MERCOLA
Take Control of Your Health

Harvard Professor Exposes Google and Facebook

Analysis by Dr. Joseph Mercola ✔ Fact Checked | December 10, 2022

STORY AT-A-GLANCE

- In her book, "The Age of Surveillance Capitalism," social psychologist and Harvard professor Shoshana Zuboff reveals how the biggest tech companies in the world have hijacked our personal data — so-called "behavioral surplus data streams" — without our knowledge or consent and are using it against you to generate profits for themselves
- Companies like Facebook, Google and third parties of all kinds have the power — and are using that power — to target your personal inner demons, to trigger you, and to take advantage of you when you're at your most vulnerable to entice you into action that serves them, commercially or politically
- Your entire existence — even your shifting moods, deciphered by facial recognition software — has become a source of revenue for corporate entities as you're being cleverly maneuvered into doing (and typically buying) or thinking something you may not have done, bought or thought otherwise
- Facebook's massive experiments, in which they used subliminal cues to see if they could make people happier or sadder and affect real-world behavior offline, proved that — by manipulating language and inserting subliminal cues in the online context — they can change real-world behavior and real-world emotion, and that these methods and powers can be exercised "while bypassing user awareness"
- The Google Nest security system has a hidden microphone built into it that isn't featured in any of the schematics for the device. Voice data, and all the information delivered through your daily conversations, is tremendously valuable to Big Data, and add to their ever-expanding predictive modeling capabilities

> *"In a room where people unanimously maintain a conspiracy of silence, one word of truth sounds like a pistol shot."* ~ Czesław Miłosz[1]

In recent years, a number of brave individuals have alerted us to the fact that we're all being monitored and manipulated by big data gatherers such as Google and Facebook, and shed light on the depth and breadth of this ongoing surveillance. Among them is social psychologist and Harvard professor Shoshana Zuboff.

Her book, "The Age of Surveillance Capitalism," is one of the best books I have read in the last few years. It's an absolute must-read if you have any interest in this topic and want to understand how Google and Facebook have obtained such massive control of your life.

Her book reveals how the biggest tech companies in the world have hijacked our personal data — so-called "behavioral surplus data streams" — without our knowledge or consent and are using it against us to generate profits for themselves. WE have become the product. WE are the real revenue stream in this digital economy.

> *"The term 'surveillance capitalism' is not an arbitrary term,"* Zuboff says in the featured VPRO Backlight documentary. *"Why 'surveillance'? Because it must be operations that are engineered as undetectable, indecipherable, cloaked in rhetoric that aims to misdirect, obfuscate and downright bamboozle all of us, all the time."*

The Birth of Surveillance Capitalism

In the featured video, Zuboff "reveals a merciless form of capitalism in which no natural resources, but the citizen itself, serves are a raw material."[2] She also explains how this surveillance capitalism came about in the first place.

As most revolutionary inventions, chance played a role. After the 2000 dot.com crisis that burst the internet bubble, a startup company named Google struggled to survive. Founders Larry Page and Sergey Brin appeared to be looking at the beginning of the end for their company.

By chance, they discovered that "residual data" left behind by users during their internet searchers had tremendous value. They could trade this data; they could sell it. By compiling this residual data, they could predict the behavior of any given internet user and thus guarantee advertisers a more targeted audience. And so, surveillance capitalism was born.

The Data Collection You Know About Is the Least Valuable

Comments such as "I have nothing to hide, so I don't care if they track me," or "I like targeted ads because they make my shopping easier" reveal our ignorance about what's really going on. We believe we understand what kind of information is being collected about us. For example, you might not care that Google knows you bought a particular kind of shoe, or a particular book.

However, the information we freely hand over is the least important of the personal information actually being gathered about us, Zuboff notes. Tech companies tell us the data collected is being used to improve services, and indeed, some of it is.

But it is also being used to model human behavior by analyzing the patterns of behavior of hundreds of millions of people. Once you have a large enough training model, you can begin to accurately predict how different types of individuals will behave over time.

The data gathered is also being used to predict a whole host of individual attributes about you, such as personality quirks, sexual orientation, political orientation — "a whole range of things we never ever intended to disclose," Zuboff says.

How Is Predictive Data Being Used?

All sorts of predictive data are handed over with each photo you upload to social media. For example, it's not just that tech companies can see your photos. Your face is being used without your knowledge or consent to train facial recognition software, and none of us is told how that software is intended to be used.

