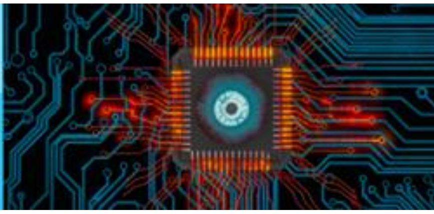
INFOVEILLANCE WORKING GROUP

COVID-19: The Potential Abuses of Personal Data Surveillance



Benoît Dupont | June 24, 2020

If we are not careful, our right to privacy might well become one of the numerous collateral victims of the COVID-19 pandemic.

To reconquer our temporarily suspended freedom of movement and protect the public against a second wave of infection, we need put in place the basic elements of a dedicated public health monitoring infrastructure.

This infrastructure would include a series of personal data collection devices, such as smart phones, surveillance cameras, connected bracelets, robots and drones. Thanks to innovations made in recent years in the areas of cloud computing, telecommunication networks and artificial intelligence, mountains of data generated by those devices can now be stored for an indefinite period of time. This data can be analysed in real time by the powerful surveillance algorithms executed by tracking and facial recognition application

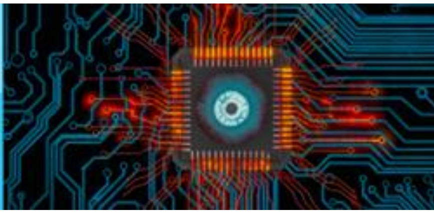
As a criminologist specializing in the study of digital transformation and adaptation of social control mechanisms, I have been studying for several years the new forms of surveillance used by governments and private companies, as well as the forms of resistance that can oppose them.

The temptation of techno-solutionism

The technologies that support this infrastructure are not new, and their implications extend beyond those of those concerning the defense of our right to privacy, as my colleague David Lyon has noted in these pages. Rather, their development has accelerated in recent years, under the pressure of surveillance capitalism, which seeks to translate every human experience into information that can create market value for the companies who own them and know how to generate profit from them.

In the current exceptional situation, where the pandemic has already caused over 350,000 deaths worldwide and where the richest countries' health systems have suffered numerous organizational failures, the use of surveillance as a means to manage this health crisis is quite attractive. Indeed, how can we not succumb to the luring sirens of digital tools that promise to automatize the detection of suspicious cases and to slow down — or even completely stop — the spread of the virus, which would allow us in turn to avoid a total collapse of the economy?

This temptation of "techno-solutionism", which relies on technical solutions to solve even the more complex social problems, carries significant risks. Is the collective fear generated by the ravages of the virus pushing us into an era of total surveillance from which it will be impossible to escape when the crisis is over and which will forever undermine our basic rights?



The ubiquity of health surveillance tools

While we wait for a vaccine to be developed, an increasing number of countries and companies are mobilizing a vast array of surveillance technologies designed to help track infected people and enforce social distancing rules. Such applications are drawing attention from privacy advocates, but they represent only the tip of the iceberg of health surveillance.

Asian countries, which have initially had the best results in containing the virus, have quickly relied on a massive access to the cellphone data of their whole populations: South Korea has put in place a data-sharing system involving 28 organizations, including the three main telecom operators and 22 credit card companies, that can follow the movements of an infected person and their contacts in less than 10 minutes.

People quarantined in Hong Kong are required to wear electronic bracelets connected to their smartphones, which ensures they do not leave their residence and which alerts the police as soon as a suspicious movement is detected. In Singapore, infected people must answer text messages several times a day, which reveals their geographical location.

In China, an application mandatory in over 200 cities and designed by an affiliate of the e-commerce company Alibaba, assigns a colour code (red, yellow or green) to the assumed contagion risk posed by each user based on data relative to their residential address, their life habits, their self-declared symptoms, etc. The data is routinely shared with the police. The speed at which such a technical solution was implemented is a direct result of the systematic citizen tracking and surveillance initiatives taken by the Chinese government as part of its social credit system.

As of mid-May, some 50 tracking applications were available in 30 countries. However, a quarter of those have not yet adopted privacy protection policies and 60% have not implemented specific anonymity protection measures.

In a more radical fashion, Israel mobilized the surveillance capabilities of its internal intelligence service, the Shin Bet, in order to identify those who have been in contact with infected patients. Using GPS data provided by mobile phone operators as part of its counter-terrorism apparatus, the Shin Bet has located approximately 4 000 people which have subsequently tested positive, inaugurating a hybrid form of surveillance combining national security with public health objectives.

A genuine technology arsenal

Companies that want to put their employees back to work and welcome back their clients are also contributing to this “care-veillance” escalation.

Start-ups specializing in artificial intelligence are proposing video-surveillance systems integrating social distancing detectors, which can automatically detect any situation where people come within less than two meters one from the other. Others integrate thermal sensors to their facial recognition technologies to measure continuously, and without physical contact, the body temperature of employees when they move about the premises of the company.

Public and private transportation operators are testing facial recognition devices to check whether their users and drivers are wearing their masks. Manufacturing companies are testing smart watches or badges that can alert users when they are violating social distancing rules and help build employee risk profiles.

Drones and robots finally complete this technology arsenal. Several Italian, Spanish, French and U.S. cities have deployed thermal sensor equipped drones that fly over public spaces to detect people with fever or who might violate confinement rules. Those devices can even interact with people through speakers.

Always up-to-date in the field of surveillance technology, Singapore is experimenting with the use of robot dogs equipped with cameras and speakers to enforce social distancing rules in public parks.

Regulating the creeping implementation of a total surveillance infrastructure

Taken separately, each of these surveillance technologies provides a concrete solution to a new and devastating health threat. Taken as a whole, however, they are tracing the contours of a future world where the ubiquity of benevolent surveillance will infiltrate even the most hidden depths of our behaviours and habits.

It is also likely that this care-veillance will contribute to perpetuate numerous forms of discrimination, with its use of risk profiles, the criteria of which will remain opaque. This will certainly accentuate the vulnerability of the most marginalized groups of our society.

Far from being a plot implemented by dark forces, the convergence of increasingly invasive surveillance technologies is rather a reflection of our insatiable thirst for security and our blind trust in the power of technology to reduce uncertainty.

But this scenario is not an inevitable fate and our assessment of the situation should not leave us paralysed and helpless, quite the contrary. In view of the real risk of seeing this surveillance infrastructure strengthen its hold well beyond this pandemic situation, it has become urgent to debate and get mobilized in order to establish transparent and stringent rules that would limit the risks it imposes on our individual liberties and our social cohesion.

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).