatory initiatives "cannot ensure that the online marketplace as a whole will follow the standards adopted by industry leaders ... notwithstanding several years of industry and governmental effort." In their report to Congress, the Commissioners cited the explosion of secret online tracking and monitoring for chasing eyeballs with new hidden methods like "cookies" and "web bugs."[15] They noted that a mere 8 percent of popular websites featured a seal of approval from one of the internet industry's privacy watchdogs, intended as an important mechanism for self-regulation.

The report argued that only federal law could protect online consumers. Proposed stipulations included clear and conspicuous notice of information practices; consumer choice over how personal information is used; individuals' access to all personal information including rights to correct or delete; and enhanced security of personal information.[16] Even these basic privacy protections would have set America and the world on a different path to the digital century, but history, contingency, and chance had other plans: September 11, 2001.

According to Peter Swire, chief counselor for Privacy in the Clinton Administration and later a member of President Barack Obama's Review Group on Intelligence and Communication Technologies, "With the attacks of September 11, 2001, everything changed. The new focus was overwhelmingly on security rather than privacy."[17] The legal provisions debated just months earlier vanished from the conversation more or less overnight, giving way to a new preoccupation with "Total Information Awareness."

Friedman's ideology of radical market freedom took care of the supply side, shielding the nascent surveillance capitalist firms from laws that would have curbed the destruction of privacy and all that followed from it. Then, 9/11 thrust the intelligence community, the US government, and, indeed, governments around the world into an unfamiliar demand curve, mobilized by outrage and anxiety. In America, a 'state of exception' was invoked to unleash a new human data imperative: velocity and volume at any price. In this new environment "Congress lost interest in regulating information usage in the private sector," Swire recalls. "Without the threat of legislation, the energy went out of many of the self-regulatory efforts that industry had created."[18]

In the US and across the EU, legislation was quickly put in place that decisively expanded surveillance activities.[19] Instead of federal legislation to outlaw the novel surveillance practices, the new aim was to enrich the conditions for their expansion and application outside constitutional, legal, and regulatory constraints. Yale legal scholar Jack Balkin explained that while the US Constitution inhibits surveillance by government actors, privacy protections for information held in private servers is "limited if not nonexistent." If the intelligence community was to indulge its obsession to ascertain the future, then it would have to "rely on private enterprise to collect and generate information for it."[20]

Google took the lead and in the process surveillance capital was given a free pass to invent, own, and operate the twenty-first century production, concentration, and use of human-generated data. By 2010, former NSA director Mike McConnell publicly acknowledged that collaboration was inevitable noting, "With more than 90 percent" of the physical infrastructure of the web "owned by private industry … the challenge is to shape an effective partnership with the private sector so information can move quickly back and forth from public to private …"[21]

IV. Our Accidental Dystopia: Surveillance Capitalism's Stages of Development

Most of us are whipsawed by each day's headlines bleating the latest atrocity: the loss of privacy, the spread of disinformation, collective-scale behavioral modification. The issues are siloed, fragmented. We are forever trying to grasp the elephant while fixating on its parts, leaving us in a tangle of disorientation and confusion with little grasp of economic cause and social harm effect. If we have learned anything from this state of affairs, it's that we cannot fix what we do not understand.

The value of reinterpreting surveillance capitalism as a developing institutional order is that this tower of Babel finally resolves into a coherent picture – linked effects of a unitary process evolving in time. Each stage is defined by more complex economic operations that cause new social harm effects and enable the absorption of new governance functions. Each stage creates the conditions for the next. Each builds on what went before. Seemingly disparate social harms are organically related in time – the effects of economic operations also related in time. This picture alerts us to the ways in which effective remedies for later stage social harms depend upon changing early-stage operational causes. In other words, the durable solutions lie upstream, where this river originates.

Four stages of surveillance capitalism's institutionalization are visible thus far: Extraction, Expropriation, Exploitation, and Enforcement. I'll describe them briefly.

Stage One: Extraction
The first stage introduces the secret massive-scale extraction of human generated data, the formative achievement that lays the economic foundation for all that follows. Human-generated data are concentrated in the surveillance capitalist order.

And there is no law to stop it.

