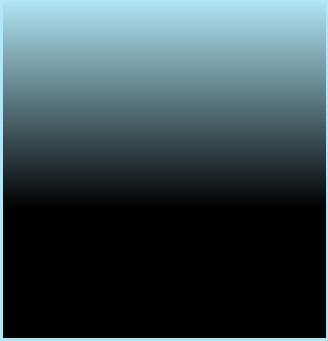
SURVEILLANCE



CAPITALISM

A Reader

Surveillance Capitalism

A Reader

MOZZARELLA.WEBSITE

CONTENTS

The Secrets of Surveillance Capitalism

by Shoshana Zuboff
From Frankfurter Allgemeine Zeitung *May 3, 2016*

Google surpassed Apple as the world's most highly valued company in January for the first time since 2010. (Back then each company was worth less than 200 billion. Now each is valued at well over 500 billion.) While Google's new lead lasted only a few days, the company's success has implications for everyone who lives within the reach of the Internet. Why? Because Google is ground zero for a wholly new subspecies of capitalism in which profits derive from the unilateral surveillance and modification of human behavior. This is a new *surveillance capitalism* that is unimaginable outside the inscrutable high velocity circuits of Google's digital universe, whose signature feature is the Internet and its successors. While the world is riveted by the showdown between Apple and the FBI, the real truth is that the surveillance capabilities being developed by surveillance capitalists are the envy of every state security agency. What are the secrets of this new capitalism, how do they produce such staggering wealth, and how can we protect ourselves from its invasive power?

Most Americans realize that there are two groups of people who

are monitored regularly as they move about the country. The first group is monitored involuntarily by a court order requiring that a tracking device be attached to their ankle. The second group includes everyone else…

Some will think that this statement is certainly true. Others will worry that it could become true. Perhaps some think it's ridiculous. It's not a quote from a dystopian novel, a Silicon Valley executive, or even an NSA official. These are the words of an auto insurance industry consultant intended as a defense of "automotive telematics" and the astonishingly intrusive surveillance capabilities of the allegedly benign systems that are already in use or under development. It's an industry that has been notoriously exploitative toward customers and has had obvious cause to be anxious about the implications of self-driving cars for its business model. Now, data about where we are, where we're going, how we're feeling, what we're saying, the details of our driving, and the conditions of our vehicle are turning into beacons of revenue that illuminate a new commercial prospect. According to the industry literature, these data can be used for dynamic real-time driver behavior modification triggering punishments (real-time rate hikes, financial penalties, curfews, engine lock-downs) or rewards (rate discounts, coupons, gold stars to redeem for future benefits).

Bloomberg Business Week notes that these automotive systems will give insurers a chance to boost revenue by selling customer driving data in the same way that Google profits by collecting information on those who use its search engine. The CEO of Allstate Insurance wants to be like Google. He says, "There are lots of people who are monetizing data today. You get on Google, and it seems like it's free. It's not free. You're giving them information; they sell your information. Could we, should we, sell this information we get from people driving around to various people and capture some additional profit source…? It's a long-term game."

Who are these "various people" and what is this "long-term game"? The game is no longer about sending you a mail order catalogue or even about targeting online advertising. The game is selling access to the real-time flow of your daily life—your

reality—in order to directly influence and modify your behavior for profit. This is the gateway to a new universe of monetization opportunities: restaurants who want to be your destination. Service vendors who want to fix your brake pads. Shops who will lure you like the fabled Sirens. The "various people" are anyone, and everyone who wants a piece of your behavior for profit. Small wonder, then, that Google recently announced that its maps will not only provide the route you search but will also suggest a destination.

The goal: to change people's actual behavior at scale

This is just one peephole, in one corner, of one industry, and the peepholes are multiplying like cockroaches. Among the many interviews I've conducted over the past three years, the Chief Data Scientist of a much-admired Silicon Valley company that develops applications to improve students' learning told me, "The goal of everything we do is to change people's actual behavior at scale. When people use our app, we can capture their behaviors, identify good and bad behaviors, and develop ways to reward the good and punish the bad. We can test how actionable our cues are for them and how profitable for us."

The very idea of a functional, effective, affordable product as a sufficient basis for economic exchange is dying. The sports apparel company Under Armour is reinventing its products as wearable technologies. The CEO wants to be like Google. He says, "If it all sounds eerily like those ads that, because of your browsing history, follow you around the Internet, that's exactly the point—except Under Armour is tracking real behavior and the data is more specific...making people better athletes makes them need more of our gear." The examples of this new logic are endless, from smart vodka bottles to Internet-enabled rectal thermometers and quite literally everything in between. A Goldman Sachs report calls it a "gold rush," a race to "vast amounts of data."

The assault on behavioral data

We've entered virgin territory here. The assault on behavioral data is so sweeping that it can no longer be circumscribed by the concept of privacy and its contests. This is a different kind of challenge now, one that threatens the existential and political

canon of the modern liberal order defined by principles of self-determination that have been centuries, even millennia, in the making. I am thinking of matters that include, but are not limited to, the sanctity of the individual and the ideals of social equality; the development of identity, autonomy, and moral reasoning; the integrity of contract, the freedom that accrues to the making and fulfilling of promises; norms and rules of collective agreement; the functions of market democracy; the political integrity of societies; and the future of democratic sovereignty. In the fullness of time, we will look back on the establishment in Europe of the "Right to be Forgotten" and the EU's more recent invalidation of the Safe Harbor doctrine as early milestones in a gradual reckoning with the true dimensions of this challenge.

There was a time when we laid responsibility for the assault on behavioral data at the door of the state and its security agencies. Later, we also blamed the cunning practices of a handful of banks, data brokers, and Internet companies. Some attribute the assault to an inevitable "age of big data," as if it were possible to conceive of data born pure and blameless, data suspended in some celestial place where facts sublimate into truth.

Capitalism has been hijacked by surveillance

I've come to a different conclusion: The assault we face is driven in large measure by the exceptional appetites of a wholly new genus of capitalism, a systemic coherent new logic of accumulation that I call *surveillance capitalism*. Capitalism has been hijacked by a lucrative surveillance project that subverts the "normal" evolutionary mechanisms associated with its historical success and corrupts the unity of supply and demand that has for centuries, however imperfectly, tethered capitalism to the genuine needs of its populations and societies, thus enabling the fruitful expansion of market democracy.

Surveillance capitalism is a novel economic mutation bred from the clandestine coupling of the vast powers of the digital with the radical indifference and intrinsic narcissism of the financial capitalism and its neoliberal vision that have dominated commerce for at least three decades, especially in the Anglo economies. It is an unprecedented market form

that roots and flourishes in lawless space. It was first discovered and consolidated at Google, then adopted by Facebook, and quickly diffused across the Internet. Cyberspace was its birthplace because, as Google/Alphabet Chairperson Eric Schmidt and his coauthor, Jared Cohen, celebrate on the very first page of their book about the digital age, "the online world is not truly bound by terrestrial laws...it's the world's largest ungoverned space."

While surveillance capitalism taps the invasive powers of the Internet as the source of capital formation and wealth creation, it is now, as I have suggested, poised to transform commercial practice across the real world too. An analogy is the rapid spread of mass production and administration throughout the industrialized world in the early twentieth century, but with one major caveat. Mass production was interdependent with its populations who were its consumers and employees. In contrast, surveillance capitalism preys on dependent populations who are neither its consumers nor its employees and are largely ignorant of its procedures.

Internet access as a fundamental human right

We once fled to the Internet as solace and solution, our needs for effective life thwarted by the distant and increasingly ruthless operations of late twentieth century capitalism. In less than two decades after the Mosaic web browser was released to the public enabling easy access to the World Wide Web, a 2010 BBC poll found that 79% of people in 26 countries considered Internet access to be a fundamental human right. This is the Scylla and Charybdis of our plight. It is nearly impossible to imagine effective social participation—from employment, to education, to healthcare—without Internet access and know-how, even as these once flourishing networked spaces fall to a new and even more exploitative capitalist regime. It's happened quickly and without our understanding or agreement. This is because the regime's most poignant harms, now and later, have been difficult to grasp or theorize, blurred by extreme velocity and camouflaged by expensive and illegible machine operations, secretive corporate practices, masterful rhetorical misdirection, and purposeful cultural misappropriation.

Taming this new force depends upon careful naming. This symbiosis of naming and taming is vividly illustrated in the recent history of HIV research, and I offer it as analogy. For three decades scientists aimed to create a vaccine that followed the logic of earlier cures, training the immune system to produce neutralizing antibodies, but mounting data revealed unanticipated behaviors of the HIV virus that defy the patterns of other infectious diseases.

HIV research as analogy

The tide began to turn at the International AIDS Conference in 2012, when new strategies were presented that rely on a close understanding of the biology of rare HIV carriers whose blood produces natural antibodies. Research began to shift toward methods that reproduce this self- vaccinating response. A leading researcher announced, "We know the face of the enemy now, and so we have some real clues about how to approach the problem."

The point for us is that every successful vaccine begins with a close understanding of the enemy disease. We tend to rely on mental models, vocabularies, and tools distilled from past catastrophes. I am thinking of the twentieth century's totalitarian nightmares or the monopolistic predations of Gilded Age capitalism. But the vaccines we've developed to fight those earlier threats are not sufficient or even appropriate for the novel challenges we face. It's like we're hurling snowballs at a smooth marble wall only to watch them slide down its façade, leaving nothing but a wet smear: a fine paid here, an operational detour there.

