The New York Times https://nyti.ms/2sXbT2d

Opinion

You Are Now Remotely Controlled

Surveillance capitalists control the science and the scientists, the secrets and the truth.

By Shoshana Zuboff
Ms. Zuboff is the author of "The Age of Surveillance Capitalism."

Jan. 24, 2020

The debate on privacy and law at the Federal Trade Commission was unusually heated that day. Tech industry executives "argued that they were capable of regulating themselves and that government intervention would be costly and counterproductive." Civil libertarians warned that the companies' data capabilities posed "an unprecedented threat to individual freedom." One observed, "We have to decide what human beings are in the electronic age. Are we just going to be chattel for commerce?" A commissioner asked, ''Where should we draw the line?" The year was 1997.

The line was never drawn, and the executives got their way. Twenty-three years later the evidence is in. The fruit of that victory was a new economic logic that I call "surveillance capitalism." Its success depends upon one-way-mirror operations engineered for our ignorance and wrapped in a fog of misdirection, euphemism and mendacity. It rooted and flourished in the new spaces of the internet, once celebrated by surveillance capitalists as "the world's largest ungoverned space." But power fills a void, and those once wild spaces are no longer ungoverned. Instead, they are owned and operated by private surveillance capital and governed by its iron laws.

The rise of surveillance capitalism over the last two decades went largely unchallenged. "Digital" was fast, we were told, and stragglers would be left behind. It's not surprising that so many of us rushed to follow the bustling White Rabbit down his tunnel into a promised digital Wonderland where, like Alice, we fell prey to delusion. In Wonderland, we celebrated the new digital services as free, but now we see that the surveillance capitalists behind those services regard us as the free commodity. We thought that we search Google, but now we understand that Google searches us. We assumed that we use social media to connect, but we learned that connection is how social media uses us. We barely questioned why our new TV or mattress had a privacy policy, but we've begun to understand that "privacy" policies are actually surveillance policies.

And like our forebears who named the automobile "horseless carriage" because they could not reckon with its true dimension, we regarded the internet platforms as "bulletin boards" where anyone could pin a note. Congress cemented this delusion in a statute, Section 230 of the 1996 Communications Decency Act, absolving those companies of the obligations that adhere to "publishers" or even to "speakers."

Only repeated crises have taught us that these platforms are not bulletin boards but hyper-velocity global bloodstreams into which anyone may introduce a dangerous virus without a vaccine. This is how Facebook's chief executive, Mark Zuckerberg, could legally refuse to remove a faked video of Speaker of the House Nancy Pelosi and later double down on this decision, announcing that political advertising would not be subject to fact-checking.

All of these delusions rest on the most treacherous hallucination of them all: the belief that privacy is private. We have imagined that we can choose our degree of privacy with an individual calculation in which a bit of personal information is traded for valued services — a reasonable quid pro quo. For example, when Delta Air Lines piloted a

biometric data system at the Atlanta airport, the company reported that of nearly 25,000 customers who traveled there each week, 98 percent opted into the process, noting that "the facial recognition option is saving an average of two seconds for each customer at boarding, or nine minutes when boarding a wide body aircraft."

In fact the rapid development of facial recognition systems reveals the public consequences of this supposedly private choice. Surveillance capitalists have demanded the right to take our faces wherever they appear — on a city street or a Facebook page. The Financial Times reported that a Microsoft facial recognition training database of 10 million images plucked from the internet without anyone's knowledge and supposedly limited to academic research was employed by companies like IBM and state agencies that included the United States and Chinese military. Among these were two Chinese suppliers of equipment to officials in Xinjiang, where members of the Uighur community live in open-air prisons under perpetual surveillance by facial recognition systems.

Privacy is not private, because the effectiveness of these and other private or public surveillance and control systems depends upon the pieces of ourselves that we give up — or that are secretly stolen from us.

Our digital century was to have been democracy's Golden Age. Instead, we enter its third decade marked by a stark new form of social inequality best understood as "epistemic inequality." It recalls a pre-Gutenberg era of extreme asymmetries of knowledge and the power that accrues to such knowledge, as the tech giants seize control of information and learning itself. The delusion of "privacy as private" was crafted to breed and feed this unanticipated social divide. Surveillance capitalists exploit the widening inequity of knowledge for the sake of profits. They manipulate the economy, our society and even our lives with impunity, endangering not just individual privacy but democracy itself. Distracted by our delusions, we failed to notice this bloodless coup from above.

