The coronavirus pandemic highlights the need for a surveillance debate beyond 'privacy'

May 25 2020, by David Lyon

Governments are implementing surveillance technologies to monitor and control the spread of COVID-19. Credit: Shutterstock

The coronavirus pandemic has stirred up a surveillance storm. Researchers rush to develop new forms of public health monitoring and tracking, but releasing personal data to private companies and governments carries risks to our individual and collective rights. COVID-19 opens the lid on a much-needed debate.

For example, Google and Apple teamed up to offer privacy-preserving contact-tracing help. The scramble for data solutions is well-meaning, but whether they work or not, they generate risks beyond narrowly-defined privacy.

Everyone has extensive digital records—health, education, employment, police contact, consumer behaviour—indeed, on our whole life. Privacy is much more than shielding something we'd rather not share; surveillance also affects our chances and choices in life, often in critical ways.

Early computerization obliged governments to see that regulation was needed as personal data was collected for more and more purposes. At first the data came from credit cards, driver's licences and social insurance; today it's constant device-use. But privacy regulation alone can't keep pace with today's supersystems for data collection, analysis and use that generate the kind of negative discrimination that demands data justice.

Surveillance and profit

Shoshana Zuboff's book *The Age of Surveillance Capitalism* is making headlines for its close analysis of how Google achieves its surveillance, why and with what consequences. Zuboff insists that a new mode of economic accumulation has been rapidly emerging ever since internet-based platforms—led by Google—discovered how to monetize the so-called "data exhaust" exuded by everyday online communications: searches, posts, tweets, texts. Beyond the loss of privacy, she sees the destruction of democracy and behavioural modification, citing a former Facebook product manager who says the "fundamental purpose" of data workers is to influence and alter people's moods and behaviour.

One cannot miss Zuboff's cri de coeur and its scathing rebuke to the

"radical indifference" of these platforms. But what will it take to persuade us that today's surveillance has become a basic dimension of our societies that threatens more than personal privacy? Surveillance is complicated, arcane and apparently out-of-control but those don't excuse our complacency. Rather, they're reasons for digging into some of the main dimensions of surveillance, prying open black boxes and reasserting human agency.

Let's disturb some common assumptions that surveillance is about video cameras, state intelligence and policing, producing suspects and challenging privacy. Google assuredly does surveillance, which is commonly defined as "any focused, routine, systematic attention to personal details, for the purpose of control, influence or management."


633
HAUTEUR LIBRE 4 .420 m / 14' 6"
2

Personal devices — mainly smartphones — provide a way to constantly track and monitor our movements, habits and consumption patterns. Credit: Guillaume Bolduc/UnSplash

It's not just CCTV cameras, it's also smart devices

Yes, it's our laptops, phones and tablets. Surveillance is now digital and data-driven.

For too long, the stereotypical icon of surveillance has been the video camera. The French roots of the word surveillance means to "watch over," which is what cameras do. And these are becoming smarter, when enhanced by facial recognition technology.

Clearview AI, for instance, scrapes billions of images from platforms such as Facebook or Google, selling services to major police departments in the United States and, until recently, Canada.

But today, what deserves to be the stereotypical icon is the smartphone. This, above all, connects the individual with corporations that not only collect but analyze, sort, categorize, trade and use the data we each produce. Without our permission, our data are examined and used by others to influence, manage or govern us. Data analysis enables prediction—and then "nudging"—of specific population groups to buy, behave or vote in hoped-for ways.

It's not just the state, it's the market

While the state and its agencies often overreach through intelligence and

policing strategies, it is the market and not the state that holds the cards in the surveillance game.

Few noticed in the early 20th century that department stores, like Syndicat St-Henri in Montréal, kept detailed customer records, giving or withholding credit according to their status.

A pivotal moment was 9/11 when high-tech companies, craving customers after the dot-com bust, offered their services to government.

Today, our massively augmented data profiles indicate value to businesses. Those data are valuable to others too, like election consultants.

Surveillance is for sorting

Surveillance and suspects once belonged neatly together—those who were thought to be miscreants were watched. But in this big data era, all personal details are up for grabs.

What French sociologist Jacques Ellul worried about in 1954 has transpired: the police quest for unlimited information makes everyone a suspect. But Ellul never guessed how this could morph into a global network of systems, far beyond policing, in which everyone becomes a target.

But everyone is not targeted in the same way. Surveillance—whether for welfare, commerce or policing—sorts populations into categories for different treatment. This social sorting works in marketing to organize consumers. In China today, social credit systems are used by the government and commerce to monitor and rank citizens' behaviour and social capital.

This is not only about privacy, it's also about data justice.

Surveillance is a challenge to digital rights, because it is based on fundamental inequalities and unfair practices. Vulnerable groups discover their disadvantages are deepened.

Privacy laws rightly protect an individual's right to privacy of movement, home and communication in a democratic society. But we need a radical new direction, prompted by our knowing how data analytics, algorithms, machine learning and artificial intelligence are reshaping our social environment. The analysis and uses of the data have to be addressed, invoking new categories such as digital rights and data justice.

Surveillance challenges

Just scratching the surface of 21st-century surveillance reveals how vastly things have changed. The landscape of surveillance has shifted tectonically from following suspects, watching workers and classifying consumers to monitoring and tracking everyone—now for public health—on an unprecedented scale.

Privacy is undoubtedly a casualty, and so are basic freedoms of democracy, expectations of justice and hopes for social solidarity and public trust. These demand serious attention, not just from policy-makers and politicians, but from computer scientists, software engineers and everyone who uses a device.

Provided by The Conversation