An evolutionary dead-end

I want to say plainly that surveillance capitalism is not the only current modality of information capitalism, nor is it the only possible model for the future. Its fast track to capital accumulation and rapid institutionalization, however, has made it the default model of information capitalism. The questions I pose are these: Will surveillance capitalism become the dominant logic of accumulation in our time or, will it be an evolutionary dead-end—a toothed bird in capitalism's longer journey? What will an effective vaccine entail?

A cure depends upon many individual, social, and legal adaptations, but I am convinced that fighting the "enemy disease" cannot begin

without a fresh grasp of the novel mechanisms that account for surveillance capitalism's successful transformation of investment into capital. This has been one focus of my work in a new book, *Master or Slave: The Fight for the Soul of Our Information Civilization*, which will be published early next year. In the short space of this essay, I'd like to share some of my thoughts on this problem.

Fortune telling and selling

New economic logics and their commercial models are discovered by people in a time and place and then perfected through trial and error. Ford discovered and systematized mass production. General Motors institutionalized mass production as a new phase of capitalist development with the discovery and perfection of large-scale administration and professional management. In our time, Google is to surveillance capitalism what Ford and General Motors were to mass-production and managerial capitalism a century ago: discoverer, inventor, pioneer, role model, lead practitioner, and diffusion hub.

Specifically, Google is the mothership and ideal type of a new economic logic based on fortune telling and selling, an ancient and eternally lucrative craft that has exploited the human confrontation with uncertainty from the beginning of the human story. Paradoxically, the certainty of uncertainty is both an enduring source of anxiety and one of our most fruitful facts. It produced the universal need for social trust and cohesion, systems of social organization, familial bonding, and legitimate authority, the contract as formal recognition of reciprocal rights and obligations, and the theory and practice of what we call "free will." When we eliminate uncertainty, we forfeit the human replenishment that attaches to the challenge of asserting predictability in the face of an always- unknown future in favor of the blankness of perpetual compliance with someone else's plan.

Only incidentally related to advertising

Most people credit Google's success to its advertising model. But the discoveries that led to Google's rapid rise in revenue and market capitalization are only incidentally related to advertising. Google's success derives from its ability to predict the future—specifically the future of

behavior. Here is what I mean:

From the start, Google had collected data on users' search-related behavior as a byproduct of query activity. Back then, these data logs were treated as waste, not even safely or methodically stored. Eventually, the young company came to understand that these logs could be used to teach and continuously improve its search engine.

The problem was this: Serving users with amazing search results "used up" all the value that users created when they inadvertently provided behavioral data. It's a complete and self-contained process in which users are ends-in-themselves. All the value that users create is reinvested in the user experience in the form of improved search. In this cycle, there was nothing left over for Google to turn into capital. As long as the effectiveness of the search engine needed users' behavioral data about as much as users needed search, charging a fee for service was too risky. Google was cool, but it wasn't yet capitalism—just one of many Internet startups that boasted "eyeballs" but no revenue.

Shift in the use of behavioral data

The year 2001 brought the dotcom bust and mounting investor pressures at Google. Back then advertisers selected the search term pages for their displays. Google decided to try and boost ad revenue by applying its already substantial analytical capabilities to the challenge of increasing an ad's relevance to users—and thus its value to advertisers. Operationally this meant that Google would finally repurpose its growing cache of behavioral data. Now the data would *also* be used to match ads with keywords, exploiting subtleties that only its access to behavioral data, combined with its analytical capabilities, could reveal.

It's now clear that this shift in the use of behavioral data was an historic turning point. Behavioral data that were once discarded or ignored were rediscovered as what I call *behavioral surplus*. Google's dramatic success in "matching" ads to pages revealed the transformational value of this behavioral surplus as a means of generating revenue and ultimately turning investment into capital. Behavioral surplus was the game-changing zero-cost asset that could be diverted

from service improvement toward a genuine market exchange. Key to this formula, however, is the fact that this new market exchange was not an exchange with users but rather with other companies who understood how to make money from bets on users' future behavior. In this new context, users were no longer an end-in-themselves. Instead they became a means to profits in a new kind of marketplace in which users are neither buyers nor sellers nor products. Users are the source of free raw material that feeds a new kind of manufacturing process.

While these facts are known, their significance has not been fully appreciated or adequately theorized. What just happened was the discovery of a surprisingly profitable commercial equation—a series of lawful relationships that were gradually institutionalized in the *sui generis* economic logic of surveillance capitalism. It's like a newly sighted planet with its own physics of time and space, its sixty-seven hour days, emerald sky, inverted mountain ranges, and dry water.

A parasitic form of profit

The equation: First, the push for more users and more channels, services, devices, places, and spaces is imperative for access to an ever-expanding range of *behavioral surplus*. Users are the *human natureal resource* that provides this free raw material. Second, the application of machine learning, artificial intelligence, and data science for continuous algorithmic improvement constitutes an immensely expensive, sophisticated, and exclusive twenty-first century "means of production." Third, the new manufacturing process converts behavioral surplus into *prediction products* designed to predict behavior now and soon. Fourth, these prediction products are sold into a new kind of meta-market that trades exclusively in future behavior. The better (more predictive) the product, the lower the risks for buyers, and the greater the volume of sales. Surveillance capitalism's profits derive primarily, if not entirely, from such *markets for future behavior*.

While advertisers have been the dominant buyers in the early history of this new kind of marketplace, there is no substantive reason why such markets should be limited to this group. The already visible trend is that any actor with an interest in monetizing

probabilistic information about our behavior and/or influencing future behavior can pay to play in a marketplace where the behavioral fortunes of individuals, groups, bodies, and things are told and sold. This is how in our own lifetimes we observe capitalism shifting under our gaze: once profits from products and services, then profits from speculation, and now profits from surveillance. This latest mutation may help explain why the explosion of the digital has failed, so far, to decisively impact economic growth, as so many of its capabilities are diverted into a fundamentally parasitic form of profit.

Unoriginal Sin

The significance of behavioral surplus was quickly camouflaged, both at Google and eventually throughout the Internet industry, with labels like "digital exhaust," "digital breadcrumbs," and so on. These euphemisms for behavioral surplus operate as ideological filters, in exactly the same way that the earliest maps of the North American continent labeled whole regions with terms like "heathens," "infidels," "idolaters," "primitives," "vassals," or "rebels." On the strength of those labels, native peoples, their places and claims, were erased from the invaders' moral and legal equations, legitimating their acts of taking and breaking in the name of Church and Monarchy.

We are the native peoples now whose tacit claims to self-determination have vanished from the maps of our own behavior. They are erased in an astonishing and audacious act of *dispossession by surveillance* that claims its right to ignore every boundary in its thirst for knowledge of and influence over the most detailed nuances of our behavior. For those who wondered about the logical completion of the global processes of commodification, the answer is that they complete themselves in the dispossession of our intimate quotidian reality, now reborn as behavior to be monitored and modified, bought and sold.

The process that began in cyberspace mirrors the nineteenth century capitalist expansions that preceded the age of imperialism. Back then, as Hannah Arendt described it in *The Origins of Totalitarianism*, "the so-called laws of capitalism were actually allowed to create realities" as they traveled to less developed regions

where law did not follow. "The secret of the new happy fulfillment," she wrote, "was precisely that economic laws no longer stood in the way of the greed of the owning classes." There, "money could finally beget money," without having to go "the long way of investment in production..."

"The original sin of simple robbery"

For Arendt, these foreign adventures of capital clarified an essential mechanism of capitalism. Marx had developed the idea of "primitive accumulation" as a big-bang theory—Arendt called it "the original sin of simple robbery"—in which the taking of lands and natural resources was the foundational event that enabled capital accumulation and the rise of the market system. The capitalist expansions of the 1860s and 1870s demonstrated, Arendt wrote, that this sort of original sin had to be repeated over and over, "lest the motor of capital accumulation suddenly die down."

In his book *The New Imperialism*, geographer and social theorist David Harvey built on this insight with his notion of "accumulation by dispossession." "What accumulation by dispossession does," he writes, "is to release a set of assets...at very low (and in some instances zero) cost. Overaccumulated capital can seize hold of such assets and immediately turn them to profitable use...It can also reflect attempts by determined entrepreneurs...to 'join the system' and seek the benefits of capital accumulation."

Breakthrough into "the system"

The process by which behavioral surplus led to the discovery of surveillance capitalism exemplifies this pattern. It is the foundational act of dispossession for a new logic of capitalism built on profits from surveillance that paved the way for Google to become a capitalist enterprise. Indeed, in 2002, Google's first profitable year, founder Sergey Brin relished his breakthrough into "the system," as he told Levy:

> *Honestly, when we were still in the dotcom boom days, I felt like a schmuck. I had an Internet start-up—so did everybody else. It was unprofitable, like everybody else's, and how hard is that? But when we became profitable, I felt like we had built a real business.*

Brin was a capitalist all right, but it was a mutation of capitalism unlike anything the world had seen.

Once we understand this equation, it becomes clear that demanding privacy from surveillance capitalists or lobbying for an end to commercial surveillance on the Internet is like asking Henry Ford to make each Model T by hand. It's like asking a giraffe to shorten its neck or a cow to give up chewing. Such demands are existential threats that violate the basic mechanisms of the entity's survival. How can we expect companies whose economic existence depends upon behavioral surplus to cease capturing behavioral data voluntarily? It's like asking for suicide.

More behavioral surplus for Google

The imperatives of surveillance capitalism mean that there must always be more behavioral surplus for Google and others to turn into surveillance assets, master as prediction, sell into exclusive markets for future behavior, and transform into capital. At Google and its new holding company called Alphabet, for example, every operation and investment aims to increasing the harvest of behavioral surplus from people, bodies, things, processes, and places in both the virtual and the real world. This is how a sixty-seven hour day dawns and darkens in an emerald sky. Nothing short of a social revolt that revokes collective agreement to the practices associated with the dispossession of behavior will alter surveillance capitalism's claim to manifest data destiny.

