Written Testimony
Submitted to
The International Grand Committee on
Big Data, Privacy, and Democracy

by

Shoshana Zuboff

Ottawa, May 28, 2019

Shoshana Zuboff
Written Testimony Submitted to the International Grand Committee on
Big Data, Privacy, and Democracy
Ottawa, May 28, 2019

Co-Chairman Zimmer, Co-Chairman Collins, honorable members of the International Grand Committee, my name is Shoshana Zuboff. I am the Charles Edward Wilson Professor Emerita, Harvard Business School, and the author of the recent book *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. In advance of my testimony I note that my statements and conclusions are amply supported by the information and analysis available in my book. I might add that my scholarly work on the digital future began in 1978 – a long journey. I also want to note for the record that I am committed to the work of this group, including continuing to support the Committee offline and in future meetings.

It is a privilege to come before you today to share testimony on the themes that you have identified for consideration:

1. Holding Digital Platforms to Account;
2. Foreign Influence in Our Democracies; and
3. Data as a Human Right: Protecting Our Citizens – Data Security and Privacy.

SURVEILLANCE CAPITALISM IS A NOVEL ECONOMIC LOGIC

My contribution to these proceedings is to argue that the lack of platform accountability, the weaponization of digital connection, and the destruction of data privacy and security are not distinct problems to be addressed with distinct regulatory and legislative actions. Rather, they are each effects of the same cause. What is that cause? It is the comprehensive, internally consistent, and unprecedented economic logic that I have called *surveillance capitalism*. These effects identified by the Committee are fragments of a new social order: the world according to surveillance capitalism.

The internet is now owned and operated by private surveillance capital. The medium that once promised to amplify voice, connection, empowerment, and the democratization of information has taken a dark turn as surveillance capitalism hijacks the digital future setting it on a collision course with individual autonomy, equality, and

the very possibility of a democratic society. It is important to note that surveillance capitalism has rooted and flourished during the last two decades by aggressively moving into blank spaces where it could spread unimpeded by law, regulation, or any form of democratic oversight and constraint. Its rapid growth was enabled by the unprecedented character of its practices, their inherent indecipherability, and both technical systems and public rhetoric intentionally designed to camouflage, misdirect, confuse, bamboozle, and in general produce ignorance among populations and their lawmakers. Enough is enough. It is time for the sleeping giant of democracy to stir and mobilize against surveillance capitalism's vision for people, for society, for democracy, and for capitalism itself.

The questions of law and regulation that this Committee seeks to explore cannot be answered without a clear grasp of surveillance capitalism as a novel economic logic defined by distinct economic imperatives that compel specific practices. From the viewpoint of this logic, each headline revealing fresh atrocities committed by surveillance capitalists can be understood as a predictable consequence of its unique iron laws. The 21st century solutions to this 21st century problem may include but must also move beyond existing paradigms of privacy and antitrust. Our novel circumstances require novel legislative and regulatory regimes that target, interrupt, and outlaw surveillance capitalism's key markets and mechanisms.

WHAT SURVEILLANCE CAPITALISM IS NOT

Before defining surveillance capitalism, let me first say what it is not:

First, leading surveillance capitalists have sought to persuade us that its practices are an inevitable consequence of digital technologies. This is false. 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 upon the social and economic logics that bring them to life. Surveillance capitalism relies on a ubiquitous internet-enabled networked digital architecture, machine intelligence, and platforms, but it is not the same as any of those.

Second, surveillance capitalism is not a single corporation or even a group of corporations. It was invented at Google in 2000-2001 as a solution to financial emergency during the dot-com bust and first elaborated there. It was later ported to Facebook with Google executive Sheryl Sandberg. These surveillance capitalist operations were honed in the context of online-targeted ads and rationalized as a quid pro quo for free services, but surveillance capitalism is no more limited to that context than mass production was limited to the fabrication of the Model T, where it was first comprehensively established. Surveillance capitalism quickly became the default model for Silicon Valley and most of the tech sector. By now it has spread across a wide range of products, services, and economic sectors, including insurance, retail, health care, finance, entertainment, education, transportation, and more, birthing whole new ecosystems of suppliers, producers, customers, market-makers, and market players.

Third, surveillance capitalism is not a person or a group of people. The founders of the pioneer surveillance capitalist corporations — Mark Zuckerberg at Facebook, Larry Page and Sergey Brin at Google — exploited specific historical circumstances in combination with a range of offensive strategies and tactics in order to protect themselves from external constraint either in the form of law and regulation or sound corporate governance. These circumstances produced some stark facts, as I write in my book: "Two men at Google who enjoy neither the legitimacy of the vote, democratic oversight, nor the demands of shareholder governance exercise control over the organization and presentation of the world's information. One man at Facebook who enjoys neither the legitimacy of the vote, democratic oversight, nor the demands of shareholder governance exercises control over an increasingly universal means of social connection along with the information concealed in its networks." The unimpeded freedom of these individuals has been bad for people and for democracy. There are good reasons to curb their power. As important as this may be, however, it will not alter the fundamental issues that this committee seeks to address. The entrenched economic logic of surveillance capitalism will not vanish, even with a new cast of characters.