Stage Two: Expropriation
In his 1967 dissenting opinion in the Fourth Amendment case of Warden v. Hayden, Justice William O. Douglas wrote, "Privacy involves the choice of the individual to disclose or to reveal what he believes, what he thinks, what he possesses ... Those who wrote the Bill of Rights believed that every individual needs both to communicate with others and to keep his affairs to himself. That dual aspect of privacy means that the individual should have the freedom to select for himself the time and circumstances when he will share his secrets with others and decide the extent of that sharing."[22]

Douglas's "freedom to select" alerts us to a class of rights that precede privacy, and the enactment of such rights are the proximate cause of privacy. These rights to know are 'epistemic rights,' which in modern democratic societies have been considered inalienable and elemental rights of individuals. With the secret seizure of human data from domains of experience that have long been considered private, the epistemic rights embedded in Douglas's "freedom to select" are expropriated and accumulated as corporate rights. Because privacy is an effect of this "freedom to select," the expropriation of epistemic rights eliminates the privacy choice. This dynamic clarifies the advancement of stage two from concentrations of human data, to concentrations of epistemic rights, to concentrations of privacy, to concentrations of recently private knowledge about people as corporate property.

These concentrations are not metaphorical. They reflect elaborate infrastructures of material and people. For example, a comprehensive review of AI's global institutional structure concludes that the artificial intelligence landscape is almost entirely controlled by "big tech." These firms evangelize AI because they stand to benefit from improvements in their own businesses. Some of the vertical ecosystems have gone global as "scale begets learning through the accumulation of data and increases competitive advantage". The surveillance capitalist giants control the capital, the data, the technologies, the scientists, and the science. They acquire most AI firms and poach most AI talent. Consistent with the structure of concentration in these corporations, the report observes that "Secrecy rather than patenting remains the preferred strategy to protect their research findings."[23]

The social harm effects are the wholesale destruction of privacy and the construction of a new axis of inequality defined by the growing gap between 'what I can know and what can be known about me.' At this stage of development, surveillance capitalism governs the production of and access to knowledge about people and society for its own advantage, which establishes its dominance over and information society.

And there is no law to stop it.

Stage Three: Exploitation

Now, growing concentrations of knowledge are transformed into power. "Targeting" is the preferred euphemism as the scale and scope of data feed a range of digital cueing mechanisms engineered to tune, herd, constrain, direct, and condition individual and collective behavior to maximize engagement for maximum predictability and extraction. Operations engineered for profit maximization are systemically biased toward more corrupt and inflammatory content, which is proven to yield higher levels of "engagement."[24]

These economic operations cause social harm effects across multiple vectors as they produce epistemic chaos. Such chaos begins with the degradation of information integrity, as defactualized content is artificially driven to the center of social discourse by algorithmic targeting engineered for engagement. Such targeting aims to shape behavior through a variety of mechanisms including subliminal cues, engineered social comparisons, psychological microtargeting, rewards and punishments, and more. These mechanisms further intensify inequality as expressed in the growing gap between 'what I can do and what can be done to me,'

degrading the integrity of individual and collective behavior. And as targeting operations mediate information and communication, they erode common sense and produce a more splintered and polarized society.[25]

The governance functions associated with these harms are illustrated in the *Wall Street Journal's* "Facebook Files," which showed Mr. Zuckerberg's power to play his celestial keyboard, reinforcing or extinguishing the behavior of billions of people. Anger is rewarded or ignored. News stories become more trustworthy or unhinged. Publishers prosper or wither. Political discourse turns uglier or more moderate. People live or die.[26]

And there is no law to stop it.

Stage Four: Enforcement

At this stage firms begin to enforce governance prerogatives by leveraging their ownership and control of information and communication spaces, systems, and infrastructures. By now the institutional order is sufficiently entrenched to openly vie for governance of mission-critical spheres of democratic capabilities (such as healthcare), but also to openly contest democratic institutions and their elected and appointed officials. The aim now is to absorb political governance functions in an increasingly open showdown over governance.

There have been more frequent sightings of this stage four behavior – Facebook's current threats to withdraw from Europe, Facebook's Oversight Board, the Google-Facebook contest with the Australian parliament. April 2020 brought a showdown between the European Commission and its member governments on the one hand, and Apple and Google on the other. The companies had abruptly introduced a COVID-19 exposure notification protocol for Androids and iPhones that was incompatible with government-supported exposure notification and contract tracing applications already in development. Tense negotiations followed, as democratically elected leaders and government officials tried unsuccessfully to persuade Apple's CEO Tim Cook, Google's Sundar Pichai, and assorted corporate executives to adapt their operating system for the use of European public health authorities and urgent epidemiological research.

