Surveillance Capital & Resistance

Wednesday 4 March 2020, by SOLENBERGER Peter (Date first published: 1 March 2020).

SURVEILLANCE IS CONSTANTLY in the news. As I began writing this review, a major surveillance story broke that Facebook-owned WhatsApp is suing the NSO Group, an Israeli spyware company, for compromising mobile phones running WhatsApp.

WhatsApp encrypts voice, text, image and other data and is used by activists and journalists in many countries to communicate securely. The encryption is end-to-end, so that even WhatsApp can't see the content. The NSO Group sells spyware that can be remotely installed via a seemingly innocuous WhatsApp message and then tracks and reports every conversation, text or image before encryption.

The NSO Group sells its spyware to governments and police forces around the world. The WhatsApp suit revealed that the Indian government is using the software to monitor critics of its authoritarian Hindu-nationalist policies. The Saudi government used NSO Group software to spy on journalist Jamal Khashoggi before it assassinated him in October 2018.

Facebook, which owns WhatsApp, is itself notorious for compromising users' data. In July 2019 the Federal Trade Commission fined Facebook $5 billion for failing to secure its users' data. In a scandal unmasked in March 2018, Facebook's "partner" policies had allowed Cambridge Analytica, a rightwing political consulting company, to access the data of 50 million U.S. Facebook users to help Donald Trump win the 2016 presidential election. (See "Far-right 'researchers' steal Facebook info" at https://solidarity-us.org/facebook_cambridge_analytica/.)

Facebook is attempting to disguise itself as a defender of internet privacy by suing the NSO Group and resisting demands by governments to create a "backdoor" in WhatsApp so that they can get around the encryption. It is suggesting that it might encrypt Facebook messages too.

End-to-end encryption of messages is important but it doesn't touch Facebook's main surveillance business: collecting, storing and selling the unencrypted information users give it. And Facebook can figure out most of what it wants to know from messages without seeing their content.

From its own and other surveillance sources Facebook knows about the people sending and receiving messages: names, addresses, phone numbers, email addresses, family, friends, likes, dislikes, browsing history, purchases, credit scores, property ownership, travel, voting records, etc. It can add message metadata: who communicates with whom, when, where, how long, how much data. Putting all that together it can see networks and infer content, to the extent it needs to.

Governments with sophisticated surveillance agencies can see all this too. But the pressure to go beyond metadata to access encrypted data is pervasive. Police demand access to "fight crime." Security agencies demand access to "fight terrorism."

Well-intentioned advocates demand "backdoors" to stop hate speech, incitement to genocide, fake news, and child pornography. As I began writing, a New York Times article castigated Apple for end-to-end encryption of its messages, which allow them to be used to distribute child pornography. Yet encryption is the only practical method most people have to thwart corporate and government surveillance.

This is just following the thread of one day's stories.

Three Books on Surveillance

Not surprisingly, authors have begun writing books about surveillance. Three books published in 2019 investigate the possibilities opened by technology to improve work and life and the way contemporary capitalism ruins those possibilities.

The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power by Shoshana Zuboff exposes corporate surveillance by Google, Facebook, Microsoft, Amazon and now an avalanche of companies.

Zuboff, a Harvard Business School professor emerita, wrote two previous books on technology and society: In the Age of the Smart Machine: The Future of Work and Power and, with her late husband James Maxmin, The Support Economy: Why Corporations Are Failing Individuals and the Next Episode of Capitalism.

The Age of Surveillance Capitalism is an indignant exposure and a demand that democratic governments reign in corporate surveillance so that people can freely express their humanity.

Activists and the Surveillance State: Learning from Repression, edited by Aziz Choudry, is a collection of essays on surveillance and repression in the name of national security and resistance to it.

The essays recount experiences in English-speaking capitalist democracies: the United States, Canada, Britain, Mauritius, South Africa, Australia and New Zealand. All the authors are activists. Most are academics or journalists. Choudry is an Associate Professor at McGill University in Montreal.

Activists and the Surveillance State has a more radical perspective than Surveillance Capitalism. Its contributors are anticapitalist and anti-imperialist, veterans of campaigns on behalf of national liberation, antiracist and indigenous, environmental, women's and queer struggles. All have run up against surveillance and political policing and resisted it.

Permanent Record is Edward Snowden's memoir of his journey from computer geek in a family with a long military tradition to whistleblower on mass surveillance by the U.S. "intelligence community." Snowden thanks writer Joshua Cohen for having "taken me to writing school, helping to transform my rambling reminiscences and capsule manifestos into a book that I hope he can be proud of."

The book would make great fiction: a coming-of-age story, a story of moral conflict, a spy story, an action adventure complete with an evil empire and an heroic but seemingly doomed resistance, and a love story. Except that it's true.

In the course of telling his story Snowden recounts in very accessible terms how the U.S. government collects, stores and mines data on the digital communications of almost everyone connected to the internet. Encryption and use of the "dark web" (the TOR network and others) can thwart the surveillance, but thwarting it gets you tagged too: "What do you have to hide?"

