The Political Economy of Communication
9(1), 4–21
© The Author 2021
http://www.polecom.org

Pandemic Lessons: Total Surveillance and the Post-Trust Society

Mark Andrejevic, Monash University, Australia

Zala Volcic, Monash University, Australia

Keywords: COVID19; pandemic; surveillance; trust; biometrics; environmentality

Abstract

As the first global pandemic of the digitally networked era, COVID-19 helped unfold an emerging surveillant imaginary: one in which automated, real-time tracking might keep pace with the threat of viral infection. Even more than the previous globally resonant event that helped reconfigure this imaginary—the 9/11 attacks—the pandemic highlighted the ubiquity of risk and the multiplicity of potential threat vectors. The threat of contagion was figured as coextensive with the realm of the social: the entire sphere of human circulation. Monitoring and preventing or pre-empting viral spread, then, required the mobilization of a surveillance apparatus with a similar reach: one able to embrace the full range of human activity as comprehensively as possible. This imperative spawned a range of approaches to monitoring and tracking that are likely to outlive the pandemic. They promoted themselves in the name of convenience, security, and profit. The technologies that enable such forms of surveillance are, of necessity, automated, because they seek to capture information on a scale that would be impossible for unaided humans. In this respect they partake of what might be described as a post-panoptic logic—one that dispenses with the parsimony of the Panopticon and, at least in some respects, with the forms of subjectification it envisioned. This article draws on examples of environmental surveillance mobilized during the pandemic to explore the dimensions of the diagram of post-panopticism. It argues that the forms of monitoring that were developed during the pandemic are likely to outlast it.

As was evident with the suicide bombings of 9 September 2001, the COVID-19 pandemic highlighted what might be described as the risks inherent to societal interdependence at the global level. In the former case, the potential ubiquity of the terrorist threat provided a forcible reminder of the indispensable relations of trust without which society cannot function—and which served, simultaneously, as vectors of vulnerability. Similarly, in the subsequent case of the pandemic, the threat of contagion was coextensive with the realm of the social: the entire sphere of human circulation. In both cases the prospect of surveillance enhanced by recent technological developments promised to address the inherent vulnerabilities of the social. However, the pandemic pressed closest to the body, and inaugurated the development of a range of technologies for granular surveillance that are likely to outlast the contemporary crisis. The ready repurposing of surveillance technologies for pandemic management builds on existing trends in the current surveillance economy, which relies on data collection as a means of rationalizing the deployment of resources and managing risk (Amoore and De Goede, 2005). The pandemic response helped accelerate the penetration of the surveillance economy into the realm of health care, a lucrative frontier for Silicon Valley and its adjuncts (Yeo, 2021). In this respect, the mobilization of digital monitoring and tracking technology in response to the pandemic is continuous with the ongoing expansion of the surveillance economy. Our analysis of the relationship between increasingly granular forms of real-time monitoring in the name of public health, then, intervenes in contemporary critiques of the political economy of digital surveillance and the interactive infrastructures that enable it.

This article, therefore, draws on the example of pandemic surveillance technologies and practices to explore the emerging regime of environmental-level monitoring, and the forms of pre-emption and governance with which it is associated. The infrastructure for this level of monitoring was in development long in advance of the pandemic, which provided a fresh set of imperatives for putting it to use, that is, tracking circulation at the individual level, detecting symptoms from a distance, enforcing quarantine restrictions, and verifying vaccine status. Monitoring at this level that is comprehensive enough to cover the movement of the virus is, of necessity, reliant on automated processes and networked sensors. The possibility of envisioning such a comprehensive level of response, in other words, is reliant upon the fact that COVID-19 was the first pandemic that could be slotted into the surveillance logic of the networked, digital era. It is perhaps not surprising in this regard, that conspiracies around the buildout of cellular telephone networking attached themselves to the pandemic. Such paranoiac fantasies amount to a pastiche of cognitive mapping—a warped recognition that there is, indeed, a connection between biopolitical forms of control and the burgeoning digital infrastructure.

The broader claim to make about the development of environmental surveillance and governance is that it provides a technological fix for the version of primary individualism that its automated systems promote through a data-driven economy of targeting and customization. Thus, the article closes with some reflections on how responses to the calls for social solidarity in the face of contagion are symptomatic of the version of sociality promulgated on commercial media platforms.

Ubiquitous threat and comprehensive surveillance

The notion that consumer-facing forms of data collection might help address risk and counter potential threats was boosted by responses to the 9/11 attacks in the United States. Shortly after the attacks, the Defense Advanced Research Projects Administration developed its plan for a "database of databases" called Total Information Awareness, housed in its own sub-department, the Information Awareness Office (Rotenberg, 2006). The premise of the program, as outlined in a report to Congress was to, "to use data mining technologies to sift through personal transactions in electronic data to find patterns and associations connected to terrorist threats and activities" (Stevens, 2003: 2). As the original proposal for the plan stipulated, collecting and aggregating information at this scale would require, "a new infrastructure and new information technology" (Defence Advanced Research Projects Agency, 2002, 3). The goal was to bring together existing intelligence databases with publicly available transactional data, as well as commercial databases including records of credit card purchases, car rentals, air travel, and so on. The program also outlined plans for the development of new sensing infrastructures to increase data collection capacity, including systems that it described as "Human ID at a Distance." (Phillips, 2002). This program focused on biometric identification systems for passive, long-range identification to track individuals and provide "early warning support for force protection and homeland defense" (Phillips, 2002). The goal was to supplement transactional and communication data with the ability to track people's movements and behavior via networks of "smart" camera systems. We might describe this as a means of combining stored data from both online and offline sources to match records with bodies. At the same time, a variety of initiatives for automated and crowdsourced surveillance emerged in the post-9/11 era, including systems for monitoring vulnerable infrastructure such as ports, dams, and reservoirs (Berinato, 2003; Linn, 2011). This was a pre-smartphone era, so the forms of app-based monitoring that emerged in the wake of the pandemic were not yet available, but homeland security and intelligence agencies internationally launched programs mobilizing members of the public to photograph and call in anything that looked suspicious to them. The tagline in the US was, "if you see something say something." The message to the public was that potential vectors of threat were so broadly dispersed throughout the realm of the social that it would be impossible for conventional forms of policing to monitor them without assistance: the populace had an important role to play in safeguarding its own security. This message complemented the emerging interactive ethos of the online economy; networked interactivity made crowdsourced securitization a possibility. People could, for example, monitor soft targets via webcam while they were browsing online, and they could put to use the networked cameras they carried around with them for extending the monitoring gaze of the security apparatus (Berinato, 2003).