As just one example, the Chinese government is using facial recognition software to track and monitor minority groups and advocates for democracy, and that could happen elsewhere as well, at any time.

So that photo you uploaded of yourself at a party provides a range of valuable information — from the types of people you're most likely to spend your time with and where you're likely to go to have a good time, to information about how the muscles in your face move and alter the shape of your features when you're in a good mood.

By gathering a staggering amount of data points on each person, minute by minute, Big Data can make very accurate predictions about human behavior, and these predictions are then "sold to business customers who want to maximize our value to their business," Zuboff says.

Your entire existence — even your shifting moods, deciphered by facial recognition software — has become a source of revenue for many tech corporations. You might think you have free will but, in reality, you're being cleverly maneuvered and funneled into doing (and typically buying) or thinking something you may not have done, bought or thought otherwise. And, "our ignorance is their bliss," Zuboff says.

The Facebook Contagion Experiments

In the documentary, Zuboff highlights Facebook's massive "contagion experiments,"[3,4] in which they used subliminal cues and language manipulation to see if they could make people feel happier or sadder and affect real-world behavior offline. As it turns out, they can. Two key findings from those experiments were:

1. By manipulating language and inserting subliminal cues in the online context, they can change real-world behavior and real-world emotion
2. These methods and powers can be exercised "while bypassing user awareness"

In the video, Zuboff also explains how the Pokemon Go online game — which was actually created by Google — was engineered to manipulate real-world behavior and

activity for profit. She also describes the scheme in her New York Times article, saying:

> *"Game players did not know that they were pawns in the real game of behavior modification for profit, as the rewards and punishments of hunting imaginary creatures were used to herd people to the McDonald's, Starbucks and local pizza joints that were paying the company for 'footfall,' in exactly the same way that online advertisers pay for 'click through' to their websites."*

You're Being Manipulated Every Single Day in Countless Ways

Zuboff also reviews what we learned from the Cambridge Analytica scandal. Cambridge Analytica is a political marketing business that, in 2018, used the Facebook data of 80 million Americans to determine the best strategies for manipulating American voters.

Christopher Wylie, now-former director of research at Cambridge Analytica, blew the whistle on the company's methods. According to Wylie, they had so much data on people, they knew exactly how to trigger fear, rage and paranoia in any given individual. And, by triggering those emotions, they could manipulate them into looking at a certain website, joining a certain group, and voting for a certain candidate.

So, the reality now is, companies like Facebook, Google and third parties of all kinds, have the power — and are using that power — to target your personal inner demons, to trigger you, and to take advantage of you when you're at your weakest or most vulnerable to entice you into action that serves them, commercially or politically. It's certainly something to keep in mind while you surf the web and social media sites.

> *"It was only a minute ago that we didn't have many of these tools, and we were fine,"* Zuboff says in the film. *"We lived rich and full lives. We had close connections with friends and family.*
>
> *Having said that, I want to recognize that there's a lot that the digital world brings to our lives, and we deserve to have all of that. But we deserve to have it without paying the price of surveillance capitalism.*

Right now, we are in that classic Faustian bargain; 21st century citizens should not have to make the choice of either going analog or living in a world where our self-determination and our privacy are destroyed for the sake of this market logic. That is unacceptable.

Let's also not be naïve. You get the wrong people involved in our government, at any moment, and they look over their shoulders at the rich control possibilities offered by these new systems.

There will come a time when, even in the West, even in our democratic societies, our government will be tempted to annex these capabilities and use them over us and against us. Let's not be naïve about that.

When we decide to resist surveillance capitalism — right now when it is in the market dynamic — we are also preserving our democratic future, and the kinds of checks and balances that we will need going forward in an information civilization if we are to preserve freedom and democracy for another generation."

Surveillance Is Getting Creepier by the Day

But the surveillance and data collection doesn't end with what you do online. Big Data also wants access to your most intimate moments — what you do and how you behave in the privacy of your own home, for example, or in your car. Zuboff recounts how the Google Nest security system was found to have a hidden microphone built into it that isn't featured in any of the schematics for the device.

"Voices are what everybody are after, just like faces," Zuboff says. Voice data, and all the information delivered through your daily conversations, is tremendously valuable to Big Data, and add to their ever-expanding predictive modeling capabilities.

She also discusses how these kinds of data-collecting devices force consent from users by holding the functionality of the device "hostage" if you don't want your data collected and shared.

