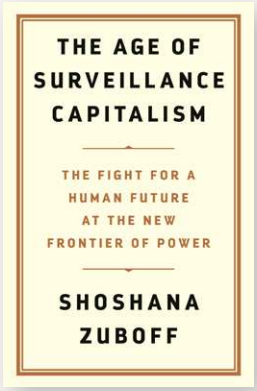
Resisting surveillance

*Interview with **Shoshana Zuboff** by Olaf Bruns*

Shoshana Zuboff is a Professor Emerita at Harvard Business School. Ever since the publication of 'In the Age of the Smart Machine' in 1988 her career has been devoted to the study of the digital, its individual and social consequences, and its relationship to the future of capitalism. Her new book 'The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power' came out in January 2019.



Shoshana Zuboff's new book 'Surveillance Capitalism' explores a new step in the history of capitalism, where big tech, and increasingly other branches of the economy, are making profits with data, extracted from citizens without their consent, and transformed into raw material for behaviour predictions - with destructive effects on the economy, democracy and individual lives.

***Progressive Post:** Your new book is called 'Surveillance capitalism' what precisely do you understand by this concept?*

Shoshana Zuboff: The way capitalism evolves is by taking things that live outside of the marketplace and bringing them into the market dynamic, in order to be sold and purchased. And in this respect, surveillance capitalism emulates this traditional pattern of capitalist history. But it does so with a dark twist. Surveillance capitalism unilaterally claims private experience and brings it into the marketplace, rendering it as behavioural data, as raw material for computational processes, where predictive patterns are discerned. And these new 'prediction products' are then sold into a new kind of marketplace that trade exclusively in these future bets on human behaviour.

***PP:** How did it come about?*

SZ: Surveillance capitalism was invented at Google in 2001 as a reaction to a financial emergency. It was invented to quickly monetise the online search services. And it became so successful that it migrated to Facebook and then within the next few years became the default option for most of the tech sector start-ups: applications and so forth. But we can no longer say that surveillance capitalism is confined to the tech-sector because now we see it spreading across the entire economy: it's in the insurance sector, the automobile sector, it's in the finance, health, education and now in virtually every product you encounter that has the word 'smart' in front of it. And every service that has the word 'personalised' in its name is participating in these ecosystems that define surveillance capitalism supply chains.

*#SurveillanceCapitalism: disentangling our lives, recovering freedom - and interview with **@shoshanazuboff***

| Nest is a thermostat that can be connected to other devices at home. It collects data from all aspects of the occupant's behaviour at home.

Surveillance capitalists understand that the more people know about these kinds of practices, the more they want to protect themselves. If BigTech wants to collect data from us, they have to do it secretly.

PP: *Let me be naïve: they are not after my online banking details, neither are they judging or blackmailing somebody who watches porn online or even reads subversive political ideas. Why should we really fear this?*

SZ: The unilateral claiming of private human experience is the essence of the surveillance relationship. There's no one coming to you and say: 'here's what we want to do – do you allow us to do this?' Surveillance capitalists understand that the more people know about these kinds of practices, the more they protest and want ways to protect themselves. If these new entities are going to collect data in order to predict our future behaviour, they have to do it secretly. This is the fundamental social relationship of surveillance capitalism: it's a one-way mirror.

And it has a variety of implications. At the societal level, with surveillance capitalism and its secret ways of universally collecting every kind of depth and breadth of information about us, we have created private institutions that exist outside of constitutional governance - certainly in the United States, even if it is somewhat different in Europe. So until now, they have largely existed outside the rule of law, outside of democratic oversight and values and they produce tremendous asymmetries of knowledge: that they know everything about us. But we know almost nothing about them. They use their knowledge for other's commercial purposes.

PP: *We haven't named them yet, but it's about the big ones: Facebook, Google and so on. Google still claims: 'don't be evil' – but aren't they?l*

SZ: This is not about people being evil, which is extremely important when it comes to issues of law and regulation. And it's not even about bad people versus good people. This is about a new economic logic, with specific economic imperatives. These are companies that are now bound to these economic imperatives if they want to be successful.

PP: *Karl Marx once wrote that if you have a hand mill, you get a society with a feudal lord and if you have a steam mill, you get a society with an industrial capitalist. Is there a determinism in technology here too? If you manage to lock people up in zillions of tiny, isolated and virtual treadmills, you get surveillance capitalism?*

SZ: I think this is a fundamental category error: the conflation of technology with surveillance capitalism. I want to make very clear that surveillance capitalism is not the same as the digital.

Let me give you an example: back in 2000s, before the invention of surveillance capitalism, a very elite group of designers, data scientists and engineers at Georgia Tech University had the idea of what they called the 'aware home' – very similar to what we call the 'smart home' today. But it had a single, closed loop: all the information went directly to the occupant of the home. And they were very explicit: because these data are so intimate and personal, only the occupants could decide what to do with them.

Fast forward to 2017: The University of London has analysed one single 'smart home' device: the 'Nest thermostat' - owned by Google. 'Nest' is an eco-system with a thermostat and other devices in your home that can be connected to that thermostat. And it's collecting a lot of data from all kinds of aspects of your behaviour in your home. The researchers found out that when installing one Nest thermostat, a conscientious consumer would need to review a minimum of one thousand privacy contracts. Because all these behavioural data are now streaming through 'Nest' to third parties.

So here we have the same technologies, but each one inhabited by a fundamentally different economic logic. And it's the economic logic here, as Max Weber warned us so long ago, that is the determinant of how these technologies are brought into our lives, of their uses and their consequences.