WHAT IS SURVEILLANCE CAPITALISM?

Now that we know what it is not, we may ask, *what is surveillance capitalism?* In 2001, as Google's leaders began to understand the economic power of their new invention, Larry Page ruminated, "If we did have a category, it would be personal information." He noted that as a result of cheap cameras, sensors, and storage, "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."

Page's vision perfectly reflects the history of 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. Industrial capitalism famously claimed nature for the market, to be reborn as "land" or "real estate" for sale and purchase.

Surveillance capitalism repeats this process but with a dark and startling twist: it declares *private human experience* as free raw material for translation into production and sales. Once private human experience is claimed for the market, it is rendered as behavioral data for computation and analysis. While some of these data may be applied to product or service improvements, the rest are declared as a proprietary *behavioral surplus.* This surplus is defined by its rich predictive value.

Behavioral surplus extraction began with online browsing, search, and social media behavior but now encompasses every movement, conversation, facial expression, sound, text, and image that is, or can be, or will be, accessible to the always-on ubiquitous internet-enabled digital extraction architecture that I call *Big Other*. In this digital surround, every device, interface, and touch point is redefined as a node in a vast supply network dedicated to relentlessly tracking, hunting, inducing, and taking more behavioral surplus. From the beginning these operations were intentionally designed to bypass "user" awareness. Google's data scientists celebrated their ability to take without users' knowledge, and to learn more about people than they intended to disclose. This relationship of surveillance was baked into the cake from the start and is essential to its strange form of value creation.

These new supply chains ultimately feed a new "means of production" known as "machine intelligence." These are the new age factories where behavioral surplus is fabricated into *prediction products:* calculations that anticipate what we will do now, soon, and later. The first prediction products were clickthrough rates – predictions of how users would react to specific ads.

Recently the world caught a rare glimpse of these mechanisms. A leaked Facebook document in 2018 cites Facebook's unparalleled "machine learning expertise" aimed at meeting its customers' "core business challenges." It describes Facebook's ability to use its unrivaled data stores "to predict future behavior," targeting individuals on the basis of how they will behave, purchase, and think: now, soon, and later. The document links prediction, intervention, and modification. For example, a Facebook service called "loyalty prediction" is touted for its ability to analyze behavioral surplus in order to predict individuals who are "at risk" of shifting their brand allegiance. The idea is that these predictions can trigger advertisers to intervene promptly, targeting aggressive messages to stabilize loyalty and thus achieve guaranteed outcomes by altering the course of the future.

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."[1]

This illustration clarifies a critical point, one that confuses both the public and its lawmakers. Surveillance capitalists harbor two distinct data sets that I call "the two texts." The first is the public-facing text that contains information that users provide. The second is what I call "the shadow text." These data are the result of their proprietary analyses of the first text. This is the heart and soul of surveillance capitalists' economic and social power, based on exclusive access to computational equipment and skills, including most of

the approximately 10,000 data scientists on earth. Discussions of data transparency, ownership, access, and portability will always fall short, because they refer only to the first text, not the crucial proprietary shadow text.

In a final stage of the new economic logic, prediction products are rapidly swept up into the life of the market, traded in newly constituted marketplaces for behavioral predictions that I call *behavioral futures markets*. Surveillance capitalists have grown immensely wealthy from these trading operations based on the promise of certainty in the form of guaranteed outcomes. Many companies are eager to lay bets on such guarantees of our future behavior. Online-targeted advertising was simply the first of these markets in human futures, where "clickthrough rates" were sold as predictions of human behavior.

Today, every product or service that begins with the word "smart" or "personalized," every internet-enabled device, every "digital assistant," is simply a supply-chain interface for the unobstructed flow of behavioral data on its way to predicting our futures for others' financial gain. Between 2000 when surveillance capitalism was invented and 2004 when Google went public, its revenues increased by 3,590%. These results redefined the financial bar for companies and their investors, driving the new economics across the tech sector and eventually the rest of the economy. Surveillance capitalism's mechanisms and methods now infect nearly every economic sector. What began as a solution to financial emergency in 2001 is now a burgeoning surveillance-based economic order: *a surveillance economy.*

THE ECONOMIC IMPERATIVES PHASES I & II: EXTRACTION AT SCALE AND SCOPE

Markets that trade in human futures produce specific competitive dynamics. The core economic imperatives of surveillance capitalism are clarified by reverse engineering these competitive dynamics. Trade in predictions of human futures compels the extraction of ever more predictive sources of behavioral surplus entailing specific consequences that produce both economic and non-economic harms.

The first competitive phase emphasized the need for a critical volume of data and

thus economies of scale. This turned the online medium into a ruthless hunting ground for behavioral surplus. The second emphasized varieties of data — economies of scope. In this phase users were sent from their desktops to their mobile phones, out into the world where real behavior could be captured and rendered as data: your drive, run, shopping excursion, search for a parking space, voice, face, posture, gait, and always... location, location, location.