Surveillance Capitalism

Jacob Silverman reviewed The Age of Surveillance Capitalism for The New York Times on January 18, 2019 (https://www.nytimes.com/2019/01/18/books/review/shoshana-zuboff-age-of-surveillance-capitalism.h

tml). His review captures the appeal of the book to readers open to a critique of capitalism run amok with information technology.

Enter, as a critical guide, Shoshana Zuboff, who has emerged as the leading explicator of surveillance capitalism. With decades of experience studying issues of labor and power in the digital economy, Zuboff in 2015 published a paper, “Big Other: Surveillance Capitalism and the Prospects of an Information Civilization,” which has since become an essential source for anyone looking to reckon seriously with what she described as a distinct, emerging economic logic.

Now she has followed up that paper with a doorstop of a book, an intensively researched, engagingly written chronicle of surveillance capitalism’s origins and its deleterious prospects for our society.

The Age of Surveillance Capitalism tells the story of the rise of surveillance capitalism. Google was formed in 1998 and developed a slick internet search engine by collecting, storing, indexing and accessing vast quantities of data from crawling the internet (moving from website to website via links) and from saving users’ queries and clicks to see what they wanted.

The problem for Google and other internet technology companies was that they hadn’t figured out how to make money from their marvelous toys. Hence the dot-com bust. Then Google figured it out. They knew the who, what, when and where of searches and could combine that with what they knew from previous searches and from other data sources.

This allowed them to target ads more precisely, to report whether users clicked on the ads, and to charge higher prices when they did. The more Google knew about users, the better their targeting, the more clicks, and the more they could charge.

This set off a scramble to collect data. Google offered not only free searches but also free email, email groups, docs, drives, calendars, maps, browsers, operating systems, messaging, whatever they could think of. As users contributed more and more data, Google mined it, charged more for ads, and got richer and richer.

So far the data appropriation depended on users typing in data. But why stop there? Google Assistant and Google Home could answer voice queries — and listen to whatever else was happening in the vicinity. Android devices (laptops, tablets, smartphones, watches, etc.) and apps could report where users were and, with the help of various sensors, what they were doing.

Google wasn’t the only villain. Facebook, Microsoft, Amazon and others quickly followed. Cars, appliances and other devices became internet-connected. You look at your television, but it also looks at you and reports what it sees. Smart thermostats, nanny cams, garage door openers, even refrigerators spy.

The tech companies claim that surveillance is “personalization,” and to a certain extent it is convenient. But as Zuboff points out, every “privacy policy” is really a surveillance policy.

While the story is fascinating, the edifice Zuboff builds on its foundation is much less satisfying. She overtheorizes her findings. For example, she coins the term “behavioral surplus” to describe the data the surveillance capitalists extract beyond what’s needed to improve the digital product and says this is the basis for a new capitalist exploitation, superseding the exploitation of workers in production.

The reality is much simpler. Surveillance capitalism is good old government-supported monopoly capitalism using new technology.

Zuboff overstates the effectiveness of surveillance capitalism. The targets of advertising can ignore it, as consumers have ignored "hidden persuaders" in all previous media.

Surveillance capitalists dream of behavioral modification to get people to buy what they direct them to buy and to think what they direct them to think. If capitalism really could satisfy human needs, they might succeed. But the contrast between the fiction of a "good life" under capitalism and the reality generates dissatisfaction, alienation, anger and thought.

Zuboff underestimates the danger of government spying using the new technology. True in China, she says, but it couldn't happen here. But we know that a revolving door connects Big Tech and the "intelligence community" (IC).

We know that Cambridge Analytica used Facebook data to build a "friends list" of 50 million people they thought might be persuaded to vote for Trump. They or the IC could as easily have created an enemies list for harassment, blacklisting and blackmail.

Finally, Zuboff puts too much faith in the possibility of reforming surveillance capitalism and restoring the good old days of the New Deal, with capitalism regulated by the "double movement" of markets and democracy. She dismisses Marx as a utopian, but her proposed solution of democratic capitalism seems far more utopian than socialism.

The Surveillance State

Activists and the Surveillance State focuses on more traditional surveillance by political police. Almost exactly a century ago the Palmer Raids rounded up and jailed or deported activists in the "Red Scare" following World War I and the Russian Revolution. A. Mitchell Palmer, the Attorney General under Democratic Party hero Woodrow Wilson, led the repression.

Palmer picked 24-year-old J. Edgar Hoover to head the newly formed General Intelligence Division (GED) of the Justice Department's Bureau of Investigation. The GED's task was to investigate, infiltrate and destroy radical groups. Fifty years later Hoover was still at it, with the Counter-Intelligence Program (COINTELPRO) against civil rights, Black Power, Puerto Rican Nationalist, Native American, antiwar, feminist, environmental and socialist groups.