For example, Google's Nest thermostats will collect data about your usage and share it with third parties, that share it with third parties and so on ad infinitum — and Google takes no responsibility for what any of these third parties might do with your data.

You can decline this data collection and third party sharing, but if you do, Google will no longer support the functionality of the thermostat; it will no longer update your software and may affect the functionality of other linked devices such as smoke detectors.

Two scholars who analyzed the Google Nest thermostat contract concluded that a consumer who is even a little bit vigilant about how their consumption data is being used would have to review 1,000 privacy contracts before installing a single thermostat in their home.

Modern cars are also being equipped with multiple cameras that feed Big Data. As noted in the film, the average new car has 15 cameras, and if you have access to the data of a mere 1% of all cars, you have "knowledge of everything happening in the world."

Of course, those cameras are sold to you as being integral to novel safety features, but you're paying for this added safety with your privacy, and the privacy of everyone around you.

Pandemic Measures Are Rapidly Eroding Privacy

The current coronavirus pandemic is also using "safety" as a means to dismantle personal privacy. As reported by The New York Times, March 23, 2020:[5]

> *"In South Korea, government agencies are harnessing surveillance-camera footage, smartphone location data and credit card purchase records to help trace the recent movements of coronavirus patients and establish virus transmission chains.*
>
> *In Lombardy, Italy, the authorities are analyzing location data transmitted by citizens' mobile phones to determine how many people are obeying a*

government lockdown order and the typical distances they move every day. About 40 percent are moving around "too much," an official recently said.

In Israel, the country's internal security agency is poised to start using a cache of mobile phone location data — originally intended for counterterrorism operations — to try to pinpoint citizens who may have been exposed to the virus.

As countries around the world race to contain the pandemic, many are deploying digital surveillance tools as a means to exert social control, even turning security agency technologies on their own civilians …

Yet ratcheting up surveillance to combat the pandemic now could permanently open the doors to more invasive forms of snooping later. It is a lesson Americans learned after the terrorist attacks of Sept. 11, 2001, civil liberties experts say.

Nearly two decades later, law enforcement agencies have access to higher-powered surveillance systems, like fine-grained location tracking and facial recognition — technologies that may be repurposed to further political agendas …

'We could so easily end up in a situation where we empower local, state or federal government to take measures in response to this pandemic that fundamentally change the scope of American civil rights,' said Albert Fox Cahn, the executive director of the Surveillance Technology Oversight Project, a nonprofit organization in Manhattan."

Humanity at a Cross-Roads

Zuboff also discusses her work in a January 24, 2020, op-ed in The New York Times.[6,7] "You are now remotely controlled. Surveillance capitalists control the science and the scientists, the secrets and the truth," she writes, continuing:

"We thought that we search Google, but now we understand that Google searches us. We assumed that we use social media to connect, but we learned that connection is how social media uses us.

We barely questioned why our new TV or mattress had a privacy policy, but we've begun to understand that 'privacy' policies are actually surveillance policies … Privacy is not private, because the effectiveness of … surveillance and control systems depends upon the pieces of ourselves that we give up — or that are secretly stolen from us.

Our digital century was to have been democracy's Golden Age. Instead, we enter its third decade marked by a stark new form of social inequality best understood as 'epistemic inequality' … extreme asymmetries of knowledge and the power that accrues to such knowledge, as the tech giants seize control of information and learning itself …

Surveillance capitalists exploit the widening inequity of knowledge for the sake of profits. They manipulate the economy, our society and even our lives with impunity, endangering not just individual privacy but democracy itself …

Still, the winds appear to have finally shifted. A fragile new awareness is dawning … Surveillance capitalists are fast because they seek neither genuine consent nor consensus. They rely on psychic numbing and messages of inevitability to conjure the helplessness, resignation and confusion that paralyze their prey.

Democracy is slow, and that's a good thing. Its pace reflects the tens of millions of conversations that occur … gradually stirring the sleeping giant of democracy to action.

These conversations are occurring now, and there are many indications that lawmakers are ready to join and to lead. This third decade is likely to decide our fate. Will we make the digital future better, or will it make us worse?"[8,9]

Epistemic Inequality

Epistemic inequality refers to inequality in what you're able to learn. "It is defined as unequal access to learning imposed by private commercial mechanisms of information capture, production, analysis and sales. It is best exemplified in the fast-growing abyss between what we know and what is known about us," Zuboff writes in her New York Times op-ed.[10]

Google, Facebook, Amazon and Microsoft have spearheaded the surveillance market transformation, placing themselves at the top tier of the epistemic hierarchy. They know everything about you and you know nothing about them. You don't even know what they know about you.