And there is no law to stop it.

Surveillance capitalism's whirlwind two-decade developmental journey now reveals itself as one vector of a larger contest between institutional orders. At each developmental stage we see a zero-sum dynamic in which the deepening institutional order of surveillance economics propagates democratic disorder.

This clash of institutional orders clarifies the reason for Congressional action. We have drifted into an accidental dystopia. The only countervailing institutional order capable of obstructing surveillance capitalism's path to dominance is the liberal democratic state. Surveillance capitalism is the younger challenger, but it embodies many unprecedented strengths. And while it is true that democracy is the old and slow incumbent, it brings powerful advantages that are difficult to rival. Chief among these is the legitimate authority and requisite power to make, impose, and enforce the rule of law. What laws must be devised if there is to be any hope of rescuing the digital century for democracy?

V. A Democratic Resurgence

A century ago, the corporate concentration of power was understood as economic power, and owners had all the authority on the strength of their property rights. The harms of concentration fell on people in their economic roles as workers, consumers, and competitors. Decades of contest and collective action eventually produced antitrust laws, but also new charters of rights for workers and consumers, the laws to protect them, and the public institutions charged with their enforcement and governance.

As important as those creations remain today, they do not protect us from the new harms we face. Ours is an accidental dystopia for the many reasons we have reviewed, including these: neither lawmakers nor citizens anticipated the harms that follow when the dominant economic institutional order is founded on the secret extraction of personal human experience once assumed to be private and now transformed into raw material for commercial operations. Nor did we grasp the harms that follow when revenues depend upon making all human behavior more predictable across all domains of everyday life. Nor did we imagine the social degradation unleashed when information and communication spaces are owned, operated, and mediated by an economic system in which information integrity is negatively correlated with revenues.

These conditions illuminate the changing nature of corporate concentration. In the age of surveillance capitalism, corporate power is not only economic but social. Its social harms are not confined to individuals in their roles as workers and consumers. They fall upon 'users': a new category of humanity that means all of us, all the time, everywhere. Ours is a young information civilization that has not yet found its footing in democracy because the social harms we face cannot be shoehorned into Cinderella's 20th century legal slipper. So, now it is **we** who march naked, without the rights, laws, and institutions purpose-built to govern our digital century in the name of democracy.

The tech giants and their fellow travelers have been willing to treat their destructive effects on people and society as collateral damage — the unfortunate but inevitable byproduct of digital technologies employed in perfectly legal economic operations. In April 2020 as the world tried to come to grips with Covid-19, former Google CEO Eric Schmidt, boasted that the pandemic would teach Americans to be "a little bit grateful" for powerful tech companies.[27] Other tech executives welcomed what they believed would be the inevitable end of 'techlash' thanks to widespread pandemic-induced dependency.

But as we enter the third decade of the digital century, something extraordinary is occurring: the aura of inevitability is giving way to the realization that the emperor is not only naked but dangerous. The data from prominent US attitude surveys suggests a public rupture of faith with surveillance capitalism and the power of its dominant corporations. Instead of a little gratitude there is a lot of anger and dismay.

I will tailor my remarks to just a few of the most recent surveys and the extraordinary majorities that voice dissent over surveillance capitalism's social harms. As evidenced in the following surveys, the American population is overwhelmingly calling for action to curb the unaccountable

power of surveillance capitalism and its giant protagonists. Americans want an end to the social harms that spin from these corporate orbits with increasing velocity and destructive force. There is a clear sense that human rights, the durability of society, and democracy itself are on the line.

A Knight Foundation/Gallup survey in July 2020 found that 77 percent of adult Americans believe Big Tech companies have too much power.[28] Ninety-four percent of respondents were concerned about privacy and 92 percent were concerned about the spread of disinformation and its effects on society. Only 30 percent were concerned about innovation. An Accountable Tech survey in January 2021 found 71 percent of respondents favoring regulatory intervention.[29] Eighty-one percent preferred privacy over the benefits of targeted advertising, and 73 percent were opposed to behavioral tracking and personal data collection for the sake of targeted ads. Finally, in significant majorities, respondents were in favor of banning social media companies from boosting extreme content (84 percent) as well as banning the collection of personal data for targeting (81 percent). Another 86 percent favored holding companies legally accountable for boosting violent content on their platforms.