Activists and the Surveillance State examines the experience of activists with surveillance, political policing and resistance. It deals only in passing with digital surveillance, but the traditional methods of observation, infiltration, agents provocateurs, arrests, interrogation, torture, trials, prison and assassinations are even more effective, if also more labor-intensive and expensive.

The book consists of eleven essays. The first two analyze the surveillance state not as an aberration, but as a "rational" (from the capitalists' standpoint) development of the capitalist state. Exploitation, oppression, repression.

The following eight essays, present case studies from the U.K., Mauritius, South Africa, the United States, Australia, the Canadian state, and New Zealand. The final essay argues for continued research into and exposure of corporate and state spying and political policing.

It is well worth reading for activists experiencing or thinking about what Choudry describes as "the sharp edge of state power."

Permanent Record

Edward Snowden was born in 1983, the year the internet was born, as the Defense Department

separated its military network from the public one. He came from a military and government family. His father was a Coast Guard officer, an engineer, and his maternal grandfather a Coast Guard rear admiral.

His ancestors had served in every war the United States fought. His mother worked for the government. Snowden grew up with a strong sense of duty, but also with a sense of justice. His family served their country because it was just.

As a boy, Snowden was quite good with computers, which led him into the world of online hacking, not for money or malice but for the fun of it. He saw no conflict between his hacking and his sense of duty. His hacking uncovered inconsistency, incompetence, irrationality and hypocrisy. But he maintained his sense that sometime, somehow, someone with good intentions and smarts would intervene to put matters right.

Snowden enlisted in the army after 9/11, continuing the family tradition. He was injured in basic training too badly to serve in combat. Rousted out of the army, he decided to join the CIA, NSA or some other agency of the intelligence community. But Congress wouldn't approve hiring more government workers or raising their salaries and instead approved contracting on a dodgy cost-plus basis.

So Snowden got a job working nominally for Dell but really for the IC. He became a systems administrator. His job was to make sure that all the databases in his area were up and running and communicating with each other.

In the course of his work he began to realize that the IC had much more data than made sense if it was engaged in targeted surveillance for national security. Without public knowledge or legal authorization or oversight, the IC was engaged in mass surveillance.

He was torn between duty to the ideals that had brought him to the IC and his own comfort and safety. He had work that challenged him and paid well. He was living happily with Lindsay Mills, the love of his life. Why rock the boat?

As we know, Snowden decided to rock the boat, or rather blow the whistle. He copied and encrypted a huge trove of data which proved that the U.S. government was engaged in mass surveillance of its citizens and most of the online world.

He got the data to journalists Glenn Greenwald, Laura Poitras, and Ewen MacAskill, and they published stories in The Guardian and The Washington Post. Other media picked up the story.

After a dramatic international odyssey, Snowden and Mills are living in political exile in Moscow. Not the happy ending they deserve, but they are heroes to those who care about democracy.

Beyond Surveillance

What can activists do to stop or limit corporate and government spying? The article on Cambridge Analytica cited above has some suggestions about protecting yourself on the internet and promoting noncapitalist internet alternatives. Probably the most important of these online activist sites is the Electronic Frontier Foundation (https://www.eff.org).

But these are something like recycling and promoting community recycling to fight climate change — important, but far from sufficient to solve the problem.

Stopping or significantly curtailing surveillance would require a movement far beyond what exists

now. The movement would have to link up with other movements, since working people struggling to support themselves and their families, pay debts, and enjoy limited time off are not immediately going to see the need to mobilize to stop targeted advertising or what the IC euphemistically calls "bulk collection" of data.

They'll see the need to mobilize against surveillance when it affects them, when they're blacklisted by employers for union activity or targeted for protesting police violence, immigration raids, attacks on abortion clinics, or environmental destruction.

The ongoing demonstrations in Hong Kong show how connections can be made. The demonstrators took to the streets to protest inequality, corruption and rollbacks of democracy. The police attacked them, so they learned that they had to fight the police too.

The police used surveillance to identify protestors, so they learned to smash CCTV cameras and to wear masks. The government prohibited the wearing of masks, so they had to fight that too. The connection was made.

The three books reviewed above expose corporate and state surveillance. They suggest a world in which technology would be used not to spy on workers, but to make work easier, less time-consuming, more flexible, more engaging, not to market whatever the corporations want consumers to buy, but to make consumption more satisfying, more fulfilling, less wasteful. They invite resistance today to bring that future forward.

Peter Solenberger

P.S.

Solidarity

https://solidarity-us.org/atc/205/surveillance-capital/

The Age of Surveillance Capitalism:
The Fight for a Human Future at the New Frontier of Power
By Shoshana Zuboff
New York: Public Affairs/Hachette Book Group, 2019, 704 pages, $38 hardcover.

Activists and the Surveillance State:
Learning from Repression
Edited by Aziz Choudry
London: Pluto Press, 2019, 264 pages, $29 paperback.

Permanent Record
By Edward Snowden
New York: Metropolitan Books/Henry Holt and Co., 2019, 352 pages, $30 hardcover.