The imperatives of extraction at scale and scope produce an unusual perspective on data that I call *radical indifference*. It requires that content is judged by its volume, range, and depth of surplus. These metrics treat all data as equivalently valuable, despite the obvious fact that data originate in distinct human situations, convey profoundly dissimilar human meanings, and therefore are fundamentally unequal. Radical indifference is an asocial framework for evaluating data. As such, it is the source of all the troubles associated with what has come to be called "fake news." Just as early-twentieth-century managers were once taught the "administrative point of view" as the mode of knowledge required for the hierarchical complexities of the new large-scale corporation, today's high priests practice the applied arts of radical indifference.

Radical indifference is a response to economic imperatives, and only occasionally do we catch an unobstructed view of its strict application as a managerial discipline. One such occasion was a 2016 internal Facebook memo acquired by BuzzFeed in 2018. Written by one of the company's long-standing and most influential executives, Andrew Bosworth, it provided a window into radical indifference as an applied discipline. "We talk about the good and the bad of our work often. I want to talk about the ugly," Bosworth began. He went on to explain how equivalence wins out over equality in the march toward totality, certainty, and thus the growth of surveillance revenues:

We connect people. That can be good if they make it positive. Maybe someone finds love. Maybe it even saves the life of someone on the brink of suicide. So we connect more people. That can be bad if they make it negative. Maybe it costs a life by exposing someone to bullies. Maybe someone dies in a terrorist attack coordinated on our tools.

And still we connect people. The ugly truth is that… anything that allows us to connect more people more often is de facto good. It is perhaps the only area where the metrics do tell the true story as far as we are concerned... That's why all the work we do in growth is justified. All the questionable contact importing practices. All the subtle language that helps people stay searchable by friends. All of the work we do to bring more communication in.… The best products don't win. The ones everyone uses win… make no mistake, growth tactics are how we got here."

As Bosworth makes clear, from the viewpoint of radical indifference the positives and negatives must be viewed as equivalent, despite their unequal moral meanings and human consequences. From this perspective the only rational objective is the pursuit of products that snare "everyone," not "the best products."

A significant result of the systematic application of radical indifference is that the public-facing "first text" is vulnerable to corruption with content that would normally be perceived as repugnant: lies, systematic disinformation, fraud, violence, hate speech, and so on. As long as content contributes to "growth tactics," Facebook "wins." This vulnerability can be an explosive problem on the demand side, the user side, but it breaks through the fortifications of radical indifference only when it threatens to interrupt the flow of surplus into the second "shadow" text: the one that is for them but not for us.

The norm is that information corruption is not catalogued as problematic unless it poses an existential threat to supply operations—Bosworth's imperative of connection—either because it might trigger user disengagement or because it might attract regulatory scrutiny. This means that any efforts toward "content moderation" are best understood as defensive measures, not as acts of public responsibility. In other words, and this is key, surveillance capitalism's networks are intentionally constructed to launch viruses in full knowledge that there are no vaccines, no fail safe systems, no breaks that can be applied to global infection. Vaccines put supply chains of behavioral surplus at risk. This constitutes an existential threat as a primary violation of economic imperatives.

The greatest challenge to radical indifference has come from Facebook and Google's overreaching ambitions to supplant professional journalism on the internet. Both corporations inserted themselves between publishers and their populations, subjecting journalistic "content" to the same categories of equivalence that dominate surveillance capitalism's other landscapes. In a formal sense, professional journalism is the precise opposite of radical indifference. The journalist's job is to produce news and analysis that separate truth from falsehood. This rejection of equivalence defines journalism's raison d'être as well as its organic reciprocities with its readers. Under surveillance capitalism, though, these reciprocities are erased.

A consequential example was Facebook's decision to standardize the presentation of its News Feed content so that "all news stories looked roughly the same as each other… whether they were investigations in The Washington Post, gossip in the New York Post, or flat-out lies in the Denver Guardian, an entirely bogus newspaper." This expression of equivalence without equality made Facebook's first text exceptionally vulnerable to corruption from what would come to be called "fake news."

This is the context in which Facebook and Google became the focus of international attention following the discovery of organized political disinformation campaigns and profit-driven "fake news" stories during the 2016 US presidential election and the UK Brexit vote earlier that year. Economists Hunt Allcott and Matthew Gentzkow, who have studied these phenomena in detail, define "fake news" as "distorted signals uncorrelated with the truth" that impose "private and social costs by making it more difficult… to infer the true state of the world... " They found that in the lead-up to the 2016 US election there were 760 million instances of a user reading these intentionally orchestrated lies online, or about three such stories for each adult American.