Data published six months later in July 2021 further suggest that the American public no longer accepts the secret massive-scale extraction of human data as either inevitable or desirable. In an extensive US survey commissioned by the Future of Technology Commission, 93 percent of respondents agreed with the following statement: "It should be illegal for private companies to collect information about people without their permission."[30] It was the largest majority in agreement with any statement in this lengthy section of the study.

In 2022, the American public finally may be ready to shout that the emperor has no clothes, redefining illicit data extraction as theft and thus dismantling the keystone of surveillance capitalism's profits and power: the secret massive-scale extraction of human generated data.

An early vanguard of privacy-oriented scholars feared the internet companies' concentrated power and corrosive effect on democracy. [31] It is useful to note that these pioneers now have been joined by a new wave of scholarship mobilized by concerns over the startling concentrations of power in the giant tech firms and their implications for the democratic social order.[32]

Where does the widespread rupture of public faith leave us? Democracy is the only countervailing institutional order with the legitimate authority and power to change our course. If the ideal of human self-governance is to survive the digital century, then all solutions point to one solution: *a democratic resurgence*. But instead of the usual laundry lists of remedies, lawmakers need to proceed with a clear grasp of the adversary: a single hierarchy of economic causes and their social harm effects.

While liberal democracies have begun to engage with the challenges of regulating today's privately owned information spaces, the sober truth is that we need lawmakers ready to engage in a once-a-century exploration of far more basic questions. How should we structure and govern information, connection, and communication in a democratic digital century? What new charters of rights, legislative frameworks and institutions are required to ensure that data collection and use serve the genuine needs of individuals and society? What measures will protect citizens from

unaccountable power over information, whether it is wielded by private companies or governments?

Privacy law after privacy looks like this:

1) ***Interrupt supply by outlawing secret massive-scale extraction of human-generated data***. We can't rid ourselves of later-stage social harms unless we interrupt and outlaw their foundational economic causes. This means we move beyond the current focus on downstream issues where we argue about content moderation, illegal content, and 'filter bubbles,' as lawmakers and citizens stamp their feet at recalcitrant executives who have already claimed these unceasing data flows as their property. Downstream is where the companies want us to be, so consumed in the details of the property contract that we forget the real issue, which is that their property claim itself is illegitimate. The edifice of surveillance economics is built on this foundation of sand. Every argument that begins with 'data' is an argument that we have already lost. Like a magician's rabbit, the endless, and often pointless, downstream discussions direct our attention away from the mechanics of the trick. It's like arguing over the details of a seven-year old's factory contract instead of outlawing child labor. Similarly, structural solutions like "breaking up" the tech giants may be valuable in some cases, but they will not affect the underlying economic operations of surveillance capitalism.

Instead, we need to focus laser-like on the bedrock of surveillance economics, which is the secret extraction of human data from realms of life until recently assumed as "private." Remedies that focus on regulating and eliminating extraction are content neutral. They do not threaten freedom of expression. Instead, they liberate social discourse and information flows from the "artificial selection" of profit-maximizing commercial operations that allow for misinformation with no regard for integrity. They restore the sanctity of social communications and individual expression.

No secret extraction means no illegitimate concentrations of knowledge about people. No concentrations of knowledge mean no targeting algorithms. No targeting means that corporations can no longer control and curate information flows and social speech or shape human behavior to favor their interests. Regulating and outlawing extraction would eliminate the surveillance dividend and with it the financial incentives for surveillance, opening the competitive landscape to new forms of information capitalism that reunite the digital technologies with the real needs of people and society, as data collection is tied to fundamental rights and data use is tied to the public good.

2) ***New conditions summon new rights.*** A democratic information civilization cannot progress without new charters of *epistemic rights.* Citizens of democratic societies have regarded personal experience as inseparable from the individual: inalienable. It follows that the right to know about one's own personal experience has been considered elemental — bonded to each of us like a shadow. My epistemic rights are the cause of which my privacy is the effect. We each decide if and how our experience is shared, with whom, and for what purpose.

Justice Douglas's "freedom to select" is the elemental epistemic right to decide who knows us, how, when, and to what purpose. It is the right from which cause from which all privacy flows.