The belief that privacy is private has left us careening toward a future that we did not choose, because it failed to reckon with the profound distinction between a society that insists upon sovereign individual rights and one that lives by the social relations of the one-way mirror. The lesson is that *privacy is public* — it is a collective good that is logically and morally inseparable from the values of human autonomy and self-determination upon which privacy depends and without which a democratic society is unimaginable.

Still, the winds appear to have finally shifted. A fragile new awareness is dawning as we claw our way back up the rabbit hole toward home. Surveillance capitalists are fast because they seek neither genuine consent nor consensus. They rely on psychic numbing and messages of inevitability to conjure the helplessness, resignation and confusion that paralyze their prey. Democracy is slow, and that's a good thing. Its pace reflects the tens of millions of conversations that occur in families, among neighbors, co-workers and friends, within communities, cities and states, gradually stirring the sleeping giant of democracy to action.

These conversations are occurring now, and there are many indications that lawmakers are ready to join and to lead. This third decade is likely to decide our fate. Will we make the digital future better, or will it make us worse? Will it be a place that we can call home?

Epistemic inequality is not based on what we can earn but rather on what we can learn. It is defined as unequal access to learning imposed by private commercial mechanisms of information capture, production, analysis and sales. It is best exemplified in the fast-growing abyss between what we know and what is known about us.

Twentieth-century industrial society was organized around the "division of labor," and it followed that the struggle for economic equality would shape the politics of that time. Our digital century shifts society's coordinates from a division of labor to a "division of learning," and it follows that the struggle over access to knowledge and the power conferred by such knowledge will shape the politics of our time.

The new centrality of epistemic inequality signals a power shift from the ownership of the means of production, which defined the politics of the 20th century, to the ownership of the production of meaning. The challenges of epistemic justice and epistemic rights in this new era are summarized in three essential questions about knowledge, authority and power: Who knows? Who decides who knows? Who decides who decides who knows?

During the last two decades, the leading surveillance capitalists — Google, later followed by Facebook, Amazon and Microsoft — helped to drive this societal transformation while simultaneously ensuring their ascendance to the pinnacle of the epistemic hierarchy. They operated in the shadows to amass huge knowledge monopolies by taking without asking, a maneuver that every child recognizes as theft. Surveillance capitalism begins by unilaterally staking a claim to private human experience as free raw material for translation into behavioral data. Our lives are rendered as data flows.

Early on, it was discovered that, unknown to users, even data freely given harbors rich predictive signals, a surplus that is more than what is required for service improvement. It isn't only what you post online, but whether you use exclamation points or the color saturation of your photos; not just where you walk but the stoop of your shoulders; not just the identity of your face but the emotional states conveyed by your "microexpressions"; not just what you like but the pattern of likes across engagements. Soon this behavioral surplus was secretly hunted and captured, claimed as proprietary data.

The data are conveyed through complex supply chains of devices, tracking and monitoring software, and ecosystems of apps and companies that specialize in niche data flows captured in secret. For example, testing by The Wall Street Journal showed that Facebook receives heart rate data from the Instant Heart Rate: HR Monitor, menstrual cycle data from the Flo Period & Ovulation Tracker, and data that reveal interest in real estate properties from Realtor.com — all of it without the user's knowledge.

These data flows empty into surveillance capitalists' computational factories, called "artificial intelligence," where they are manufactured into behavioral predictions that are about us, but they are not *for us*. Instead, they are sold to business customers in a new kind of market that trades exclusively in human futures. Certainty in human affairs is the lifeblood of these markets, where surveillance capitalists compete on the quality of their predictions. This is a new form of trade that birthed some of the richest and most powerful companies in history.

Illustration by Erik Carter; Photograph by Getty Images

In order to achieve their objectives, the leading surveillance capitalists sought to establish unrivaled dominance over the 99.9 percent of the world's information now rendered in digital formats that they helped to create. Surveillance capital has built most of the world's largest computer networks, data centers, populations of servers, undersea transmission cables, advanced microchips, and frontier machine intelligence, igniting an arms race for the 10,000 or so specialists on the planet who know how to coax knowledge from these vast new data continents.

With Google in the lead, the top surveillance capitalists seek to control labor markets in critical expertise, including data science and animal research, elbowing out competitors such as start-ups, universities, high schools, municipalities, established corporations in other industries and less wealthy countries. In 2016, 57 percent of American computer science Ph.D. graduates took jobs in industry, while only 11 percent became tenure-track faculty members. It's not just an American problem. In Britain, university administrators contemplate a "missing generation" of data scientists. A Canadian scientist laments, "the power, the expertise, the data are all concentrated in the hands of a few companies."