As radical indifference would predict, however, "fake news" and other forms of information corruption have been perennial features of Google and Facebook's online environments. There are countless examples of disinformation that survived and even thrived because it fulfilled economic imperatives, and I point out just a few. In 2007 a prominent financial analyst worried that the subprime mortgage bust would harm

Google's lucrative ad business. It seems a strange observation until you learn that in the years prior to the Great Recession, Google eagerly welcomed shady subprime lenders into its behavioral futures markets, anxious to net the lion's share of the $200 million in monthly revenue that mortgage lenders were spending on online advertising. A 2011 Consumer Watchdog report on Google's advertising practices leading up to and during the Great Recession concluded that "Google has been a prominent beneficiary of the national home loan and foreclosure crisis… by accepting deceptive advertising from fraudulent operators who falsely promise unwary consumers that they can solve their mortgage and credit problems." Despite these increasingly public facts, Google continued to serve its fraudulent business customers until 2011, when the US Treasury Department finally required the company to suspend advertising relationships with "more than 500 internet advertisers associated with the 85 alleged online mortgage fraud schemes and related deceptive advertising."

Only a few months earlier, the Department of Justice had fined Google $500 million, "one of the largest financial forfeiture penalties in history," for accepting ads from online Canadian pharmacies that encouraged Google's US users to illegally import controlled drugs, despite repeated warnings. As the US Deputy Attorney General told the press, "The Department of Justice will continue to hold accountable companies who in their bid for profits violate federal law and put at risk the health and safety of American consumers."

It is by now obvious that the rogue forces of disinformation grasp the facts of radical indifference more crisply than do lawmakers or surveillance capitalism's genuine users and customers. These rogue forces learned to exploit the blind eye of radical indifference in an open society in order to escalate the perversion of the public text, for the purpose of political manipulation. This kind of information corruption has also been a continuous feature of the Facebook environment. The turmoil associated with the 2016 US and UK political disinformation campaigns on Facebook was a well-known problem that had disfigured elections and social discourse in Indonesia, the Philippines, Columbia, Germany, Spain, Italy, Chad, Uganda, Finland, Sweden, Holland, Estonia, and the

Ukraine. Scholars and political analysts had called attention to the harmful consequences of this online disinformation for years. One political analyst in the Philippines worried in 2017 that it might be too late to fix the problem: "We already saw the warning signs of this years ago... Voices that were lurking in the shadows are now at the center of the public discourse."

THE ECONOMIC IMPERATIVES PHASE III:
PREDICTION REQUIRES ECONOMIES OF ACTION

Eventually, surveillance capitalists discovered that the most-predictive behavioral data come from intervening in real life behavior in order to nudge, coax, tune, and herd human activity at scale, always pushing behavior toward profitable outcomes, or what I call *economies of action*. Data scientists refer to this as a shift from "monitoring" to "actuation." As one data scientist explained to me, "We can engineer the context around a particular behavior and force change that way...*We are learning how to write the music, and then we let the music make them dance.*

At this new level of competitive intensity, it is no longer enough to automate information flow*s about us;* the goal now is to *automate us.* In this phase, the 'means of production' are subordinated to an increasingly complex "means of behavioral modification" in which the digital medium is called into action as a seamless environment of reinforcement to shape the behaviors of individuals, groups, and populations. These processes continue to be meticulously designed to produce ignorance by circumventing individual awareness and thus eliminate any possibility of self-determination. As long as surveillance capitalism and its behavioral futures markets are allowed to thrive, ownership of the new means of behavioral modification eclipses ownership of the means of production as the fountainhead of capitalist wealth and power in the twenty-first

In this way, surveillance capitalism produces a new kind of power – I call it *instrumentarian power* — which aims to shape human behavior toward others' ends. Instead of armaments and armies, murder and terror, it works its will through the

automated medium of the increasingly ubiquitous, internet-enabled, computational architecture of "smart" networked devices, things, and spaces of *Big Other*.

These new capabilities were honed in an experimental mode, especially at Facebook and Google. Facebook's 2012 and 2013 "massive-scale contagion experiments" confirmed that the corporation could manipulate subliminal cues on its pages to successfully change real-world behavior and feelings. It further demonstrated that it could do this while bypassing its users' awareness. Thanks to another leaked document in 2017 we learned that the same methods were touted to business customers in Australia and New Zealand, aimed at effecting the behavior of six million teenagers and young adults in those countries based on detailed knowledge of when young people feel 'stressed,' 'defeated,' 'overwhelmed,' 'anxious,' 'nervous,' 'stupid,' 'silly,' 'useless,' and a 'failure.'"[2] The report reveals Facebook's interest in leveraging this surplus for economies of action.

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 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. It boasts information on "mood shifts" among young people based on "internal Facebook data," and it claims that Facebook's prediction products can not only "detect sentiment" but also predict how emotions are communicated at different points during the week, matching each emotional phase with appropriate ad messaging for the maximum probability of guaranteed outcomes. "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." [3]

These are the very same practices adopted by Cambridge Analytica, as described by whistleblower Chris Wylie, whom I regard as information civilization's prodigal son. CA used behavioral surplus to exploit and trigger users' "inner demons," as Wylie put it, orchestrating subliminal cues online in order to effect real world behavior and emotions.