For example, as the natural bearer of such rights, I do not give Amazon's facial recognition system the right to know if I am afraid or happy. I do not give the corporation the right to exploit my fear for targeting and behavioral prediction that benefit others' commercial objectives. It's not simply that my feelings are not for sale, it's that my feelings are unsale-able because they are inalienable. Though I do not give Amazon my fear, they take it from me anyway, just another data point in the trillions gathered that day.

New legal rights are crystalized in response to the changing conditions of life. Justice Brandeis' commitment to privacy rights, for example, was stimulated by the spread of photography and its ability to invade and steal what was regarded as private. In 1890 he wrote, "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."

Our elemental epistemic rights are not codified in law because until now they have not come under systematic threat, any more than we have laws to protect our rights to stand up or sit down or yawn. But the surveillance capitalists have declared their "right to know" our lives, mobilizing pervasive surveillance at a scale and depth of intimacy that beggar imagination, while claiming the right to own and profit from that knowledge. Thus dawns a new age, founded on and shielded by the false inevitability of surveillance capitalism. Now the once taken-for-granted right to know and to decide who knows 'about me' must be codified in law and protected by democratic institutions, if it is to exist at all.

3) ***Unprecedented harms demand unprecedented solutions.*** Just as new conditions of life reveal the need for new rights, the unprecedented harms of the epistemic coup require purpose-built solutions. This is how law evolves, growing and adapting from one era to the next — Brandeis's "eternal youth."

A mature democratic information society will require independent trustworthy public oversight institutions that hold the market and the state to account in the knowledge that the solution to surveillance capitalism is not a Big Brother state. These institutions are dedicated to a democratic digital future: transparent, governed by the rule of law, immune to political interference, and empowered with the budgetary, technological, and human resources necessary to oversee and enforce the availability and integrity of information for people and democracy.

4) ***Interrupt and outlaw demand for illicit data collection.*** Solutions that interrupt illicit data supply are complimented by solutions that interrupt demand by disrupting the financial incentives that reward surveillance economics. We can outlaw markets that trade in human futures because we have seen their antihuman, antisocial, and antidemocratic harms. This is not a radical prospect. Democratic societies have outlawed other markets that produce reliably dangerous consequences: Markets that trade in human beings were outlawed, even when they supported whole economies. We outlaw markets that trade in human organs and babies because they inflict damage on people and society.

****

When it comes to privacy law after privacy, the digital century forces us to choose: *We may be a surveillance society, or we may be a democracy, but we cannot be both.* The liberal democracies must take the lead because they have the power and legitimacy to do so. But they should know that their allies and collaborators include the people of every society struggling against the double insult of an accidental dystopian future. We have a democratic digital century to build, and there is no time to waste.