What is the new vaccine? We need to reimagine how to intervene in the specific mechanisms that produce surveillance profits and in so doing reassert the primacy of the liberal order in the 21st century capitalist project. In undertaking this challenge we must be mindful that contesting Google, or any other surveillance capitalist, on the grounds of monopoly is a 20th century solution to a 20th century problem that, while still vitally important, does not necessarily disrupt surveillance capitalism's commercial equation. We need new interventions that interrupt, outlaw, or regulate 1) the initial capture of behavioral surplus, 2) the use of behavioral surplus as free raw material, 3) excessive and exclusive concentrations of the new means of production, 4) the

manufacture of prediction products, 5) the sale of prediction products, 6) the use of prediction products for third- order operations of modification, influence, and control, and 5) the monetization of the results of these operations. This is necessary for society, for people, for the future, and it is also necessary to restore the healthy evolution of capitalism itself.

A coup from above

In the conventional narrative of the privacy threat, institutional secrecy has grown, and individual privacy rights have been eroded. But that framing is misleading, because privacy and secrecy are not opposites but rather moments in a sequence. Secrecy is an effect; privacy is the cause. Exercising one's right to privacy produces choice, and one can choose to keep something secret or to share it. Privacy rights thus confer decision rights, but these decision rights are merely the lid on the Pandora's Box of the liberal order. Inside the box, political and economic sovereignty meet and mingle with even deeper and subtler causes: the idea of the individual, the emergence of the self, the felt experience of free will.

Surveillance capitalism does not erode these decision rights—along with their causes and their effects—but rather it redistributes them. Instead of many people having some rights, these rights have been concentrated within the surveillance regime, opening up an entirely new dimension of social inequality. The full implications of this development have preoccupied me for many years now, and with each day my sense of danger intensifies. The space of this essay does not allow me to follow these facts to their conclusions, but I offer this thought in summary.

Surveillance capitalism reaches beyond the conventional institutional terrain of the private firm. It accumulates not only surveillance assets and capital, but also rights. This unilateral redistribution of rights sustains a privately administered compliance regime of rewards and punishments that is largely free from detection or sanction. It operates without meaningful mechanisms of consent either in the traditional form of "exit, voice, or loyalty" associated with markets or in the form of democratic oversight expressed in law and regulation.

Profoundly anti-democratic power

In result, surveillance capitalism conjures a profoundly anti-democratic power that qualifies as a coup from above: not a coup d'état, but rather a *coup des gens*, an overthrow of the people's sovereignty. It challenges principles and practices of self-determination—in psychic life and social relations, politics and governance—for which humanity has suffered long and sacrificed much. For this reason alone, such principles should not be forfeit to the unilateral pursuit of a disfigured capitalism. Worse still would be their forfeit to our own ignorance, learned helplessness, inattention, inconvenience, habituation, or drift. This, I believe, is the ground on which our contests for the future will be fought.

Hannah Arendt once observed that indignation is the natural human response to that which degrades human dignity. Referring to her work on the origins of totalitarianism she wrote, "If I describe these conditions without permitting my indignation to interfere, then I have lifted this particular phenomenon out of its context in human society and have thereby robbed it of part of its nature, deprived it of one of its important inherent qualities."

So it is for me and perhaps for you: The bare facts of surveillance capitalism necessarily arouse my indignation because they demean human dignity. The future of this narrative will depend upon the indignant scholars and journalists drawn to this frontier project, indignant elected officials and policy makers who understand that their authority originates in the foundational values of democratic communities, and indignant citizens who act in the knowledge that effectiveness without autonomy is not effective, dependency-induced compliance is no social contract, and freedom from uncertainty is no freedom.

Big Data's Hidden Labor

by Evan Malmgren

From Jacobin *March 14, 2017*

Who owns your data? We are used to signing the question away in unread terms of service agreements, but it has increasingly become a matter of livelihood. Shipping companies like UPS and Amazon micromanage their workers with advanced surveillance networks, while international retailers and fast-food chains now generate employee schedules with complex, data-fed efficiency algorithms. Monsanto "smart farm" technologies extract valuable insights from independent farmers en masse, and Uber drivers may even help develop their own self-driving replacements by building driving databases of unprecedented size and detail.

Capitalists have long collected profitable data from their workers without compensation, but only more recently has the proliferation of networked smart technologies—"the internet of things"—extended this surveillance beyond the workplace, adding a dimension of unwaged value-creation to our personal lives. Digital retailers profile us to give targeted recommendations; streaming services learn our tastes to predict what content we will enjoy; and fitness apps track our calories and steps to help us make

"healthier" decisions. Soon, VR headsets may even be tracking minute eye movements and spontaneous retinal activity.

These technologies usually feed our personal information back to private companies, where insights about our shopping habits, interests, and bodily functions reap huge profits. Big data can't exist without our input, and the analytics market wouldn't have grown to a $130 billion dollar industry without wide-scale cooperation. Just as passive data collection adds new layers of invisible labor to the "smart farmer's" workday, it increasingly transforms our leisure time into productive work.

Enclosing the Commons

When Google's PageRank algorithm started trawling the web back in 1996, Larry Page and Sergey Brin had unwittingly begun a process that would turn the information pipeline on its head. Sorting an ever- expanding cache of URLs by link density and user engagement statistics, the Stanford PhD students eventually developed an algorithm that has outsourced their search engine to its clientele, the customers of a free service. Users strengthen the algorithm simply by searching the web, thus attracting more consumers to the improved product, and in turn generating a larger base to further hone the engine.

An ideal form of the neoclassical economist's "virtuous cycle," this process is one of the first clear examples of consumer-driven big data. It was innovative because it collapsed an act of mass production—the creation of useful data—into one of mass consumption, eventually driving search competitors like AltaVista, Hotbot, and WebCrawler (as well as overcrowded web portals like MSN, AOL, and Lycos) into obscurity on the back of a hidden labor force.

Few know that in late 2001, Google was quietly considering a shift from this "virtuous cycle," testing a voting system that would allow users to transparently impact the ranking of their search results. SiteLab co-founder Dana Todd called the more engaged approach "user aware," but the transparent feature never hit the market. As Google discovered, mass data harvesting operates best in a concealed and indirect manner.

An active, straightforward exchange—as with a questionnaire or customer service survey, for instance—reveals the labor involved in feeding a magical algorithm. Instead of opting for active solicitation, Google has intensified its passive data collection, expanding its reach to include your movements through physical space (Google Maps), anticipated futures (Google Calendar), and metrics on everyday internet usage (Google Chrome). These accumulated data sets are all extensions of what the company's privacy page refers to as the "things that make you 'you.'"

These hidden exchanges quickly became central not only to Google's but also Amazon's business model. The leviathan internet retailer began to monetize personal user data around the same time as Google, using a vast set of individual purchase histories to feed algorithms that built item-item similarity indexes and consumer profiling tools as early as 2003. The company quickly established itself as a pioneer in targeted online advertising, leveraging metadata as a complex recommendation system. It appeared that Amazon had automated the job of a helpful retail clerk, but in reality, the company had merely hoisted the clerk's labor onto the consumers themselves, to be carried out within the act of consumption.

At first glance, it might seem that this model perfectly echoes film critic Annette Michelson's 1979 adage that, in the age of television advertising, "You are the end product delivered en masse to the advertiser." But the internet's data economy has proved a bit more complex: Google and Amazon had begun to embrace consumer data just as other early-internet titans were struggling to monetize their popularity. At the time, advertisers were wary of the web, which lacked television's captive audience, and showed a poor rate of return on converting attention into profit. Google and Amazon sidestepped the problem by congealing their global markets into a workforce. While Google relied on user inputs to build a dominant product, Amazon turned their customers into a massive personalized marketing team. Both turned user data into a valuable commodity in its own right.

Thus, in an amendment to Michelson's adage, in the age of digital communications, your *data*—rather than you yourself—is the

product delivered en masse. In repurposing consumer engagement as tangible goods and services, Amazon and Google demonstrated that freely extracted personal data could be turned for a profit. It is no coincidence that these companies easily weathered the burst of the dot-com bubble, or that their models have all but defined the "Internet 2.0" generation that followed.

Of the sleeker, smartphone-enabled internet companies that rose from the ashes of the dotcom crash, Facebook burns brightest. Envisioned as a monetized user database from the outset, Mark Zuckerberg's social network cycled through a slew of design changes before settling on a site layout that compelled its users to divulge the maximum quantity of personal information. As we check the website's boxes, complete its forms, and play in its sandbox of likes, posts, and reactions, algorithms sift through our online selves and apply predictive analytics to divine our politics, income brackets, and opaque personal interests.

These detailed profiles are packaged and sold to advertisers en masse, without remittance for the consumer-producers whose labor imbues them with value. With an annual revenue stream reported in excess of $27 billion at the end of 2016, Facebook has ballooned into one of the world's largest internet companies, topped only by Amazon and Google, whose 2016 revenues were reported around $136 and $90 billion respectively.

These companies have built an industry of assembling and marketing comprehensive metadata—interlinking chains of minor details that become more valuable as they grow in complexity. Edward Snowden usefully explained the power of metadata in a 2015 livestream:

> *Metadata is very much like what a private eye does when they follow someone around. They're not even close enough to you, when they're sitting behind you in a café, to get every word that you're saying in a whispered conversation. But they're going to know where you were, they're going to know who you met with, they're going to know when you did it, they're going to know how you left, they're going to know where you went. And when you get this*

in aggregate, you tell the full story of someone's life.