In other words surveillance capitalism's routine methods were simply pivoted a few degrees to aim at political rather than commercial outcomes. Indeed, that firm's chief revenue officer quietly announced his less glamorous but more lucrative postelection strategy: "After this election, it'll be full-tilt into the commercial business." Writing in a magazine for car dealers just after the US election, he notes that CA's new analytic methods reveal "how a customer wants to be sold to, what their personality type is, and which methods of persuasion are most effective... What it does is change people's behavior through carefully crafted messaging that resonates with them.… It only takes small improvements in conversion rates for a dealership to see a dramatic shift in revenue."

Economies of action were further developed at Google, where Street View chief John Hanke's internal skunk works, Niantic Labs, developed the augmented reality game Pokémon Go. The real game, it turns out, was learning how to herd innocent players to eat, drink, and purchase in the restaurants, bars, fast food joints, and shops that paid to play in the game's behavioral futures markets. Niantic Labs sold guarantees of footfall rates, the precise real-world analogy to clickthrough rates in the online milieu. These same herding capabilities are now integrated into WAZE, a real-life Google application intended to help users navigate traffic that now offers its businesses customers opportunities to leverage the shadow text in order to herd drivers to their service establishments.

These population-level capabilities of behavior modification and control ultimately aim for bigger game. The target now is the "smart city," or what Google once preferred to call the "Google city." The idea is to replace democratic governance with computation aimed at fulfilling guaranteed outcomes for business customers. The city is now the terrain upon which surveillance capitalists intend to remake society in their image and according to their interests. As we convene in Ottawa, it is vital for you to know that the fair city of Toronto is now the frontier of this most critical contest. Alphabet-owned Sidewalk Labs is spinning its euphemisms of "governance innovation," Orwellian code for the deconstruction of local democracy in favor of Sidewalk's computational rule, which is in the final analysis a reincarnation of absolutist tyranny, served with cappuccino and draped in 21st century ones and zeros. If Sidewalk can take Toronto, Canadians will have

gifted surveillance capitalism a platform for a wider assault on the rule of law and the democratic social order, all of it to advance surveillance capitalism's long range plans, profits, and vision of society as a collective to be ordered and tuned by computation in the service of others' commercial outcomes.

HOW DID THEY GET AWAY WITH IT?

In my book I explore sixteen reasons that explain how surveillance capitalists "got away with it." These include the clever exploitation of historical, political, and economic conditions that allowed them to succeed. Two deserve mention here. First, surveillance capitalism came of age at a time when government regulation was despised as an encroachment on freedom. Second, surveillance capitalism was invented in 2001, the same year that the West became engulfed in a "war on terror." In the US, and to a certain extent other nations too, the fledgling capabilities of the new tech companies were protected and nurtured in the hopes that they would contribute to the larger cause of "total information awareness" and do so outside the scope of Constitutional constraints.

There were other reasons on the demand side. Chief among these was the *unprecedented* nature of the new practices, which made them difficult to perceive and understand. Another is the historic concentration of technology and specialist expertise aimed at engineering user *ignorance* of surveillance capitalist operations.

Finally as alternatives to surveillance capitalism are foreclosed, we are left in a state of "no exit," trapped in an involuntary merger of personal necessity and economic extraction. The same channels that we rely upon for daily logistics, social interaction, work, education, healthcare, access to products and services, and much more, now double as supply chain operations for surveillance capitalism's surplus flows. The result is that effective social participation leads through "the means of behavioral modification," eroding the choice mechanisms that we have traditionally associated with the private realm — exit, voice, and loyalty. There can be no exit from processes that are intentionally designed to bypass individual awareness and produce ignorance, especially

when these are the very same processes upon which we must depend for effective daily life.

"User" dependency is thus a classic Faustian pact in which our felt needs for effective life vie against the inclination to resist surveillance capitalism's bold incursions. This conflict produces a psychic numbing that inures us to the realities of being tracked, parsed, mined, and modified. It disposes us to rationalize the situation in resigned cynicism, to shelter behind defense mechanisms like the infamous formulation, "I have nothing to hide", or to find other ways to stick our heads in the sand out of frustration and helplessness. In this way, surveillance capitalism imposes a fundamentally illegitimate choice that twenty-first century individuals should not have to make, and its normalization leaves us dancing in our chains—where it is all to easy to forget that *anyone who has nothing to hide is nothing.*

DEMOCRACY AT RISK

Humanity has survived the millennia by passing stories from one generation to the next that teach us how to live. These stories have been the North Star to our collective moral compass. They protect us from a future of forgetting. It is in this spirit that I want to recount a twentieth-century story with urgent implications for our twenty-first century future.

In 1971 the United States Senate Subcommittee on Constitutional Rights, led by North Carolina Senator Sam Ervin and including luminaries from across the political spectrum such as Edward Kennedy, Birch Bayh, Robert Byrd, and Strom Thurmond, undertook what would become a multiyear investigation into "a variety of programs designed to predict, control, and modify human behavior," triggered by a growing sense of public alarm at the spread of psychological techniques for behavior control. A migration of behavior-modification practices from military to civilian applications targeted captive populations in prisons, psychiatric wards, classrooms, institutions for the mentally challenged, schools for the autistic, and factories.