Notes

[1] Shoshana Zuboff, "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization," *Journal of Information Technology* 30, no. 1 (March 1, 2015): 75–89, https://doi.org/10.1057/jit.2015.5; Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: PublicAffairs, 2019).
[2] Pascale Davies, "Meta Warns It May Shut down Facebook and Instagram in Europe," *Euronews*, February 7, 2022, https://www.euronews.com/next/2022/02/07/meta-threatens-to-shut-down-facebook-and-instagram-in-europe-over-data-transfer-issues.
[3] Sam Biddle, "Facebook Uses Artificial Intelligence to Predict Your Future Actions for Advertisers, Says Confidential Document," *The Intercept*, April 13, 2018, https://theintercept.com/2018/04/13/facebook-advertising-data-artificial-intelligence-ai/.
[4] Sergey Brin and Lawrence Page, "The Anatomy of a Large-Scale Hypertextual Web Search Engine," *Computer Networks and ISDN Systems*, Proceedings of the Seventh International World Wide Web Conference, 30, no. 1 (April 1, 1998): 107–17, https://doi.org/10.1016/S0169-7552(98)00110-X.
[5] Andrew Zipern, "Technology Briefing | Internet: Google Enters Corporate World," *The New York Times*, February 12, 2002, sec. Business, https://www.nytimes.com/2002/02/12/business/technology-briefing-internet-google-enters-corporate-world.html.
[6] Douglas Edwards, *I'm Feeling Lucky: The Confessions of Google Employee Number 59* (New York: Houghton Mifflin Harcourt, 2011), 291.
[7] Edwards, 340–45.
[8] Jessi Hempel, "Sheryl Sandberg: Facebook's New Number Two," *CNN Money*, April 11, 2008, https://money.cnn.com/2008/04/11/technology/facebook_sandberg.fortune/.
[9] "Google: Ad Revenue 2001-2020," Statista, n.d., https://www.statista.com/statistics/266249/advertising-revenue-of-google/; "Facebook: Annual Segment Revenue 2020," Statista, n.d., https://www.statista.com/statistics/267031/facebooks-annual-revenue-by-segment/.
[10] Jenna Ross, "The Biggest Companies in the World in 2021," Visual Capitalist, June 10, 2021, https://www.visualcapitalist.com/the-biggest-companies-in-the-world-in-2021/.
[11] Zuboff, *The Age of Surveillance Capitalism*.
[12] Milton Friedman, "A Friedman Doctrine-- The Social Responsibility Of Business Is to Increase Its Profits," *The New York Times*, September 13, 1970, sec. Archives, https://www.nytimes.com/1970/09/13/archives/a-friedman-doctrine-the-social-responsibility-of-business-is-to.html.
[13] Angus Burgin, *The Great Persuasion: Reinventing Free Markets since the Depression* (Cambridge, MA: Harvard University Press, 2012), chap. 5.
[14] President William J. Clinton and Vice President Albert Gore, Jr., "A Framework For Global Electronic Commerce" (The White House, n.d.), https://clintonwhitehouse4.archives.gov/WH/New/Commerce/read.html.
[15] Robert Pitofsky et al., "Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress," *Federal Trade Commission*, May 1, 2000, 35.
[16] Pitofsky et al. The report's legislative proposals set forth a basic level of privacy protection for all visits to consumer-oriented commercial websites to the extent not already provided by the

Children's Online Privacy Protection Act (COPPA). Such legislation would set out the basic standards of practice governing the collection of information online and provide an implementing agency with the authority to promulgate more-detailed standards pursuant to the Administrative Procedure Act, including authority to enforce those standards. All consumer-oriented commercial websites that collect personal identifying information from or about consumers online, to the extent not covered by the COPPA, would be required to comply with the four widely accepted fair information practices: (1) Notice. Websites would be required to provide consumers clear and conspicuous notice of their information practices, including what information they collect, how they collect it (e.g., directly or through nonobvious means such as cookies), how they use it, how they provide Choice, Access, and Security to consumers, whether they disclose the information collected to other entities, and whether other entities are collecting information through the site. (2) Choice. Websites would be required to offer consumers choices as to how their personal identifying information is used beyond the use for which the information was provided (e.g., to consummate a transaction). Such choice would encompass both internal secondary uses (such as marketing back to consumers) and external secondary uses (such as disclosing data to other entities). (3) Access. Websites would be required to offer consumers reasonable access to the information a website has collected about them, including a reasonable opportunity to review the information and to correct inaccuracies or delete information. (4) Security. Websites would be required to take reasonable steps to protect the security of the information they collect from consumers.

[17] Peter Swire, "The Second Wave of Global Privacy Protection: Symposium Introduction," *Ohio State Law Journal* 74, no. 6 (2013): 845, https://kb.osu.edu/handle/1811/71601.

[18] Swire, 846.

[19] Paul M. Schwartz, "Systematic Government Access to Private-Sector Data in Germany," *International Data Privacy Law* 2, no. 4 (November 1, 2012): 230, 235, https://doi.org/10.1093/idpl/ips026; W. Gregory Voss, "After Google Spain and Charlie Hebdo: The Continuing Evolution of European Union Data Privacy Law in a Time of Change," *Business Lawyer* 71, no. 1 (January 6, 2016), https://papers.ssrn.com/abstract=2711996; Mark Scott, "Europe, Shaken by Paris Attacks, Weighs Security With Privacy Rights - The New York Times," *New York Times - Bits Blog*, November 18, 2015, https://web.archive.org/web/20151119015821/https://bits.blogs.nytimes.com/2015/11/18/europe-shaken-by-paris-attacks-weighs-security-with-privacy-rights/; Frank A. Pasquale, "Privacy, Antitrust, and Power," *George Mason Law Review* 20, no. 4 (2013): 1009–24; Pasquale, 1009–24; Alissa J. Rubin, "Lawmakers in France Move to Vastly Expand Surveillance," *The New York Times*, May 5, 2015, sec. World, https://www.nytimes.com/2015/05/06/world/europe/french-legislators-approve-sweeping-intelligence-bill.html; Georgina Prodhan and Michael Nienaber, "Merkel Urges Germans to Put aside Fear of Big Data," *Reuters*, June 9, 2015, sec. Technology News, https://www.reuters.com/article/us-germany-technology-merkel-idUSKBN0OP2EM20150609.