Facebook doesn't just know your relationship status, the things you "like," and where you took your profile pictures—they also tether this information to anything you do on an external app accessed through a Facebook login, or any webpage that you access from there. This allows them to associate your Tinder swipes with your Venmo transactions; your Uber rides with your Instagram followers; your Seamless orders with your preferred news sources and how you access them. Likewise for Google: if you have Google Maps installed on your smartphone, the tech giant can process all of your movements alongside your search history, newsletter subscriptions, favorite YouTube videos, and anything you do on a web page with a Google+ button.

Of course, it would be impossible to strain useful patterns from this overwhelming noise without an extensive material infrastructure. For this reason, big data has been referred to as the new oil: it is worthless in its raw form, but grows to a fortune with proper refinement.

To give a sense of the capital accumulation undergirding this extraction of data-wealth: Twitter leases around a fifth of a 990,000 square-foot data center in Atlanta, where it stores over five hundred petabytes of data, and processes, caches, and analyzes over half a million tweets per day; Facebook's seven data centers range from 160,000 to 487,000 square feet in size, with the company claiming an excess of $3.6 billion in "networking equipment" at the end of 2015; and Google spends more than $5 billion per quarter on its sixteen massive data centers, located on four continents and housing over a million servers. These colossal entry barriers mean that newcomers are unable to compete with established big data companies, and cannot similarly extract surplus value from user engagement with free services. As a result, a handful of tech giants enjoy near-monopolistic control of our bulk metadata.

Despite a small concentration of ownership, the ability to process large volumes of personal information has still resulted in some benefits for individuals and society at large. Google prioritizes news stories that I genuinely find interesting,

Ticketmaster sends me custom event notifications based on artists that I follow on SoundCloud, and I always notice the sponsored posts announcing holiday sales by certain socialist magazines. On a macro scale, big data has positive implications for urban planners who want to design smarter cities, health-care professionals who want to predict epidemics and cure diseases, and engineers who want to identify or even predict new problems to solve.

And yet, we cannot forget that big data's developments are ultimately enabled by us—the creators of its constituent bits—and not by magical processing centers alone. The average Facebook user was worth roughly fifteen dollars per year at the start of 2016; for Google, that figure was around thirty-three dollars. These may seem like small numbers, but they become massive when multiplied across a vast consumer base, and will only continue to grow as analytic firms and machine learning technologies improve their capacity to process raw information into profitable insights.

Anyone would expect reimbursement for participating in an inpatient study, or for sitting on a consumer panel at a product testing. Now that we provide these kinds of data services remotely, the only distinction is a greater degree of alienation. We don't expect payment for our data simply because its creation is not considered to be "work."

In Search of Alternatives

Labor should be understood—and compensated—in terms of value creation, and not a degree of compulsion. People may be willing to engage in value-creating activities of their own volition, but that doesn't mean that we should allow this newly possible wealth to pool in the hands of a relatively small group of developers and tech executives. If we fail to recognize big data as a society-wide project, we risk squandering an incredible technical achievement: the ability to convert leisure time into material utility.

This advancement does not necessarily signal a move towards a post-work society, but one in which labor is increasingly embedded in voluntary and even enjoyable activities. This unification of work and play is central to Marx's utopian vision, outlined in *Critique of the Gotha Programme*, of

a society in which "labor has become not only a means of life but life's prime want."

Utopian socialists like Charles Fourier once envisioned a future society in which productive work would take the form of personal enjoyment and creative fulfillment, even straying into territories of outlandish extravagance. We are unlikely to fully escape the necessity of life's occasional drudgery, or to arrive at anything resembling Fourier's Phalanstère, but there is no reason to reject the possibility of realizing this vision in a limited or partial form.

If we can assert a right to personal data ownership, one can imagine a future in which wages are increased to compensate for information collected from existing labor, and the workday is shortened thanks to additional value gleaned from idle time. Big data has already added a productive element to many acts of consumption, and to many things that we already do on a regular basis. If we are to realize the full social potential of big data, the necessary political task is to demand recognition of the hidden labor involved in its construction.

The Big Data Era of Mosaicked Deidentification

by Kalev Leetaru

From Forbes *August 24, 2016*

The era of "big data" has brought with it an incredible wealth of massive new datasets cataloging global society. Making possible this deluge of publicly accessible data is the concept of anonymization, in which datasets are purged of personally identifying information. In this way, archives of web searches, cell phone records, credit card receipts and medical records can all be released to the world to enable incredible new research. Yet, as these datasets have proliferated, so too has research demonstrating that even the most carefully anonymized datasets can be deidentified with relative ease. Perhaps most famously, Latanya Sweeney demonstrated in 2000 that 87% of the American population can be uniquely identified by a combination of just their ZIP code, gender and date of birth. Even if all other details are removed from a dataset, having just these three pieces of information (or being able to recover them by merging with another dataset) is enough to reidentify that person.

Yet it was six years later that the concept of anonymized data truly burst onto the international stage when AOL released a massive anonymized search dataset which contained

21 million searches conducted by 650,000 of its users. Each user was assigned a random numeric identifier which AOL Research thought was sufficient to mask the identities of its users. Yet, it quickly became readily apparent through the archive just how much personal information people give away when they search on the web. From vanity searches on one's name to checking the local weather to searches for parts for a particular automobile to how to treat a particular medical condition, just knowing the set of searches performed by a particular person can be used to fairly quickly reidentify that person.

The Netflix Prize Dataset was famously deanonymized by cross-referencing it against the Internet Movie Database, the Massachusetts Governor's medical records were identified by combining the Massachusetts Group Insurance Commission dataset against voter registration data, genomic datasets have been deanonymized, credit card data can be deanonymized at 90% accuracy using just three purchases and even an anonymized dataset of a year's worth of cell phone records of 1.5 million subscribers can be rapidly reidentified using just four reference points.

In some cases, poor anonymization design leads to critical flaws. When New York City released its now-famous taxi database, it "anonymized" the dataset by MD5 hashing the hack license and medallion numbers of each driver. In actuality, this did not anonymize the dataset since MD5 is merely a deterministic encoding and given the limited universe of possible values a researcher was able to rapidly reidentify the entire dataset.

Combining this data with Google Images searches for photographs of "celebrities in taxis in Manhattan in 2013" grad student Anthony Tockar was able to take the medallion number that is typically clearly visible in such photographs and the pickup location and time and cross-reference it against the taxi database to identify celebrity destinations and how much they paid and tipped for each fare.

The careful reader will notice a common theme among each of these situations: combining multiple innocuous datasets together to fill in each's holes. Put another way, each dataset on its own yields limited

information, but when combined with other public datasets in unexpected ways, the missing blanks can be filled in.

This concept of combing datasets to fill in the blanks is known as "mosaicking" and in fact it turns out that it works equally well for declassified US Government documents. Several years ago I worked with a team at Columbia University on new approaches to visualizing and mining the vast troves of declassified documents available in digital form today. One of the team's projects was called the "Declassification Engine" and focused on how mosaicking can turn the very human process of declassification against itself to estimate or even completely recover the blacked out redacted sections that inevitably mask portions of many declassified materials.

It turns out there is no single central declassification agency in the US Government. When a given agency decides to declassify a document, its own declassification staff review the document and identify any passages they deem still sensitive and the document is then released with those passages blacked out. However, documents are frequently authored by multiple agencies, each of which may decide to declassify the document. In such cases one agency might decide to redact the first paragraph and release the rest, while another agency might redact the last paragraph and release the rest. By pooling every declassified document released over time from every US agency, one can identify duplicate declassifications and merge them together, in some cases restoring portions of the redacted text. In other cases one can look at the text immediately surrounding the redacted passage and identify highly similar contexts from other documents and from news coverage of the time to estimate the likely redacted text.

Indeed, while there are a number of potentially stronger anonymization approaches being explored such as differential privacy, a growing chorus of concern is emerging about the state of anonymization today and the approaches most commonly used at the moment. Yet most worryingly, many of the government agencies I've interacted with here in DC have little understanding of data privacy and many of the government data scientists I've been in meetings with

have dismissed such concerns as overblown. Despite the wealth of case examples showing the severe limitations of current anonymization approaches, many in the data science community I've met still cling to the belief that just replacing usernames with random numbers somehow magically secures a dataset against any possible reidentification. As more and more organizations begin to release sensitive datasets to the public, the data science community must spend more time thinking about how to safely and responsibility manage this flow of anonymized data that is the lifeblood of the big data era.

Google now knows when its users go to the store and buy stuff

by Elizabeth Dwoskin and Craig Timberg
From The Washington Post *May 23, 2017*

Google has begun using billions of credit-card transaction records to prove that its online ads are prompting people to make purchases—even when they happen offline in brick-and-mortar stores, the company said Tuesday.

The advance allows Google to determine how many sales have been generated by digital ad campaigns, a goal that industry insiders have long described as "the holy grail" of online advertising. But the announcement also renewed long-standing privacy complaints about how the company uses personal information.

To power its multibillion-dollar advertising juggernaut, Google already analyzes users' Web browsing, search history and geographic locations, using data from popular Google-owned apps like YouTube, Gmail, Google Maps and the Google Play store. All that information is tied to the real identities of users when they log into Google's services.

The new credit-card data enables the tech giant to connect these digital trails to real-world purchase records in a far more extensive way than was possible before. But in doing so, Google is yet again treading in ter-

ritory that consumers may consider too intimate and potentially sensitive. Privacy advocates said few people understand that their purchases are being analyzed in this way and could feel uneasy, despite assurances from Google that it has taken steps to protect the personal information of its users.

Google also declined to detail how the new system works or what companies are analyzing records of credit and debit cards on Google's behalf. Google, which saw $79 billion in revenue last year, said it would not handle the records directly but that its undisclosed partner companies had access to 70 percent of transactions for credit and debit cards in the United States.