The Subcommittee subjected the principles and applications of behavior modification to intense constitutional scrutiny, questioning and ultimately rejecting the use of behavioral modification as an extension of state power. One outcome was the denial of federal funding to any program or institution that used such techniques.

From the first lines of the preface of the subcommittee's 1974 report, authored by Senator Ervin, it should be evident to any twenty-first-century captive of surveillance capitalism that US society has undergone a social discontinuity more profound than the mere passage of decades suggests. Ervin located the subcommittee's work at the heart of the Enlightenment project, pledging to defend the liberal ideals of freedom and dignity:

When the founding fathers established our constitutional system of government, they based it on their fundamental belief in the sanctity of the individual... They understood that self-determination is the source of individuality, and individuality is the mainstay of freedom... Recently, however, technology has begun to develop new methods of behavior control capable of altering not just an individual's actions but his very personality and manner of thinking… the behavioral technology being developed in the United States today touches upon the most basic sources of individuality and the very core of personal freedom… the most serious threat… is the power this technology gives one man to impose his views and values on another...

Concepts of freedom, privacy and self-determination inherently conflict with programs designed to control not just physical freedom, but the source of free thought as well... The question becomes even more acute when these programs are conducted, as they are today, in the absence of strict controls. As disturbing as behavior modification may be on a theoretical level, the unchecked growth of the practical technology of behavior control is cause for even greater concern."

In contrast to the 1970s, twenty-first century citizens have fallen captive to a far more powerful and comprehensive digital architecture of behavior control whose tentacles spread and root every day. Yesterday it was Facebook's integration of it communication platforms, today it is the disappearance of Nest into the maw of Google's device-led assault on everyday life. Tomorrow it is the Ford Motor Company's strategy to stream data from the 100,000 drivers of its vehicles. Our faces no longer belong to us. They are digital flows that feed the supply chains. Our voices are converted into "dialogue chunks" shuttled on digital conveyor belts to the new means of production. Our behavior is subjected to

subliminal cues, engineered social comparison dynamics, and schedules of reinforcement designed to tune and herd us at scale. Each of these exploit intimate knowledge of our demons and our dreams that would be impossible to achieve without Big Other, funded by the vast capital reserves of the surveillance capitalists and the revenues that stream from trading our futures.

Surveillance Capitalism breaks with the longstanding patterns of market democracy in several key ways. To begin, it abandons the organic reciprocities with people that have been key forces that helped to embed capitalism in society and tether it, however imperfectly, to society's interests. First, surveillance capitalists no longer rely on people as consumers. Instead, supply and demand orients the surveillance capitalist firm to businesses intent on anticipating the behavior of populations, groups, and individuals. Second, by historical standards the large surveillance capitalists employ relatively few people compared to their unprecedented computational resources. A small highly educated workforce leverages the power of a massive capital-intensive infrastructure. It is interesting to note that GM employed more people during the height of the Great Depression than either Google or Facebook employs at their heights of market capitalization. The absence of these reciprocities has significant implications because each contributed significantly to the spread of democracy. Consumer reciprocities were critical to the popular mobilization that became the American Revolution. Employee reciprocities helped drive the expansion of the democratic franchise in late nineteenth century Britain.

Instead of consumers or employees, surveillance capitalism regards its populations as sources of raw material for the rendition of behavioral surplus. In this way, surveillance capitalism assaults democracy from below and from above.

First, surveillance capitalism undermines democracy from below as its own imperatives set it on a collision course with human agency, the very autonomy that the Ervin committee understood as the elemental condition of human freedom and without which the very idea of a democratic society is impossible to imagine. Engineered ignorance robs us of decision rights over the boundaries of our own experience. Economies of action challenge our elemental rights to the future tense, to promise one

another and ourselves what we will do next, free of systematic, intentional, hidden interference. Prediction products require algorithmic certainty. Behavior must conform to parameters. Outliers are dangerous friction in a system oriented toward guaranteed outcomes.

Second, surveillance capitalism destroys democracy from above. It is an extraordinary fact that we embark upon the third decade of the twenty-first century with societies marked by more extreme asymmetries of knowledge and the power that accrues to such knowledge than have ever existed in human history. Trillions of data points and six million behavioral predictions per second are the surface of a shadow text over which democracy and its demos have no knowledge, no authority, and no control. Laws regarding data ownership, accessibility, or portability pertain to the public text and thus will not change this fact. Equally troubling is that only the surveillance capitalists have the financial, technological, and intellectual capital to know. At a time when we anticipated the democratization of knowledge, we find ourselves reverting to a pre-Gutenberg pattern of knowledge for the few not the many. They know more about us than we know about ourselves. They know much about us, but we know little about them. There knowledge is about us, but it is not for us. Their knowledge is accrued from our lives, but we are excluded from it.