[20] Jack Balkin, "The Constitution in the National Surveillance State," *Minnesota Law Review* 93, no. 1 (2008), https://openyls.law.yale.edu/handle/20.500.13051/1545.

[21] Mike McConnell, "Mike McConnell on How to Win the Cyber-War We're Losing," *The Washington Post*, February 28, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html.

[22] "WARDEN, MARYLAND PENITENTIARY, Petitioner, v. Bennie Joe HAYDEN.," Cornell Law School - Legal Information Institute, n.d.,

https://www.law.cornell.edu/supremecourt/text/387/294.
[23] Michael G. Jacobides, Stefano Brusoni, and Francois Candelon, "The Evolutionary Dynamics of the Artificial Intelligence Ecosystem," *Strategy Science* 6, no. 4 (December 2021): 412–35, https://doi.org/10.1287/stsc.2021.0148.
[24] For example, Soroush Vosoughi, Deb Roy, and Sinan Aral, "The Spread of True and False News Online," *Science* 359, no. 6380 (March 9, 2018): 1146–51, https://doi.org/10.1126/science.aap9559; Laura Edelson et al., "Understanding Engagement with U.S. (Mis)Information News Sources on Facebook," in *Proceedings of the 21st ACM Internet Measurement Conference* (New York, NY, USA: Association for Computing Machinery, 2021), 444–63, https://doi.org/10.1145/3487552.3487859.
[25] For example, Fernando P. Santos, Yphtach Lelkes, and Simon A. Levin, "Link Recommendation Algorithms and Dynamics of Polarization in Online Social Networks," *Proceedings of the National Academy of Sciences* 118, no. 50 (December 14, 2021), https://doi.org/10.1073/pnas.2102141118; Ro'ee Levy, "Social Media, News Consumption, and Polarization: Evidence from a Field Experiment," *American Economic Review* 111, no. 3 (March 2021): 831–70, https://doi.org/10.1257/aer.20191777.
[26] "The Facebook Files," *Wall Street Journal*, October 1, 2021, sec. Tech, https://www.wsj.com/articles/the-facebook-files-11631713039.
[27] Theodore Schleifer, "Google's Former CEO Hopes the Coronavirus Makes People More 'Grateful' for Big Tech," *Vox*, April 14, 2020, https://www.vox.com/recode/2020/4/14/21221141/coronavirus-eric-schmidt-google-big-tech-grateful.
[28] "American Views 2020: Trust, Media and Democracy" (Gallup and Knight Foundation, August 4, 2020), https://knightfoundation.org/reports/american-views-2020-trust-media-and-democracy/.
[29] "America's Views on Surveillance Advertising" (Accountable Tech, n.d.), https://accountabletech.org/research/surveillance-advertising/.
[30] "Poll: Nine out of Ten Voters Support Strong Online Privacy Protections While Eight Out of Ten Strongly Support Holding Social Media Companies More Accountable for 'Illegal and Harmful Content' Posted on Their Sites," *Future of Tech Commission*, September 23, 2021, https://www.futureoftechcommission.org/press-release-launch-poll.
[31] Paul M. Schwartz, "Privacy and Democracy in Cyberspace," *Vanderbilt Law Review* 52, no. 6 (1999): 1607, https://doi.org/10.2139/ssrn.205449; Peter Swire, "Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information, in Privacy and Self-Regulation in the Information Age by the U.S. Department of Commerce.," *Department of Commerce*, 1997, https://doi.org/10.2139/ssrn.11472; Dennis D. Hirsch, "The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?," *Seattle University Law Review* 34, no. 2 (February 8, 2011): 439, https://papers.ssrn.com/abstract=1758078.
[32] See for example Dina Srinivasan, ed., "The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy," *Berkeley Business Law Journal* 16, no. 1 (2019): 39–101.