"What's really fascinating to me is that as the companies become increasingly intrusive in terms of their data collection, they also become more secretive," said Marc Rotenberg, executive director of the Electronic Privacy Information Center. He urged government regulators and Congress to demand answers about how Google and other technology companies are collecting and using data from their users.

Google said it took pains to protect to protect user privacy.

"While we developed the concept for this product years ago, it required years of effort to develop a solution that could meet our stringent user privacy requirements," Google said in a statement. "To accomplish this, we developed a new, custom encryption technology that ensures users' data remains private, secure, and anonymous."

The announcement comes as Google attempts to weather an outcry from advertisers over how their ad dollars are spent. Google is working to move past an advertising boycott of YouTube, its lucrative video site, after news reports that ads for mainstream brands were appearing alongside extremist content, including sites featuring hate speech and violence.

Google for years has been mining location data from Google Maps in an effort to prove that knowledge of people's physical locations could "close the loop" between physical and digital worlds. Users can block this by adjusting the settings on smartphones, but few do so, say privacy experts.

This location tracking ability has allowed Google to send reports to retailers telling them, for example, whether people who saw an ad for a lawn mower later visited or passed by a Home Depot. The location-tracking program has grown since it was first launched with only a handful of retailers. Home Depot, Express, Nissan, and Sephora have participated.

"Google—and also Facebook—believe that in order to get digital dollars from advertisers who are still primarily spending on TV, they need to prove that digital works," said Amit Jain, chief executive of Bridg, a digital advertising start-up that matches online to offline behavior. "These companies have to invest in finding the identity of the consumer at the moment when that shopper is at the cash register."

Tuesday's announcement gives Google a clearer way to understand purchases than just location and allows them to understand purchase activity even when consumers deactivate location tracking on their smartphones.

Google executives say they are using complex, patent-pending mathematical formulas to protect the privacy of consumers when they match a Google user with a shopper who makes a purchase in a brick-and-mortar store.

The mathematical formulas convert people's names and other purchase information, including the time stamp, location, and the amount of the purchase, into anonymous strings of numbers. The formulas make it impossible for Google to know the identity of the real-world shoppers, and for the retailers to know the identities of Google's users, said company executives, who called the process "double-blind" encryption.

The companies know only that a certain number of matches have been made. In addition, Google does not know what products people bought.

"Through a mathematical property we can do double-blind matching between their data and our data," said Jerry Dischler, vice president of product management for AdWords, Google's online advertising service, in an interview. "Neither gets to the see the encrypted data that the other side brings."

The tech giant declined to describe its mathematical formulas in anything more than broad terms, citing a pending patent. Dischler said the work was based on a 2011 research paper by three MIT scientists, which was funded by Google and Citigroup.

Dischler described the modeling as a "revolutionary" step forward for both Google and advertisers. He added that users who signed into Google's services had consented to Google sharing their data with third parties.

But the company would not say how merchants had obtained consent from consumers to pass along their credit-card information. Google said it requires its partners to use only personal data that they have the "rights" to use, but it would not say whether that meant the consumers had consented.

In the past, both Google and Facebook have obtained purchase data for a more limited set of consumers who participate in store loyalty programs. Those consumers are more heavily tracked by retailers, and often give consent to share their data with third parties as a condition of signing up.

Tuesday's initiative enables Google to use transaction data from a much wider swath of consumers than ever before, but the lack of detail on how personal data was being handled caused concern for privacy advocates.

Paul Stephens, of Privacy Rights Clearinghouse, a consumer advocacy group based in San Diego, said only a few pieces of data can allow a marketer to identify an individual, and he expressed skepticism that Google's system for guarding the identities of users will stand up to the efforts of hackers, who in the past have successfully stripped away privacy protections created by other companies after data breaches.

"What we have learned is that it's extremely difficult to anonymize data," he said. "If you care about your privacy, you definitely need to be concerned."

Such data providers have been the targets of cybercriminals in the past. In 2015, a hack of data broker Experian exposed the personal information of 15 million people.

How Privacy Became a Commodity for the Rich and Powerful

by Amanda Hess
From The New York Times *May 9, 2017*

Recently I handed over the keys to my email account to a service that promised to turn my spam-bloated inbox into a sparkling model of efficiency in just a few clicks. Unroll.me's method of instant unsubscribing from newsletters and junk mail was "trusted by millions of happy users," the site said, among them the "Scandal" actor Joshua Malina, who tweeted in 2014: "Your inbox will sing!" Plus, it was free. When a privacy policy popped up, I swatted away the legalese and tapped "continue."

Last month, the true cost of Unroll.me was revealed: The service is owned by the market-research firm Slice Intelligence, and according to a report in *The Times*, while Unroll.me is cleaning up users' inboxes, it's also rifling through their trash. When Slice found digital ride receipts from Lyft in some users' accounts, it sold the anonymized data off to Lyft's ride-hailing rival, Uber.

Suddenly, some of Unroll.me's trusting users were no longer so happy. One user filed a class-action lawsuit. In a blog post, Unroll.me's chief executive, Jojo Hedaya, wrote that it was "heartbreaking to see that some of our users were upset to learn about

how we monetize our free service." He stressed "the importance of your privacy" and pledged to "do better." But one of Unroll.me's founders, Perri Chase, who is no longer with the company, took a different approach in her own post on the controversy. "Do you really care?" she wrote. "How exactly is this shocking?"

This Silicon Valley "good cop, bad cop" routine is familiar, and we spend our time surfing between these two modes of thought. Chase is right: We've come to understand that privacy is the currency of our online lives, paying for petty conveniences with bits of personal information. But we are blissfully ignorant of what that means. We don't know what data is being bought and sold, because, well, that's private. The evidence that flashes in front of our own eyes looks harmless enough: We search Google for a new pair of shoes, and for a time, sneakers follow us across the web, tempting us from every sidebar. But our information can also be used for matters of great public significance, in ways we're barely capable of imagining.

When I signed up for Unroll.me, I couldn't predict that my emails might be strategic documents for a power-hungry company in its quest for total road domination. Such privacy costs often become clear only after they've already been paid. Sometimes a private citizen is caught up in a viral moment and learns that a great deal of information about him or her exists online, just waiting to be splashed across the news—like the guy in the red sweater who, after asking a question in a presidential debate, had his Reddit porn comments revealed.

But our digital dossiers extend well beyond the individual pieces of information we know are online somewhere; they now include stuff about us that can be surmised only through studying our patterns of behavior. The psychologist and data scientist Michal Kosinski has found that seemingly mundane activity—like the brands and celebrities people "like" on Facebook—can be leveraged to reliably predict, among other things, intelligence, personality traits and politics. After our most recent presidential election, the company Cambridge Analytica boasted that its techniques were "instrumental in identifying supporters, persuading undecided voters and driving turn-

out to the polls" on Donald Trump's behalf. All these little actions we think of as our "private" business are actually data points that can be aggregated and wielded to manipulate our world.

Years ago, in 2009, the law professor Paul Ohm warned that the growing dominance of Big Data could create a "database of ruin" that would someday connect all people to compromising information about their lives. "In the absence of intervention," he later wrote, "soon companies will know things about us that we do not even know about ourselves." Or as the social scientist and *Times* contributor Zeynep Tufekci said in a recent talk: "People can't think like this: I didn't disclose it, but it can be inferred about me." When a peeping Tom looks between the blinds, it's clear what has been revealed. But when a data firm cracks open our inboxes, we may never find out what it has learned.

Privacy has not always been seen as an asset. The ancient Greeks, for instance, distinguished between the public realm ("*koinon*") and the private realm ("*idion*"). In contrast to those public citizens engaged in political life, humble private citizens were known as "*idiotai*," a word that later evolved into "idiots." Something similar is true of the English word "privacy." As Hannah Arendt wrote in *The Human Condition*, privacy was once closely associated with "a state of being deprived of something, and even of the highest and most human of man's capacities." In the 17th century, the word "private" arose as a more politically correct replacement for "common," which had taken on condescending overtones.

And yet somewhere along the way, privacy was recast as a necessity for cultivating the life of the mind. In George Orwell's *1984*, the proles are spared a life of constant surveillance, while higher-ranking members of society are exposed to Big Brother's watchful eye. The novel's protagonist, Winston, begins to suspect that real freedom lies in those unwatched slums: "If there is hope," he writes in his secret diary, "it lies in the proles." In the influential 1967 book *Privacy and Freedom*, Alan Westin described privacy as having four functions: personal autonomy, emotional release, self-evaluation and intimate communication. This modern understanding of privacy as an

intimate good grew up right alongside the technology that threatened to violate it. At the end of the 18th century, the Fourth Amendment to the United States Constitution protected Americans from physical searches of their bodies and homes. One hundred years later, technological advancements had legal minds thinking about a kind of mental privacy too: In an 1890 paper called "The Right to Privacy," Samuel Warren and Louis Brandeis cited "recent inventions and business methods"—including instant photography and tabloid gossip—that they claimed had "invaded the sacred precincts of private and domestic life." They argued for what they called the right "to be let alone," but also what they called "the right to one's personality."

Now that our privacy is worth something, every side of it is being monetized. We can either trade it for cheap services or shell out cash to protect it. It is increasingly seen not as a right but as a luxury good. When Congress recently voted to allow internet service providers to sell user data without users' explicit consent, talk emerged of premium products that people could pay for to protect their browsing habits from sale. And if they couldn't afford it? As one congressman told a concerned constituent, "Nobody's got to use the internet." Practically, though, everybody's got to. Tech companies have laid claim to the public square: All of a sudden, we use Facebook to support candidates, organize protests and pose questions in debates. We're essentially paying a data tax for participating in democracy.