***PP:** The question in the run-up to the European elections is how these means of surveillance capitalism interfere with democracy?*

SZ: Here, the second category error comes into play: we can't reduce surveillance capitalism to any single company. Right now, there's a lot of focus on Facebook because most of what has disfigured our election processes in Europe and in America came through the channels of social media. But I think it's important to bear in mind that the methods that have been used in the Cambridge Analytica case to hijack our election processes are the same methods that surveillance capitalists use every day to shape our behaviour towards their commercial ends.

We have a set of means of behavioural modification that we know now pivot to political outcomes. And in the most visceral way: the political discourse and information come to us as if it were constructed by the Fourth Estate, by journalists, who have specific standards and criteria of truthfulness and a professionalism. But is has been corrupted intentionally to trick us as, to shape our behaviour in secret ways toward others ends. This obviously is a major challenge to democracy.

> *"In the 20th century, we found a way for markets and democracies to create an equilibrium - because we created the laws and the regulations that bound the excesses of capitalism, limited them and tethered them to the needs of a democratic society."*

***PP:** Are there other challenges to democracy?*

SZ: And there are more subtle challenges as well: our democratic society is also eroded from the inside by these methodologies. Because life is more and more defined by stimulus response and by subliminal rewards and punishments that saturate our environments in this new digital media age. And this slowly erodes our capacity for moral autonomy.

And we have seen this intervention in our autonomy being experimented with literally at population level. In 2012, Facebook launched its massive online 'contagion' experiment, to see if they could use subliminal cues and awareness-shaping mechanisms to change our voting behaviour in the real world. A year later there was another contagion experiment, also with subliminal cues, to see if they could change our emotional valence to make us sadder or happier. Both experiments were successful. And when they wrote these up in scholarly journals, they bragged about the fact that these methodologies were successfully evading user awareness.

***PP:** But if these companies are already so deep under our skins, or rather inside our heads, is there still room to even think of resistance?*

SZ: I don't think that resistance is going to be the problem. Today, it's impossible for us to know exactly what aspect of our experience is being rendered, where those data are going and who is using them to what end. So, the first thing is that we must name these things because we know that when people find out about these kinds of activities, they do feel resistance. They do want to say no. So, the first thing is to open the curtains, shine light on all of this and then resistance will come as a very natural response.

It will produce a sea change in public opinion and that will bring demands for action. It will bring demands to our elected officials to become more rigorous in developing the next generation of law and regulation that will protect us from these kinds of activities.

Obviously, the European Union's General Data Protection Regulation (GDPR) has already taken us much further ahead than we've been during the last 20 years. Now we have the possibility of standing on the shoulders of the GDPR in order to develop the kinds of regulatory regimes that are specifically targeted at these mechanisms.

We talk about data ownership as a solution for privacy. But when we understand the voraciousness of surveillance capitalism and how it takes, without asking, from every aspect of our experience, is data ownership really enough? Do we really want to be arguing about owning data that should not exist in the first place? I liken this to arguing about how many hours a 7-year-old should work in a factory when in fact we should be arguing about the fact that there should be no child labour at all.

We have to ask the questions of principles here: Is it legitimate for our experience to be taken without any form of meaningful consent of our part? Is it legitimate, for our experience to be rendered as behavioural data, as raw material for predictions? Is it legitimate for those predictions to be sold into secondary markets to business customers who have a stake in predicting our future behaviour? And for those operations to be inaccessible to us so that our futures are being auctioned off to others for their profit for their commercial aims and we have no say or oversight or protection from those activities?

***PP:** Beyond the public outrage that may come when people understand how their reality is being shaped around them and even inside them, what is your message to policy makers?*

SZ: The first message for our lawmakers is that we have to understand that as important as it may be to regulate a specific company, as important as it may be to apply our antitrust laws and our privacy laws, we have to go further: we have to understand that surveillance capitalism is now pervading our economy. We have to understand its specific mechanisms and we have to have a public conversation as to whether or not these mechanisms are consonant with individual sovereignty and with democratic sovereignty and then we have to understand what are the ways in which we can specifically interrupt and outlaw these mechanisms.

*How long will it take for people to fight off #SurveillanceCapitalism? By **@shoshanazuboff** in the **#EP2019***

***PP:** But how to do that, in your view?*

SZ: My view is that surveillance capitalism is a rogue mutation of capitalism. In the 20th century, we found a way for markets and democracies to create an equilibrium. But that was only because we had created the laws and the regulations that bound the excesses of capitalism and limited them and tethered them to the needs of a democratic society and to the well-being of individuals, both the social and the economic well-being of individuals. This is where we are now in history.

We're in a world now where we can't be effective in our daily lives without marching through these channels that are also surveillance capitalism's supply chains, giving them our experience for behavioural data for these secondary operations that we have no knowledge of or control over. Hence, we must to create alternatives for that. And as soon as those alternatives exist, we are all going to move to that side of the ship.

***PP:** There are already some alternatives: Telegram instead of WhatsApp or alternative search engines like DuckDuckGo instead of Google. But these things haven't really taken off yet.*

SZ: These things require scale. We do have a search engine like DuckDuckGo that conserves our privacy and that's terribly important. People may say that Google has a better search engine, but what they don't understand is that Google might have a better search engine just because of the very practices we've been describing and that improvement in its search ability comes at a cost that is invisible to most of us. We need to be aware of the real costs you buy into Google and its search and its practices that take us all the way down the road where eventually we find Cambridge Analytica.

We have two tremendously different alternatives here. And when those two alternatives are confronted, they have to be confronted in their fullness with full knowledge and transparency of what each one entails. And as I said in the beginning: when people do have that full knowledge and transparency, they reject these practices.