These asymmetries award surveillance capitalists unauthorized social dominance. Industrial civilization enshrined the division of labor as the key principle of social order and oriented society toward the challenges of economic justice. Now an information civilization enshrines the *division of learning* as the new principle of social order and orients society toward epistemic justice. Three essential questions determine life chances in this new world: *Who knows? Who decides who knows? Who decides who decides who knows?* These are the intersecting dilemmas of knowledge, authority, and power in our time. In the absence of a democratic resurgence, it is the surveillance capitalists who occupy the catbird seat in this new world. They know, they decide who knows, and they decide who decides.

This anti-democratic and anti-egalitarian juggernaut is 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 as the technological Trojan horse of digital technology. On the strength of its annexation of human experience, this coup achieves exclusive concentrations of knowledge and power that sustain privileged influence over the division of learning in society. Bluntly stated, this means the privatization of the central principle of social ordering in the twenty-first century that imposes the social relations of a pre-modern absolutist authority. It is a form of tyranny that feeds on people but is not of the people. In a surreal paradox, this coup is celebrated as "personalization," although it defiles, ignores, overrides, and displaces everything about you and me that is personal. While democracy slept, surveillance capitalism created and claimed unilateral power over the shadow text in ways that have, at least so far, deprived democratic populations of means of combat.

By now the frustration is palpable. *The Age of Surveillance Capitalism* is a big book, but it has become an improbable international bestseller, with translations in over a dozen languages already underway. The reason appears to be a widely shared sense of a future careening off the rails. An economic logic is not something that you see, but it is something that you feel. People around the world are now feeling the effects of surveillance capitalism in their daily lives, and they don't like how it feels. Over the last five months of continuous travel in Europe and North America, I have asked every audience the same question: "What concerns bring you here today?" In every case the same short list of words rises from the room: "*anxiety, manipulation, freedom, malaise, autonomy, democracy, control, fear, resistance, rebellion, agency, power, law, rights... "* This suggests to me that the anonymous term "users" no longer holds meaning. Instead a democratic citizenry is awakening to its shared social, political, psychological, and economic interests. This blooming public awareness will find expression in new forms of collective action. It will insist on political leadership in the form of new law and regulatory regimes.

According to legal historian Lawrence Friedman this kind of phase change in the public demand for democratic remedies has many causes – cultural change, increased intensity of communications, a cyclical readiness to expand the scope of government. Above all it reflects the changing nature of the economy. 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. Only law was up to the task of tethering such the giant industrial corporations to the needs of a democratic society.

Today we face similar circumstances. The top five US companies by market capitalization are all tech companies.[4] Of the five, two are the pioneers of surveillance capitalism: Google and Facebook. Two began as more traditional sales-oriented firms that later diversified into surveillance capitalism: Microsoft and Amazon. The fifth, Apple, has been reluctant to embrace surveillance capitalism. Apple's current move into digital services will reveal a great deal about its resolve on this front. Even more important than the world-historic wealth amassed by these companies is the public's growing sense of the secrecy and vast complexity of their operations that have so far eluded any form of control. *Only democracy can meet this challenge.*

FREEDOM AND KNOWLEDGE

Lawmakers 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 upon 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 essential 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 computational, sensate, actuating 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 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."[5]

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."[6]

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."[7]

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 behavioral futures markets are rendered in infinite detail. Surveillance capitalism thus replaces mystery with certainty as it substitutes rendition, 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. 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." A top Facebook engineer put it succinctly: "We are trying to map out the graph of everything in the world and how it relates to each other." 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." Satya Nadella of Microsoft 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.

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 experience as computational data: our lives are scraped and sold to fund their freedom and our subjugation, their knowledge and our ignorance about what they know.

This new condition unravels the neoliberal 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 new applied utopianists 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 societies, and indeed as a civilization that *surveillance capitalists know too much to qualify for freedom.* The time for law has come.

WHAT IS TO BE DONE?

As stated at the outset, surveillance capitalism has thrived in the absence of law and regulation. Rather than mourning this state of affairs, I take it as a positive sign. We have not failed to reign in this rogue capitalism. On the contrary, we simply have not yet tried. And there is more good news: our societies have successfully confronted destructive forms of raw capitalism in the past, asserting new laws that tethered capitalism to the needs of people and the values of democracy. 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... We have every reason to believe that we can be successful again, liberating the digital future to its earlier promise marked by its deep compatibility with and contribution to a resurgent democracy.

In his insightful history, *Prophets of Regulation* Thomas McGraw recounts the phases and distinct purposes of regulatory regimes in the US from the 1870s in the early period of industrialization, the early twentieth century-- especially 1900-1916, the era of the New Deal, and the 1970's -1980's that brought the onset of deindustrialization. In some phases it was the muckrakers and progressives that defined the regulatory paradigm. In others it was the lawyers who dominated. Only recently has it been the economists who define the regulatory vision. Indeed, McGraw concludes that over the arc of this history, in the US at least, concerns for justice and fairness have overshadowed the more narrow aims of economic growth. "Regulation," he concludes, "is best understood as a political settlement." McGraw warns that the "economists' hour" will certainly end, and he wonders what will come next.