The smartphone is an intimate device; we stare rapt into its bright light and stroke its smooth glass to coax out information and connect with others. It seems designed to help us achieve Westin's functions of privacy, to enable emotional release and moments of passive reflection. We cradle it in bed, at dinner, on the toilet. Its pop-up privacy policies are annoying speed bumps in the otherwise instantaneous conjuring of desires. It feels like a private experience, when really it is everything but. How often have you shielded the contents of your screen from a stranger on the subway, or the partner next to you in bed, only to offer up your secrets to the data firm tracking everything you do?

The surveillance economy works on

such information asymmetry: Data-mining companies know everything about us, but we know very little about what they know. And just as "privacy" has grown into an anxious buzzword, the powerful have co-opted it in order to maintain control over others and evade accountability. As we bargain away the amount of privacy that an ordinary person expects, we've also watched businesses and government figures grow ever more indignant about their own need to be left alone. Companies mandate nondisclosure agreements and demand out-of-court arbitration to better conceal their business practices. In 2013, Facebook revoked users' ability to remain unsearchable on the site; meanwhile, its chief executive, Mark Zuckerberg, was buying up four houses surrounding his Palo Alto home to preserve his own privacy. Sean Spicer, the White House press secretary, has defended President Trump's secretive meetings at his personal golf clubs, saying he is "entitled to a bit of privacy," and the administration has cut off public access to White House visitor logs, citing security risks and "privacy concerns." When *The New York Times* reported that the president takes counsel from the Fox News host Sean Hannity, Hannity indignantly tweeted that his conversations were "PRIVATE."

We've arrived at a place where public institutions and figures can be precious about their privacy in ways we're continually deciding individual people can't. Stepping into the White House is now considered more private than that weird rash you Googled. It's a cynical inversion of the old association between private life and the lower class: These days, only the powerful can demand privacy.

Capitalism vs. Privacy

by Samuel Earle
From Jacobin *April 3, 2017*

In the popular discourse, authoritarianism typically stands as liberal capitalism's dramatic antithesis. And nowhere are their purported differences more stark than in their attitudes toward individual privacy. While in the liberal capitalist world every person's home is said to be their castle, in authoritarian regimes, it is just one more state-monitored cage.

Today, however, privacy is disappearing within the walls of advanced capitalist democracies. And multinational corporations, holding aloft the banner of total transparency, are the ones leading the charge.

In 1999, Scott McNealy, then-CEO of Sun Microsystems, famously declared, "You have zero privacy now anyway. Get over it." Google CEO Eric Schmidt warned that "if you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place." Mark Zuckerberg, the world's sixth richest man, decided that privacy was no longer a social norm, "and so we just went for it," while Alexander Nix, of the data firm Cambridge Analytica—famously employed by both the Brexit and Trump campaigns—brags that his company "profiled the personality of every single adult in the United States of America."

These days, the rhetoric of private capitalists seems indistinguishable from the rhetoric of state tyrants. Their scripts are all mixed up. Their differences have always been exaggerated, if not imagined, but we could once rely on them to at least speak differently. What's changed?

The Evaporating Bond

As an economic system founded on the idea of a private sphere—consisting of private individuals who own private property and make private profit in private markets—capitalism is assumed to protect individual privacy. The sanctity of the private realm allegedly ensures maximum freedom for the individual, as producers and consumers are liberated from unwanted interference from the state and nosy neighbors.

Capitalism's detractors have long decried its tendency to hollow out the commons and push everyone into their private bubbles, but its supporters celebrate this atomization. "Civilization," wrote Ayn Rand in 1943, "is the progress toward a society of privacy. The savage's whole existence is public, ruled by the laws of his tribe. Civilization is the process of setting man free from men." From this perspective, capitalism's emphasis on the private sphere and the resultant privacy made it the world's great civilizer.

As early as the 1970s, however, the bond between capitalism and individual privacy was becoming unstuck. In 1977, the right-wing legal jurist Richard Posner put forward his "economic theory of privacy," eventually publishing it in a paper in, aptly, 1984. There, he argued that individual privacy hindered capitalism by interrupting the free flow of information that markets need to be efficient. Posner concluded that "people should not—on economic grounds in any event—have a right to conceal material facts about themselves."

Posner was writing for *Chicago Unbound*, the law journal at the University of Chicago, the epicenter of the neoliberal storm that was spreading across the world. Milton Friedman was one of Posner's closest colleagues, and Posner himself is often included under the Chicago School umbrella. Posner's capitalist roots—with their endless exaltation of the private individual—made his arguments against individual privacy all the more surprising. The love

affair between privacy and capitalism, long taken for granted by dove-eyed liberals, was revealed to be the shallowest of relationships: a marriage of convenience that was no longer convenient.

In the digital age, this relationship has become all the more fractious. A new form of capitalism has emerged on the Internet, variously referred to as informational capitalism, digital capitalism, or surveillance capitalism. Personal information is the lifeblood of the new economy: companies collect their users' data to sell it to advertisers and generate revenue. The more companies know about individuals, the better they can target their advertisements, boost their "conversion rates," and rake in profits.

And make no mistake, there's a lot of money to be made. In the third quarter of 2016, a total of $17.6 billion was spent on digital advertising, a 20 percent rise from the previous year.

Facebook and Google have become a duopoly in this new context, accounting for about half of the total; of the $2.9 billion in growth over the last year, the pair was responsible for a remarkable 99 percent of it. In the process, they have become the two fastest growing corporations in the history of capitalism, with an ability to collect, monitor, and sell data on users in ways other companies can only imagine. Their collective net worth is $800 billion, more than the total GDP of the Netherlands.

Both their business models show that, in informational capitalism, privacy no longer impedes profit: privacy prevents profit. The belief that individuals should be allowed to control their personal information now contradicts capitalism's profit-making process. Far from sheltering private individuals from external interference, as Ayn Rand imagined, companies now want to know individuals as well as they know themselves. Corporations strive for perfect transparency, so that, in the words of Google's chief economist, Hal Varian, the search engine will "know what you want and tell it to you before you ask the question."

We might take solace in the fact that these companies don't carry the force of the state—that if their intention is to target advertisements more effectively and sell data more profitably, it

also might redound to the benefit of the user.

Many people enjoy using a service that knows them well and recognizes their personal habits, preferences, and interests. The quality of their experience increases with the amount of personal information they turn over—and who doesn't want better services?

But dangers do exist. Although much of the data that tech firms collect is frivolous, we should be wary of the aggregation effect: taken individually, each piece seems innocuous; taken together, an intimate picture of our person is revealed.

Yet even this does not get at the heart of the problem. The greatest threat lies not so much in *what* corporations know as in *how* they use that knowledge. The services they offer are entrancing, replete with conveniences and new possibilities, tailored to our every need. But when we cede so much personal information to corporations, we grant them incredible power and responsibility. Knowledge may mean power, but information often means domination.

And since the first large-scale data collection efforts in the nineteenth century, companies have been using technology to exert massive social control.

The Hollerith Machine

In 1880, with a rising population, an expanding territory, and a deepening desire for statistics—combined with a complete lack of technological strategy—the data collected by the United States Census took most of a decade to process. By the time the next census rolled around, in 1890, the processing time had been reduced to three months.

A young American engineer, Herman Hollerith, invented the system that enabled this incredible speed-up. Inspired by train conductors, he used punch cards to automatically tabulate information on a set of standardized traits, from race and gender to literacy levels and religion, across the entire population. The Hollerith Machine, as it came to be known, is now recognized as the first information system that successfully replaced pen and paper. Countries all over the world used it to collect data on their citizens

.

In 1911, Hollerith sold his company and the rights to his machine in a merger, forming what is now known as the International Business Machines Corporation (IBM). Under the leadership of Thomas J. Watson, a man revered as the "world's greatest salesman," IBM would own 90 percent of all tabulating machines in the United States. They sent them wherever the money called.

During the 1930s, it called from Adolf Hitler's Third Reich. Under the direction of IBM's German subsidiary, the Hollerith Machine located Jews and facilitated their "processing." The infamous numbers tattooed on the arms of prisoners were IBM identification numbers, matched to their individual place in IBM's punch-card system. The Nazis rewarded Watson for his services in 1937 with the prestigious Order of the Golden Eagle. Although he returned the award in 1940, his company continued to assist Germany throughout the war.

IBM didn't support the Nazis; it simply didn't care. In the same period, it completed a similar project for the United States: rounding up Japanese Americans—more than one hundred thousand of them—for the internment camps on the East Coast.

IBM's nefarious collaborations during World War II may represent an extreme case, but it would be naïve to dismiss them as immaterial. In fact, the company's actions embody a very banal truth: corporations and states regularly have shared interests and work together for mutual gain.

This happens regardless of moral principles. After all, capitalism coexists just as happily with dictatorships (Chile under Pinochet or today's China) as it does with democracies. The capitalist, guided by the great entrepreneurial spirit, sees every new setting as a new set of opportunities. The only question that remains is who is ready to exploit it.

Big Brother's New Clothes

Edward Snowden's mass leak of NSA files in 2013 revealed the active role corporations play in state surveillance. He reported a complete "blurring of public and private boundaries in surveillance activities" with "collaborations and constructive interdependencies between state security authorities and high tech firms."

Facebook, Google, and other websites

had become the government's new CCTV cameras but with one big difference: we had not only normalized ourselves to these new surveillance technologies, we actively enjoyed their company.

Behind a façade of user loyalty, tech companies make billions by promising the public one thing and the government the opposite. As Snowden revealed, Microsoft proclaims that they "believe it's important that you have control over who can and cannot access your personal data in the cloud," while working with the American government to provide easier access to that very same data.