Google created the first insanely lucrative markets to trade in human futures, what we now know as online targeted advertising, based on their predictions of which ads users would click. Between 2000, when the new economic logic was just emerging, and 2004, when the company went public, revenues increased by 3,590 percent. This startling number represents the "surveillance dividend." It quickly reset the bar for investors, eventually driving start-ups, apps developers and established companies to shift their business models toward surveillance capitalism. The promise of a fast track to outsized revenues from selling human futures drove this migration first to Facebook, then through the tech sector and now throughout the rest of the economy to industries as disparate as insurance, retail, finance, education, health care, real estate, entertainment and every product that begins with the word "smart" or service touted as "personalized."

Even Ford, the birthplace of the 20th-century mass production economy, is on the trail of the surveillance dividend, proposing to meet the challenge of slumping car sales by reimagining Ford vehicles as a "transportation operating system." As one analyst put it, Ford "could make a fortune monetizing data. They won't need engineers, factories or dealers to do it. It's almost pure profit."

Surveillance capitalism's economic imperatives were refined in the competition to sell certainty. Early on it was clear that machine intelligence must feed on volumes of data, compelling economies of scale in data extraction. Eventually it was understood that volume is necessary but not sufficient. The best algorithms also require varieties of data — economies of scope. This realization helped drive the "mobile revolution" sending users into the real world armed with cameras, computers, gyroscopes and microphones packed inside their smart new phones. In the competition for scope, surveillance capitalists want your home and what you say and do within its walls. They want your car, your medical conditions, and the shows you stream; your location as well as all the streets and buildings in your path and all the behavior of all the people in your city. They want your voice and what you eat and what you buy; your children's play time and their schooling; your brain waves and your bloodstream. Nothing is exempt.

Unequal knowledge about us produces unequal power over us, and so epistemic inequality widens to include the distance between what we can do and what can be done to us. Data scientists describe this as the shift from monitoring to actuation, in which a critical mass of knowledge about a machine system enables the remote control of that system. Now people have become targets for remote control, as surveillance capitalists discovered that the most predictive data come from intervening in behavior to tune, herd and modify action in the direction of commercial objectives. This third imperative, "economies of action," has become an arena of intense experimentation. "We are learning how to write the music," one scientist said, "and then we let the music make them dance."

This new power "to make them dance" does not employ soldiers to threaten terror and murder. It arrives carrying a cappuccino, not a gun. It is a new "instrumentarian" power that works its will through the medium of ubiquitous digital instrumentation to manipulate subliminal cues, psychologically target communications, impose default choice

architectures, trigger social comparison dynamics and levy rewards and punishments — all of it aimed at remotely tuning, herding and modifying human behavior in the direction of profitable outcomes and always engineered to preserve users' ignorance.

We saw predictive knowledge morphing into instrumentarian power in Facebook's contagion experiments published in 2012 and 2014, when it planted subliminal cues and manipulated social comparisons on its pages, first to influence users to vote in midterm elections and later to make people feel sadder or happier. Facebook researchers celebrated the success of these experiments noting two key findings: that it was possible to manipulate online cues to influence real world behavior and feelings, and that this could be accomplished while successfully bypassing users' awareness.

In 2016, the Google-incubated augmented reality game, Pokémon Go, tested economies of action on the streets. Game players did not know that they were pawns in the real game of behavior modification for profit, as the rewards and punishments of hunting imaginary creatures were used to herd people to the McDonald's, Starbucks and local pizza joints that were paying the company for "footfall," in exactly the same way that online advertisers pay for "click through" to their websites.

In 2017, a leaked Facebook document acquired by The Australian exposed the corporation's interest in applying "psychological insights" from "internal Facebook data" to modify user behavior. The targets were 6.4 million young Australians and New Zealanders. "By monitoring posts, pictures, interactions and internet activity in real time," the executives wrote, "Facebook can work out when young people feel 'stressed,' 'defeated,' 'overwhelmed,' 'anxious,' 'nervous,' 'stupid,' 'silly,' 'useless' and a 'failure.'" This depth of information, they explained, allows Facebook to pinpoint the time frame during which a young person needs a "confidence boost" and is most vulnerable to a specific configuration of subliminal cues and triggers. The data are then used to match each emotional phase with appropriate ad messaging for the maximum probability of guaranteed sales.

Facebook denied these practices, though a former product manager accused the company of "lying through its teeth." The fact is that in the absence of corporate transparency and democratic oversight, epistemic inequality rules. They know. They decide who knows. They decide who decides.

