SURVEILLANCE BEYOND PRIVACY

David Lyon | June 17, 2020

The COVID-19 pandemic is stirring up a surveillance storm, both in terms of the research energy released and of the personal-data-and-public-trust questions thrown up. Researchers rush to develop new forms of public health monitoring and tracking but releasing personal data to private companies and governments carries risks to both personal and collective rights. COVID-19 opens the lid on a much-needed debate.

For example, Google and Apple have offered geolocation data to health authorities, for contact-tracing. And this, with other schemes, is widely debated. The scramble for data 'solutions' is, one hopes, well-meaning, but whether they work or not, they generate risks beyond a narrowly-defined 'privacy.'

Everyone has extensive digital records—on our health, education, employment, police-contact, consumer-behaviour—indeed on our whole life. These are constantly being pulled together in new ways and we can only hope that those handling them respect our 'privacy.' But these data also affect our chances and choices in life, often in critical ways.

Shoshana Zuboff's big book on *The Rise of Surveillance Capitalism* has been making headlines for its close analysis of just how Google achieves its surveillance, why, and with what consequences. Her thesis is that nothing short of a new mode of economic accumulation has rapidly been 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. The impact—loss of privacy, behavioural modification and the destruction of democracy—is dire.

Whatever one makes of the fine details of Zuboff's work—it is sparking debate!—one cannot miss the *cri de coeur* and its scathing denunciation of the "radical indifference" of platforms as currently constituted and of their "doctrines of inevitability." But what will it take to persuade us that today's surveillance has become a basic dimension of our societies and that it threatens more than my 'personal privacy'? Undoubtedly, it's complicated, arcane and apparently out-of-control, but those are hardly excuses for complacency. They're reasons for digging into some of the main dimensions of surveillance, prying open black boxes and reasserting human agency.

Four jolts

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

RSC SRC

It's not just CCTV cameras, it's smartphones – surveillance is digital, data-driven.

For too long, the stereotypical icon of surveillance is the ubiquitous surveillance camera and this makes sense. The French root of *surveillance* means to 'watch over' and that's what cameras do. They become increasingly smart, when enhanced by facial recognition technology. Clearview AI, for instance, scrapes billions of images from platforms such as Facebook or Google and sells their matching services to major police departments in the US—and until recently, in Toronto.

But today, what *deserves* to be the stereotypical icon is the smartphone. This, above all, connects individuals with corporations that not only collect but analyze, sort, categorize and use the data constantly exuded by that individual. This happens without our say-so, to influence, manage or govern us. Data analysis enables prediction, then 'nudging' of specific population groups to buy, behave or vote in hoped-for ways. The flow of data through personal devices powers surveillance today.

It's not just the state, it's the market – surveillance is for influence, profit-driven

While the state and its agencies *do* all-too-often overreach themselves through no doubt well-intentioned intelligence and policing strategies, the market, not the state, holds the key cards in the surveillance game. State surveillance still menaces democracy and freedom to differing degrees around the world. Aspects of COVID-19 surveillance may cross that line, too. But the state is no longer alone.

Few noticed in the early C20th that department stores, like *Syndicat St Henri* in Montreal, kept detailed customer records, giving or withholding credit according to their status. Today our profiles indicate our 'lifetime value' to businesses but they also propel advertising to us, subtly influencing our behaviours and practices, with limited regulation.

A pivotal moment was 9/11 when high-tech companies, craving customers after the dot-com bust, offered their services to government. Such 'public-private' partnerships are commonplace today.

Now, our massively augmented data-profiles indicate our 'lifetime value' to companies. And those data may also be valuable to others, too, such as 'election consultants' – think Aggregate IQ, and Cambridge Analytica.

It's not just suspects, it's everyone – surveillance is for sorting, reputation-driven

'Surveillance' and 'suspects' once belonged neatly together – those thought to be miscreants were watched. What French sociologist Jacques Ellul worried about in 1954 has transpired: the police quest for more and more 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. The systems in question, whether for welfare, commerce or policing, sort populations into categories for different treatment, rather like the emergency room triage. This 'social sorting,' works in marketing to slot people into niches of where you live—find out for yourself by looking it up! Those device-data make up your profile which to companies and others is your reputation. In China today, growing social credit systems are run by government; ours, by companies.

It's not just privacy, it's data justice

Early computerization obliged governments to see that regulation was needed as personal data were 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.

Privacy laws address bodily, spatial and especially informational and communicational privacy and to support the freedoms one expects in a democracy. They have achieved much but we are still left very vulnerable. A radical new direction is needed, prompted by our knowledge of the ways that data analytics, algorithms, Machine Learning and AI are reshaping our social environment. Not just the *collection*, but the analysis and uses of the data have to be addressed, invoking new categories such as digital rights and data justice.

Surveillance challenges

Merely scratching the surface of C21st 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 but so also 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—in fact from everyone who uses a device

The stakes are high, but the future is not foreclosed.

The Royal Society of Canada has established the Infoveillance Working Group to consider the implications of surveillance, data, privacy and equality. The working group has begun work in analyzing a transition from individualistic notions of 'privacy protection' to the arrival of surveillance capitalism, which refers to an economic system of accumulation based on the commodification of personal data. Surveillance capitalism has many features including datafication (social action transformed into quantified data), dataism (a naïve belief in the capacity of data to solve human problems), dataveillance (using data for surveillance of populations and individuals), and discriminatory profiling (with particular implications for people from already-marginalized communities).

The Working Group Members are: Jane Bailey (University of Ottawa); Benoît Dupont (Université de Montréal); Anatoliy Gruzd (Ryerson University); and David Lyon (Queen's University)