This new incarnation of surveillance synthesizes Orwell's dystopia with Aldous Huxley's *Brave New World*. In Orwell's creation, an authoritarian surveillance state maintains order; in Huxley's, the self-medication of soma, an antidepressant drug that keeps everyone smiling, does the same work. Today, surveillance is carried out less by a Big Brother as by a set of Best Friends: these services remember our birthdays, answer our questions without casting judgment, and suggest films and books we might like. Far from being based on fear, the new surveillance system is fun, caring, and helpful. When Facebook crashed in some US cities during summer 2014, many Americans called 911.

The tech firms assure us that their products center on us, the customers. But this masks not only their own profit motives but also their perfect harmony of interests with the state. Governments allow corporations to systematically collect individual information—no matter what risks or consequences it may present for consumers—because governments receive access to that data in return. Corporations, for their part, hand data over to governments because they receive favorable legislation in return.

This harmony becomes all the more apparent when one examines the revolving door between the state and tech companies. The Center for Responsive Politics recently found that the five biggest tech firms—Apple, Amazon, Google, Facebook, and Microsoft—spent $49 million on lobbying in 2015 alone, more than double the $20 million the five largest banks spent and roughly $3 million more than the five largest oil companies.

During the Obama years, the tech industry embedded itself in Washington. Almost two hundred people who worked for Barack Obama's administration in 2015 were working for Google by the end of 2016, while fifty-eight moved in the opposite direction. Under Obama, Google executives were reported to meet in the White House more than once a week on average.

While Silicon Valley leans Democratic, they've also found favor in the Trump White House. The Silicon Valley billionaire Peter Thiel now serves as one of Trump's key advisers, and one of Trump's first moves after the election was to hold a tech summit at Trump Tower, inviting leaders to a reception that no other industry received. "I'm here to help you folks do well," he promised.

A Tool of Control

In the 1990s, the Internet seemed to promise an era of new freedom and expanded global connectivity. When Harvard law professor Lawrence Lessig expressed trepidation in 2000, he was widely dismissed. "Left to itself," he warned, "cyberspace will become a perfect tool of control." Few agreed: "Lessig doesn't offer much proof that a Soviet-style loss of privacy and freedom is on its way," sneered one skeptical reviewer.

Seventeen years have passed, and we now have a surveillance apparatus that exceeds anything past authoritarian states could've mustered.

But we should not reduce the dangers of informational capitalism to government surveillance. These tech companies' underlying philosophy represents a threat to freedom in itself. Silicon Valley ideology has saturated cyberspace and is rebuilding the world in its image, likely surpassing anything Lessig could have foreseen.

Tech CEOs celebrate today as "the most measured age in history," equating gathering information with the Enlightenment ideal of knowledge-discovery. Corporations promise us that so long as they have access to everyone's information, they can right all of society's wrongs. This encapsulates the Big Data mindset: solving human problems only requires collecting enough information. With full faith in this ideology, most informational capitalists agree with Google chief economist Varian:

any resistance to the loss of privacy will dissipate because "the advantages, in terms of convenience, safety, and services, will be so great."

But this data-driven understanding of progress constricts the individual. Privacy is meant to be a space of creative experimentation, free from judgment and beyond external control. A world without privacy, by contrast, risks a world of complete conformity. Ideally, the individual's private experimentations challenge prevailing norms and ideologies; this friction, the argument goes, pushes society forward. Under informational capitalism, however, what once demanded respect for privacy—progress—now demands its rejection.

Under big-data capitalism, the privacy of the individual is subsumed within an ideology of profit-linked progress. Where liberalism held that restricting freedom of expression is a "peculiar evil, one that is robbing the human race," informational capitalism updates this: the refusal to share personal information robs the human race. To keep some aspects of yourself private now stands in the way of progress.

That Silicon Valley's concept of progress aligns so perfectly with its own profit interests is striking. Not only does this ideology promote technology as the solution to all problems—and who will supply the technology?—but it also makes profit and progress require the exact same resource: more and more personal information. The harmony between progress and profit is not perfect, however, and the seed of this contradiction reveals Silicon Valley's authoritarian aspect most clearly.

While in terms of "progress" these tech companies present themselves as radical pioneers—they move fast and break things, as the mantra goes—when it comes to profit this "radicalness" masks a conflicting desire for complete conformity. As privacy scholar Julie Cohen notes, informational capitalism ultimately wishes to "produce tractable, predictable citizen-consumers whose preferred modes of self-determination play out along predictable and profit-generating trajectories."

To do so, these tech firms establish a dense web of options—as in Spotify's and Netflix's curated recommendations—tailored to a particular version

of an individual's identity, "designed to promote consumptive and profit-maximising choices that will systematically disfavour innovations designed to promote other values." As Google's former design ethicist Tristan Harris puts it, "if you control the menu, you control the choices"—and if you control the choices, you control the actions.

Capitalism has always tried to align society's ambitions with its own. With the Internet, its reach becomes almost inescapable. Few, if any, opposing forces still exist. Of the fifteen most visited websites in the world, only one, Wikipedia, does not operate under Silicon Valley's logic. Coupled with the increasing importance of the Internet as a site for human development, its pervasive influence cannot be healthy for a diverse, democratic society. This dynamic only intensifies when two companies, Google and Facebook, virtually control the market.

As a place of self-formation, public discussion, and social organization, the Internet frames our thinking, our knowledge, and our behavior. Today, it is constructed almost exclusively in favor of maximizing profit.

In a mockery of its initial utopian promise, the Internet has become not only a tool of mass surveillance, but also an advanced advertising technology and a means of social control. If we want to challenge this state of a airs, we should begin by having more meaningful conversations about the Internet we want. It matters too much to remain the sole preserve of corporations.

Data, if it must be collected, should be democratized, not filtered through secret algorithms for private gain. Until informational capitalism's tyrannical control of the Internet is broken, the dangers will only deepen. As with all tyrannies, citizens' lives will become more and more transparent, while the activities of the powerful become ever more opaque.

Is It Time to Break Up Google?

by Jonathan Taplin
From The New York Times *April 22, 2017*

In just 10 years, the world's five largest companies by market capitalization have all changed, save for one: Microsoft. Exxon Mobil, General Electric, Citigroup and Shell Oil are out and Apple, Alphabet (the parent company of Google), Amazon and Facebook have taken their place.

They're all tech companies, and each dominates its corner of the industry: Google has an 88 percent market share in search advertising, Facebook (and its subsidiaries Instagram, WhatsApp and Messenger) owns 77 percent of mobile social traffic and Amazon has a 74 percent share in the e-book market. In classic economic terms, all three are monopolies.

We have been transported back to the early 20th century, when arguments about "the curse of bigness" were advanced by President Woodrow Wilson's counselor, Louis Brandeis, before Wilson appointed him to the Supreme Court. Brandeis wanted to eliminate monopolies, because (in the words of his biographer Melvin Urofsky) "in a democratic society the existence of large centers of private power is dangerous to the continuing vitality of a free people." We need look no further than the conduct of

the largest banks in the 2008 financial crisis or the role that Facebook and Google play in the "fake news" business to know that Brandeis was right.

While Brandeis generally opposed regulation—which, he worried, inevitably led to the corruption of the regulator—and instead advocated breaking up "bigness," he made an exception for "natural" monopolies, like telephone, water and power companies and railroads, where it made sense to have one or a few companies in control of an industry.

Could it be that these companies—and Google in particular—have become natural monopolies by supplying an entire market's demand for a service, at a price lower than what would be offered by two competing firms? And if so, is it time to regulate them like public utilities?

Consider a historical analogy: the early days of telecommunications.

In 1895 a photograph of the business district of a large city might have shown 20 phone wires attached to most buildings. Each wire was owned by a different phone company, and none of them worked with the others. Without network effects, the networks themselves were almost useless.

The solution was for a single company, American Telephone and Telegraph, to consolidate the industry by buying up all the small operators and creating a single network—a natural monopoly. The government permitted it, but then regulated this monopoly through the Federal Communications Commission.

AT&T (also known as the Bell System) had its rates regulated, and was required to spend a fixed percentage of its profits on research and development. In 1925 AT&T set up Bell Labs as a separate subsidiary with the mandate to develop the next generation of communications technology, but also to do basic research in physics and other sciences. Over the next 50 years, the basics of the digital age—the transistor, the microchip, the solar cell, the microwave, the laser, cellular telephony—all came out of Bell Labs, along with eight Nobel Prizes.

In a 1956 consent decree in which the Justice Department allowed AT&T

to maintain its phone monopoly, the government extracted a huge concession: All past patents were licensed (to any American company) royalty-free, and all future patents were to be licensed for a small fee. These licenses led to the creation of Texas Instruments, Motorola, Fairchild Semiconductor and many other start-ups.

True, the internet never had the same problems of interoperability. And Google's route to dominance is different from the Bell System's. Nevertheless it still has all of the characteristics of a public utility.

We are going to have to decide fairly soon whether Google, Facebook and Amazon are the kinds of natural monopolies that need to be regulated, or whether we allow the status quo to continue, pretending that unfettered monoliths don't inflict damage on our privacy and democracy.

It is impossible to deny that Facebook, Google and Amazon have stymied innovation on a broad scale. To begin with, the platforms of Google and Facebook are the point of access to all media for the majority of Americans. While profits at Google, Facebook and Amazon have soared, revenues in media businesses like newspaper publishing or the music business have, since 2001, fallen by 70 percent.