> *"They operated in the shadows to amass huge knowledge monopolies by taking without asking, a maneuver that every child recognizes as theft,"* Zuboff writes.
>
> *"Surveillance capitalism begins by unilaterally staking a claim to private human experience as free raw material for translation into behavioral data. Our lives are rendered as data flows."*

These data flows are about you, but not for you. All of it is used against you — to separate you from your money, or to make you act in a way that is in some way profitable for a company or a political agenda. So, ask yourself, where is your freedom in all of this?

They're Making You Dance to Their Tune

If a company can cause you to buy stuff you don't need by sticking an enticing, personalized ad for something they know will boost your confidence at the exact moment you're feeling insecure or worthless (a tactic that has been tested and perfected[11]), are you really acting through free will?

If an artificial intelligence using predictive modeling senses you're getting hungry (based on a variety of cues such as your location, facial expressions and verbal

expressions) and launches an ad from a local restaurant to you in the very moment you're deciding to get something to eat, are you really making conscious, self-driven, value-based life choices? As noted by Zuboff in her article:[12]

> *"Unequal knowledge about us produces unequal power over us, and so epistemic inequality widens to include the distance between what we can do and what can be done to us. Data scientists describe this as the shift from monitoring to actuation, in which a critical mass of knowledge about a machine system enables the remote control of that system.*
>
> *Now people have become targets for remote control, as surveillance capitalists discovered that the most predictive data come from intervening in behavior to tune, herd and modify action in the direction of commercial objectives.*
>
> *This third imperative, 'economies of action,' has become an arena of intense experimentation. 'We are learning how to write the music,' one scientist said, 'and then we let the music make them dance' …*
>
> *The fact is that in the absence of corporate transparency and democratic oversight, epistemic inequality rules. They know. They decide who knows. They decide who decides. The public's intolerable knowledge disadvantage is deepened by surveillance capitalists' perfection of mass communications as gaslighting …*
>
> *On April 30, 2019 Mark Zuckerberg made a dramatic announcement at the company's annual developer conference, declaring, 'The future is private.' A few weeks later, a Facebook litigator appeared before a federal district judge in California to thwart a user lawsuit over privacy invasion, arguing that the very act of using Facebook negates any reasonable expectation of privacy 'as a matter of law.'"*

We Need a Whole New Regulatory Framework

In the video, Zuboff points out that there are no laws in place to curtail this brand-new type of surveillance capitalism, and the only reason it has been able to flourish over the past 20 years is because there's been an absence of laws against it, primarily because it has never previously existed.

That's the problem with epistemic inequality. Google and Facebook were the only ones who knew what they were doing. The surveillance network grew in the shadows, unbeknownst to the public or lawmakers. Had we fought against it for two decades, then we might have had to resign ourselves to defeat, but as it stands, we've never even tried to regulate it.

This, Zuboff says, should give us all hope. We can turn this around and take back our privacy, but we need legislation that addresses the actual reality of the entire breadth and depth of the data collection system. It's not enough to address just the data that we know that we're giving when we go online. Zuboff writes:[13]

> *"These contests of the 21st century demand a framework of epistemic rights enshrined in law and subject to democratic governance. Such rights would interrupt data supply chains by safeguarding the boundaries of human experience before they come under assault from the forces of datafication.*
>
> *The choice to turn any aspect of one's life into data must belong to individuals by virtue of their rights in a democratic society. This means, for example, that companies cannot claim the right to your face, or use your face as free raw material for analysis, or own and sell any computational products that derive from your face …*
>
> *Anything made by humans can be unmade by humans. Surveillance capitalism is young, barely 20 years in the making, but democracy is old, rooted in generations of hope and contest.*
>
> *Surveillance capitalists are rich and powerful, but they are not invulnerable. They have an Achilles heel: fear. They fear lawmakers who do not fear them. They fear citizens who demand a new road forward as they insist on new*

answers to old questions: Who will know? Who will decide who knows? Who will decide who decides? Who will write the music, and who will dance?"

How to Protect Your Online Privacy

While there's no doubt we need a whole new legislative framework to curtail surveillance capitalism, in the meantime, there are ways you can **protect your privacy online** and limit the "behavioral surplus data" collected about you.