The public's intolerable knowledge disadvantage is deepened by surveillance capitalists' perfection of mass communications as gaslighting. Two examples are illustrative. On April 30, 2019 Mark Zuckerberg made a dramatic announcement at the company's annual developer conference, declaring, "The future is private." A few weeks later, a Facebook litigator appeared before a federal district judge in California to thwart a user lawsuit over privacy invasion, arguing that the very act of using Facebook negates any reasonable expectation of privacy "as a matter of law." In May 2019 Sundar Pichai, chief executive of Google, wrote in The Times of his corporations's commitment to the principle that "privacy cannot be a luxury good." Five months later Google contractors were found offering $5 gift cards to homeless people of color in an Atlanta park in return for a facial scan.

Facebook's denial invites even more scrutiny in light of another leaked company document appearing in 2018. The confidential report offers rare insight into the heart of Facebook's computational factory, where a "prediction engine" runs on a machine intelligence platform that "ingests trillions of data points every day, trains thousands of models" and then "deploys them to the server fleet for live predictions." Facebook notes that its "prediction service" produces "more than 6 million predictions per second." But to what purpose?

In its report, the company makes clear that these extraordinary capabilities are dedicated to meeting its corporate customers' "core business challenges" with procedures that link prediction, microtargeting, intervention and behavior modification. For example, a Facebook service called "loyalty prediction" is touted for its ability to plumb proprietary behavioral surplus to predict individuals who are "at risk" of shifting their brand allegiance and alerting advertisers to intervene promptly with targeted messages designed to stabilize loyalty just in time to alter the course of the future.

That year a young man named Christopher Wylie turned whistle-blower on his former employer, a political consultancy known as Cambridge Analytica. “We exploited Facebook to harvest millions of people’s profiles,” Wylie admitted, “and built models to exploit what we knew about them and target their inner demons.” Mr. Wylie characterized those techniques as “information warfare,” correctly assessing that such shadow wars are built on asymmetries of knowledge and the power it affords. Less clear to the public or lawmakers was that the political firm’s strategies of secret invasion and conquest employed surveillance capitalism’s standard operating procedures to which billions of innocent “users” are routinely subjected each day. Mr. Wylie described this mirroring process, as he followed a trail that was already cut and marked. Cambridge Analytica’s real innovation was to pivot the whole undertaking from commercial to political objectives.

In other words, Cambridge Analytica was the parasite, and surveillance capitalism was the host. Thanks to its epistemic dominance, surveillance capitalism provided the behavioral data that exposed the *targets* for assault. Its methods of behavioral microtargeting and behavioral modification became the *weapons*. And it was surveillance capitalism’s lack of accountability for content on its platform afforded by Section 230 that provided the *opportunity* for the stealth attacks designed to trigger the inner demons of unsuspecting citizens.

It’s not just that epistemic inequality leaves us utterly vulnerable to the attacks of actors like Cambridge Analytica. The larger and more disturbing point is that surveillance capitalism has turned epistemic inequality into a defining condition of our societies, normalizing information warfare as a chronic feature of our daily reality prosecuted by the very corporations upon which we depend for effective social participation. They have the knowledge, the machines, the science and the scientists, the secrets and the lies. All privacy now rests with them, leaving us with few means of defense from these marauding data invaders. Without law, we scramble to hide in our own lives, while our children debate encryption strategies around the dinner table and students wear masks to public protests as protection from facial recognition systems built with our family photos.

In the absence of new declarations of epistemic rights and legislation, surveillance capitalism threatens to remake society as it unmakes democracy. From below, it undermines human agency, usurping privacy, diminishing autonomy and depriving individuals of the right to combat. From above, epistemic inequality and injustice are fundamentally incompatible with the aspirations of a democratic people.

We know that surveillance capitalists work in the shadows, but what they do there and the knowledge they accrue are unknown to us. They have the means to know everything about us, but we can know little about them. Their knowledge of us is not for us. Instead, our futures are sold for others’ profits. Since that Federal Trade Commission meeting in 1997, the line was never drawn, and people did become chattel for commerce. Another destructive delusion is that this outcome was inevitable — an unavoidable consequence of convenience-enhancing digital technologies. The truth is that surveillance capitalism hijacked the digital medium. There was nothing inevitable about it.