According to the Bureau of Labor Statistics, newspaper publishers lost over half their employees between 2001 and 2016. Billions of dollars have been reallocated from creators of content to owners of monopoly platforms. All content creators dependent on advertising must negotiate with Google or Facebook as aggregator, the sole lifeline between themselves and the vast internet cloud.

It's not just newspapers that are hurting. In 2015 two Obama economic advisers, Peter Orszag and Jason Furman, published a paper arguing that the rise in "supernormal returns on capital" at firms with limited competition is leading to a rise in economic inequality. The M.I.T. economists Scott Stern and Jorge Guzman explained that in the presence of these giant firms, "it has become increasingly advantageous to be an incumbent, and less advantageous to be a new entrant."

There are a few obvious regulations to start with. Monopoly is made by acquisition—Google buying AdMob and DoubleClick, Facebook buying Instagram and WhatsApp, Amazon buying, to name just a few, Audible, Twitch, Zappos and Alexa. At a minimum, these companies should not be allowed to acquire other major firms, like Spotify or Snapchat.

The second alternative is to regulate a company like Google as a public utility, requiring it to license out patents, for a nominal fee, for its search algorithms, advertising exchanges and other key innovations.

The third alternative is to remove the "safe harbor" clause in the 1998 Digital Millennium Copyright Act, which allows companies like Facebook and Google's YouTube to free ride on the content produced by others. The reason there are 40,000 Islamic State videos on YouTube, many with ads that yield revenue for those who posted them, is that YouTube does not have to take responsibility for the content on its network. Facebook, Google and Twitter claim that policing their networks would be too onerous. But that's preposterous: They already police their networks for pornography, and quite well.

Removing the safe harbor provision would also force social networks to pay for the content posted on their sites. A simple example: One million downloads of a song on iTunes would yield the performer and his record label about $900,000. One million streams of that same song on YouTube would earn them about $900.

I'm under no delusion that, with libertarian tech moguls like Peter Thiel in President Trump's inner circle, antitrust regulation of the internet monopolies will be a priority. Ultimately we may have to wait four years, at which time the monopolies will be so dominant that the only remedy will be to break them up. Force Google to sell DoubleClick. Force Facebook to sell WhatsApp and Instagram.

Woodrow Wilson was right when he said in 1913, "If monopoly persists, monopoly will always sit at the helm of the government." We ignore his words at our peril.

Data populists must seize our information – for the benefit of us all

by Evgeny Morozov
From The Guardian *December 16, 2016*

Of all the big firms in Silicon Valley, Amazon had the most to lose from Donald Trump's presidency. And lose it did, albeit briefly, its share price dropping 5% shortly after the election.

During the campaign, Trump warned that Amazon had a "huge antitrust problem"—a reasonable stance for the populist that he once aspired to be. Most likely, though, his animosity had more to do with the fact Amazon's founder, Jeff Bezos, also owns the Washington Post, an influential newspaper that took an early strong dislike of Trump. By the time of Amazon's massive cloud- computing conference, which kicked off in Las Vegas at the end of November, such squabbles seem to have been forgotten. Amazon went on to wow the audience with impressive gimmicks. Did you know it has a truck—yes, a real truck—to drive your data to the cloud? Apparently, it's much faster than using networks.

Amazon also unveiled its cloud-based artificial intelligence services, including systems for recognising objects in images, processing speech commands, and operating chatbot applications. Thus, it's joining Google, Microsoft, Facebook, and IBM in the already crowded field of advanced AI.

For Amazon, this is hardly new territory. By now, it must have built a robust AI operation for its own use, what with all the data it has amassed on its users (it's precisely the troves of such data that explain recent breakthroughs in one of the most promising strands of contemporary AI—deep learning).

Now, Amazon wants to make money by letting others tap into its existing AI infrastructure. It did something similar a decade ago, when it realised it had a lot of spare server infrastructure it could lend out to others. A clever move: today Amazon's cloud services often generate more profits than its retail operations in North America.

Its nascent AI operation is likely to rely on a similar model: clients will pay to tap into Amazon's ability to recognise images or voices and insert such magic into their app or service. The other four AI giants are also unlikely to settle on a charity model. As they integrate AI products into healthcare, education, energy and transport, they will eventually pass on the bill to citizens – either directly, as usage fees, or indirectly, through lucrative contracts with institutions such as the NHS.

The political implications are mind-boggling. Five American firms—China's Baidu being the only significant foreign contender—have already extracted, processed and digested much of the world's data. This has given them advanced AI capabilities, helping to secure control over a crucial part of the global digital infrastructure. Immense power has been shifted to just one sector of society as a result.

Imagine, for a moment, that all the world's land suddenly became the property of just five big banks or property developers, with the rest of us having to pay a fee whenever our feet touched the ground. This wouldn't be unprecedented. Such efforts of aristocratic and financial elites to snatch up and profit from land spawned new economic philosophies, like georgism, and boosted policy interventions, like the land value tax. But what to do about similar efforts to snatch up data?

Two approaches have proven particularly popular. One celebrates alternative models of economic organisation—for example, cooperatives that are less exploitative than platforms such as Amazon or Microsoft. Such

efforts at platform cooperativism are worthwhile; occasionally, they do produce impressive and ethical local projects.

There is no reason why a cooperative of drivers in a small town cannot build an app to help them beat Uber locally. But there is also no good reason to believe that this local cooperative can actually build a self-driving car: this requires massive investment and a dedicated infrastructure to harvest and analyse all of the data. One can, of course, also create data ownership cooperatives but it's unlikely they will scale to a point of competing with Google or Amazon.

Another approach—simply to break up or shrink big technology firms—is also problematic. It assumes that data is simply like any other product, like, say, oil or widgets. Such a view, however, is inaccurate. Oil doesn't become better or more valuable simply because you store more of it in your warehouse. Data, however, does: the more of it you harvest, the better the insights—and the higher the savings you can pass on to citizens. Today's advances in AI were possible only because a handful of companies have, in fact, enjoyed the status of quasi monopolies. Ten thousand startups, each owning a tiny piece of Google's data empire, would never produce a self-driving car either.

Leftwing populists, such as Bernie Sanders and Elizabeth Warren, do not seem to realise that data has its own properties, insisting, instead, that giant tech platforms harm competition. One fights this threat by limiting the size of these firms and ensuring they don't extend their tentacles into too many sectors and technologies. In other words, the goal is to make the marketplace more competitive.

However, in the absence of active government policy on AI, a truly competitive marketplace will never deliver on the massive expectations, as it will be too fragmented to create value from all the data. Nor will it deliver the cheap goods that consumers—faced with falling incomes—have come to depend upon. The rhetoric of improving competition cannot lie at the heart of economic populism in the 21st century. A much better agenda for left-leaning populists would be to insist that data is an essential, infrastructural good that should belong to all of us; it should

not be claimed, owned, or managed by corporations. Enterprises should, of course, be allowed to build their services around it but only once they pay their dues. The ownership of this data—and the advanced AI built on it—should always remain with the public. This way, citizens and popular institutions can ensure that companies do not hold us hostage, imposing fees for using services that we ourselves have helped to produce. Instead of us paying Amazon a fee to use its AI capabilities—built with our data—Amazon should be required to pay that fee to us.

This points to a broader deficiency with most populist projects of the left: all they can promise is just more of the same but done better, utopia be damned. So, antitrust regulations will get tougher; jobs will magically come back; the welfare state will once again be as generous as it was in the 1960s.

However, the jobs won't come back because they never really left: they were simply automated out of existence. Making big data firms smaller is not a programme that will excite anyone with even a rudimentary understanding of what makes these firms so effective and their products so affordable. Waxing nostalgic about the highly intrusive welfare state—while Silicon Valley elites cheerlead for the creative flexibility of basic income—also seems suicidal.

The left's inability to master this new populist language is all the more puzzling, given that technology is one issue where rightwing populists such as Trump and Ukip have little to offer. It's even hard to imagine what the rightwing version of data populism would be like, other than to say that we have been living and breathing such populism, albeit in a polished, neoliberal version of Barack Obama or David Cameron, for the last decade.

Data populism, in other words, is one issue on which the populist left does have a genuine advantage, but only if it understands that the traditional progressive agenda, like everything else these days, has been utterly disrupted by digital technology. Instead of denying it, progressive populists should use the data debate as an opportunity to re-establish their relevance to the crucial economic debates of today.

The Secrets of Surveillance Capitalism
http://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html

Big Data's Hidden Labor
https://www.jacobinmag.com/2017/03/big-data-smartphones-google-amazon-facebook-surveillance-tech/

The Big Data Era of Mosaicked Deidentification
https://www.forbes.com/sites/kalevleetaru/2016/08/24/the-big-data-era-of-mosaicked-deidentification-can-we-anonymize-data-anymore/

Google now knows when its users go to the store and buy stuff
https://www.washingtonpost.com/news/the-switch/wp/2017/05/23/google-now-knows-when-you-are-at-a-cash-register-and-how-much-you-are-spending/

How Privacy Became a Commodity for the Rich and Powerful
https://www.nytimes.com/2017/05/09/magazine/how-privacy-became-a-commodity-for-the-rich-and-powerful.html

Capitalism vs. Privacy
https://www.jacobinmag.com/2017/04/google-facebook-informational-capitalism/

Is It Time to Break Up Google?
https://www.nytimes.com/2017/04/22/opinion/sunday/is-it-time-to-break-up-google.html

Data populists must seize our information – for the benefit of us all
https://www.theguardian.com/commentisfree/2016/dec/04/data-populists-must-seize-information-for-benefit-of-all-evgeny-morozov

This is how in our own lifetimes we observe capitalism shifting under our gaze: once profits from products and services, then profits from speculation, and now profits from surveillance.

SHOSHANA ZUBOFF