The challenges of surveillance capitalism provide the answer. Surveillance capitalism is a human-made phenomenon and it is in the realm of politics that it must be confronted. The next great regulatory vision will be framed and implemented by warriors for democracy: elected officials, citizens, and specialists 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 that is the single most powerful bulwark against tyranny. We give up these ideals at our peril. Only democracy can impose the people's interests through law and regulation. The question is, what kind of law and regulation? Will it be comprehensive privacy legislation? Will it be an antitrust approach, as demanded by those who counsel the breakup of Facebook?

There are some things we know: despite existing economic paradigms (antitrust) and legal paradigms (privacy), surveillance capitalism has had a relatively unimpeded two decades to root and flourish. McGraw warns that historically regulators failed when they did not "frame strategies appropriate to the particular industries they were

regulating." 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 neither will be wholly adequate to this new challenge.

An example is privacy law's call for "data ownership" This is a misleading notion because it legitimates the original sin that is the unilateral taking of human experience for rendition into data. Why institutionalize illegitimate data capture? In many cases the notion of data ownership is like negotiating how many hours a day a seven year old should be allowed to work, rather than contesting the fundamental legitimacy of child labor. Data ownership also fails to reckon with the realities of behavioral surplus. Even if "users" achieve "ownership" of the data that they provided in the first instance, they will not achieve "ownership" of behavioral surplus, the predictions gleaned from it, or the fate of those predictions in markets that trade in human futures.

The prospect of "breaking up" the large 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. Breaking up the largest surveillance capitalists – Google, Facebook, Microsoft, and Amazon – can address important anti-competitive problems, but without additional measures it will not prevent the emergence of smaller and more efficient surveillance capitalist firms, while opening the field for new surveillance capitalist competitors.

There are three arenas in which legislative and regulatory strategies can be effectively aligned with the structure and consequences of surveillance capitalism. These include interrupting and outlawing surveillance capitalism's key mechanisms, creating space for competitive solutions, and nurturing new forms of citizen-based collective and collaborative action.

First, Lawmakers today will need to devise strategies that interrupt and in some cases outlaw surveillance capitalism's foundational mechanisms, including,

1) the unilateral taking of private human experience as a free source of raw material and its translation into data; 2) the extreme information asymmetries necessary for predicting human behavior 3) the manufacture of computational prediction products based on the unilateral and secret capture of human experience; 4) the operation of prediction markets that trade in human futures, 5) the operations of radical indifference that impose false equivalence across all forms of data and thus encourage viruses without vaccines.

I want to call attention especially to front and back end opportunities to disrupt surveillance capitalism. At the front end, we can outlaw the secret theft of private experience for translation into behavioral data. For example, why should private companies be allowed to take our faces as we walk down the street? At the back end, we can outlaw markets that trade in human futures, because we know that their competitive dynamics necessarily produce the harms described here — and more. We already outlaw markets that traffic in slavery and those that traffic in human organs. Markets that traffic in human futures are also pernicious. The imperatives that arise from the competitive dynamics of these markets compel actors to combat friction, including the friction of human agency and shared knowledge. The imperatives thus compel operations that bypass user awareness and in this way impose ubiquitous surveillance for the sake of profit.

Second, from the point of view of supply and demand, surveillance capitalism can be understood as a market failure. Every piece of research over the last decade and a half suggests that when "users" are informed of surveillance capitalism's backstage operations, they want protection, and they want alternatives. We will need laws and regulatory frameworks designed to advantage companies that want to break with the surveillance capitalist paradigm. Forging an alternative trajectory to the digital future will require alliances of new competitors who can summon and institutionalize an alternative ecosystem. True competitors that align themselves with the actual needs of people and the norms of a market democracy are likely to attract just about every person on earth as their customer.

Third, lawmakers will need to support new forms of collective action, just as nearly a century ago workers won legal protection for their rights to organize, to bargain collectively, and to strike. New forms of citizen solidarity are already emerging in 1) municipalities that seek an alternative to a Google-owned smart city future, 2) in communities that want to resist the social costs of so-called "disruption" imposed for the sake of others' gain, and 3) among workers who seek fair wages and reasonable security in the precarious conditions of the "gig economy." Citizens need your help, and you need citizen support if together we aim to shift the trajectory of the digital future back toward its emancipatory promise on the way to a place that we can all call *home*.

ENDNOTES

---

[1] 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/.

[2] Darren Davidson, "Facebook Targets 'Insecure' To Sell Ads," Australian, May 1, 2017.

[3] Darren Davidson.

[4] http://dogsofthedow.com/largest-companies-by-market-cap.htm

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

[6] Friedrich August von Hayek, The Collected Works of Friedrich August Hayek, ed. William Warren Bartley (Chicago: University of Chicago Press, 1988), 1:14.

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