Robert Epstein, senior research psychologist for the American Institute of Behavioral Research and Technology, recommends taking the following steps to protect your privacy:[14]

Use a virtual private network (VPN) such as Nord, which is only about $3 per month and can be used on up to six devices. In my view, this is a must if you seek to preserve your privacy. Epstein explains:

> *"When you use your mobile phone, laptop or desktop in the usual way, your identity is very easy for Google and other companies to see. They can see it via your IP address, but more and more, there are much more sophisticated ways now that they know it's you. One is called browser fingerprinting.*
>
> *This is something that is so disturbing. Basically, the kind of browser you have and the way you use your browser is like a fingerprint. You use your browser in a unique way, and just by the way you type, these companies now can instantly identify you.*
>
> *Brave has some protection against a browser fingerprinting, but you really need to be using a VPN. What a VPN does is it routes whatever you're doing through some other computer somewhere else. It can be anywhere in the world, and there are hundreds of companies offering VPN services. The one I like the best right now is called Nord VPN.*

You download the software, install it, just like you install any software. It's incredibly easy to use. You do not have to be a techie to use Nord, and it shows you a map of the world and you basically just click on a country.

The VPN basically makes it appear as though your computer is not your computer. It basically creates a kind of fake identity for you, and that's a good thing. Now, very often I will go through Nord's computers in the United States. Sometimes you have to do that, or you can't get certain things done. PayPal doesn't like you to be in a foreign country for example."

Nord, when used on your cellphone, will also mask your identity when using apps like Google Maps.

Do not use Gmail, as every email you write is permanently stored. It becomes part of your profile and is used to build digital models of you, which allows them to make predictions about your line of thinking and every want and desire.

Many other older email systems such as AOL and Yahoo are also being used as surveillance platforms in the same way as Gmail. ProtonMail.com, which uses end-to-end encryption, is a great alternative and the basic account is free.

Don't use Google's Chrome browser, as everything you do on there is surveilled, including keystrokes and every webpage you've ever visited. Brave is a great alternative that takes privacy seriously.

Brave is also faster than Chrome, and suppresses ads. It's based on Chromium, the same software infrastructure that Chrome is based on, so you can easily transfer your extensions, favorites and bookmarks.

Don't use Google as your search engine, or any extension of Google, such as Bing or Yahoo, both of which draw search results from Google. The same goes for the iPhone's personal assistant Siri, which draws all of its answers from Google.

Alternative search engines suggested by Epstein include SwissCows and Qwant. He recommends avoiding StartPage, as it was recently bought by an aggressive online marketing company, which, like Google, depends on surveillance.

Don't use an Android cellphone, for all the reasons discussed earlier. Epstein uses a BlackBerry, which is more secure than Android phones or the iPhone. BlackBerry's upcoming model, the Key3, will be one of the most secure cellphones in the world, he says.

Don't use Google Home devices in your house or apartment — These devices record everything that occurs in your home, both speech and sounds such as brushing your teeth and boiling water, even when they appear to be inactive, and send that information back to Google. Android phones are also always listening and recording, as are Google's home thermostat Nest, and Amazon's Alexa.

Clear your cache and cookies — As Epstein explains in his article:[15]

> *"Companies and hackers of all sorts are constantly installing invasive computer code on your computers and mobile devices, mainly to keep an eye on you but sometimes for more nefarious purposes.*
>
> *On a mobile device, you can clear out most of this garbage by going to the settings menu of your browser, selecting the 'privacy and security' option and then clicking on the icon that clears your cache and cookies.*
>
> *With most laptop and desktop browsers, holding down three keys simultaneously — CTRL, SHIFT and DEL — takes you directly to the relevant menu; I use this technique multiple times a day without even thinking about it. You can also configure the Brave and Firefox browsers to erase your cache and cookies automatically every time you close your browser."*

Don't use Fitbit, as it was recently purchased by Google and will provide them with all your physiological information and activity levels, in addition to everything else that

Google already has on you.

Sources and References

- [1] Goodreads.com Czesław Miłosz Quotable Quotes
- [2] Youtube.com, Shoshana Zuboff on Surveillance Capitalism
- [3] Nature September 13, 2012; 489: 295-298 (Archived)
- [4] PNAS June 17, 2014; 111(24): 8788-8790 (Archived)
- [5] New York Times March 23, 2020 (Archived)
- [6, 8] New York Times January 24, 2020
- [7, 9, 10, 12, 13] New York Times January 24, 2020 (Archived)
- [11] The Guardian May 1, 2017 (Archived)
- [14, 15] Medium March 17, 2017