American lawmakers have been reluctant to take on these challenges for many reasons. One is an unwritten policy of “surveillance exceptionalism” forged in the aftermath of the Sept. 11 terrorist attacks, when the government’s concerns shifted from online privacy protections to a new zeal for “total information awareness.” In that political environment the fledgling surveillance capabilities emerging from Silicon Valley appeared to hold great promise.

Surveillance capitalists have also defended themselves with lobbying and forms of propaganda intended to undermine and intimidate lawmakers, confounding judgment and freezing action. These have received relatively little scrutiny compared to the damage they do. Consider two examples:

The first is the assertion that democracy threatens prosperity and innovation. Former Google chief executive Eric Schmidt explained in 2011, “we took the position of ‘hands off the internet.’ You know, leave us alone … The government can make regulatory mistakes that can slow this whole thing down, and we see that and we worry about

it." This propaganda is recycled from the Gilded Age barons, whom we now call "robbers." They insisted that there was no need for law when one had the "law of survival of the fittest," the "laws of capital" and the "law of supply and demand."

Paradoxically, surveillance capital does not appear to drive innovation. A promising new era of economic research shows the critical role that government and democratic governance have played in innovation and suggests a lack of innovation in big tech companies like Google. Surveillance capitalism's information dominance is not dedicated to the urgent challenges of carbon-free energy, eliminating hunger, curing cancers, ridding the oceans of plastic or flooding the world with well paid, smart, loving teachers and doctors. Instead, we see a frontier operation run by geniuses with vast capital and computational power that is furiously dedicated to the lucrative science and economics of human prediction for profit.

The second form of propaganda is the argument that the success of the leading surveillance capitalist firms reflects the real value they bring to people. But data from the demand side suggest that surveillance capitalism is better understood as a market failure. Instead of a close alignment of supply and demand, people use these services because they have no comparable alternatives and because they are ignorant of surveillance capitalism's shadow operations and their consequences. Pew Research Center recently reported that 81 percent of Americans believe the potential risks of companies' data collection outweigh the benefits, suggesting that corporate success depends upon coercion and obfuscation rather than meeting people's real needs.

In his prizewinning history of regulation, the historian Thomas McCraw delivers a warning. Across the centuries regulators failed when they did not frame "strategies appropriate to the particular industries they were regulating." Existing privacy and antitrust laws are vital but neither will be wholly adequate to the new challenges of reversing epistemic inequality.

These contests of the 21st century demand a framework of epistemic rights enshrined in law and subject to democratic governance. Such rights would interrupt data supply chains by safeguarding the boundaries of human experience before they come under assault from the forces of datafication. The choice to turn any aspect of one's life into data must belong to individuals by virtue of their rights in a democratic society. This means, for example, that companies cannot claim the right to your face, or use your face as free raw material for analysis, or own and sell any computational products that derive from your face. The conversation on epistemic rights has already begun, reflected in a pathbreaking report from Amnesty International.

On the demand side, we can outlaw human futures markets and thus eliminate the financial incentives that sustain the surveillance dividend. This is not a radical prospect. For example, societies outlaw markets that trade in human organs, babies and slaves. In each case, we recognize that such markets are both morally repugnant and produce predictably violent consequences. Human futures markets can be shown to produce equally predictable outcomes that challenge human freedom and undermine democracy. Like subprime mortgages and fossil fuel investments, surveillance assets will become the new toxic assets.

In support of a new competitive landscape, lawmakers will need to champion new forms of collective action, just as nearly a century ago legal protections for the rights to organize, to strike and to bargain collectively united lawmakers and workers in curbing the powers of monopoly capitalists. Lawmakers must seek alliances with citizens who are deeply concerned over the unchecked power of the surveillance capitalists and with workers who seek fair wages and reasonable security in defiance of the precarious employment conditions that define the surveillance economy.

Anything made by humans can be unmade by humans. Surveillance capitalism is young, barely 20 years in the making, but democracy is old, rooted in generations of hope and contest.

Surveillance capitalists are rich and powerful, but they are not invulnerable. They have an Achilles heel: fear. They fear lawmakers who do not fear them. They fear citizens who demand a new road forward as they insist on new answers to old questions: Who will know? Who will decide who knows? Who will decide who decides? Who will

write the music, and who will dance?

Shoshana Zuboff (@ShoshanaZuboff) is professor emerita at Harvard Business School and the author of “The Age of Surveillance Capitalism.”

The Times is committed to publishing a diversity of letters to the editor. We’d like to hear what you think about this or any of our articles. Here are some tips. And here’s our email: letters@nytimes.com.

Follow @privacyproject on Twitter and The New York Times Opinion Section on Facebook and Instagram.