The climate of generalized suspicion associated with mobilization of the populace coincided with recognition of the fact that a society reliant on shared trust could be exploited. Because we cannot monitor everything all the time for ourselves, we find ourselves irreducibly reliant on ubiquitous forms of trust that often pass unremarked until they are violated. We have to trust, for example, that people in the seat next to us in planes will not do anything dangerous, that the agencies monitoring the water supply are doing their job, that the general public is not interfering with exposed fruits and vegetables in produce markets. Even driving down the street, we trust that others will voluntarily comply with the traffic signaling system and not turn their vehicles into weapons of mass destruction.

Terrorism preyed on that trust, turning it to the ends of asymmetric warfare: when trust is violated, vehicles can be spontaneously transformed into weapons, water supplies and food chains can become vectors of attack. Terrorism is more than the threat of spectacular violence visited upon vulnerable members of the civilian population; it is simultaneously a threat to social trust, and thus to the social fabric. The stimulation of surveillance it inaugurates has the potential to further erode this trust insofar as generalized surveillance invites both the intelligence apparatus and the populace to treat anyone as a possible suspect: this is the message of the "see something say something" campaign. As the surveillance studies scholar David Lyon puts it, "We fall over ourselves trying to make life-with-fear liveable, but each attempt produces more risks, more fears…Categorized innocents are now at risk and in fear in an ironic parody of terrorism" (as cited in Bauman and Lyon, 2013, 89).

Generalized surveillance participates in a self-stoking cycle of mistrust. As the sociologist Zygmunt Bauman observed in his discussion of "liquid surveillance," "Having ingested and assimilated the Weltanschauung of the ubiquity of danger, of the comprehensiveness of the grounds for mistrust and suspicion, of the notion of safe cohabitation as conceivable solely as an artefact of continuous vigilance, we have become dependent on surveillance being done and being seen to be done" (as cited in Bauman and Lyon, 2013: 90). Consider, for example, the advice given to the Australian public by a former intelligence official after the London terror attacks in 2005: "What the public needs to be looking for, what the trained officials need to be looking for, is somebody standing in the corner, somebody who's holding onto their backpack, somebody who looks really concerned and anxious…Somebody who's clean shaven or somebody wearing a vest that looks so unusual—the jumper is bulky, the vest is bulky not fit with other clothing and Middle Eastern appearance" (ABC News, 2005). The sheer incoherence of the advice (someone looking "concerned and anxious" might well be the person who is meant to be on the lookout for concerned and anxious people) suggests the universalization of suspicion (albeit with ethnic overtones). The only way to manage this level of potential threat—and thereby to dispense with the vulnerability that accompanies our reliance upon trust—is through generalized surveillance.

The US Total Information Awareness program received bad publicity and was eventually shuttered, although the approach to dataveillance it outlined continued apace, as demonstrated by the Snowden leaks (Greenwald, 2014). The model of using automated systems to collect and organize as much data as possible developed alongside the emerging surveillance economy. Indeed, the CIA's chief intelligence officer invoked the model of Google when explaining the agency's new surveillance strategy: "To collect everything and hold on to it forever" (Sledge, 2013). He differentiated this from the traditional "search and winnow" model, which relied on more targeted and selective information collection and retention. As in the case of e-commerce, the shift correlated with a focus on generalized pre-emption: with enough data the numbers might point to who the suspects should be, but that meant gathering data about targets and non-targets alike to discern the patterns that might help differentiate between the two.

Pandemic surveillance

The responses to the 9/11 attacks focused on individuals who sought to exploit social trust as a point of vulnerability, whereas in the case of the COVID-19 pandemic the virus came to stand for the threat of sociality itself. The biopolitical stage for the pandemic had been set, as it were, by the framing of terrorism in biopolitical terms as a social pathology and its spread in the Internet era as a form of virality. As the media commentator Douglas Rushkoff put it shortly after 9/11: "terrorism isn't so much an act of war as it is a virus—a very contagious set of destructive commands. It depends on our highly networked 'media space' for its transmission and exploits our society's immune deficiencies in order to find candidates to carry out its orders" (Rushkoff, 2009).

In the wake of 9/11, there was much talk of bioterror, and the Department of Homeland Security created a series of public campaigns designed to train people how to respond to a range of attacks, including those deploying biological and chemical weapons. The conservative Senator Bill Frist wrote a book on bioterrorism that provided a fitness and health regime designed to make people less vulnerable to biological agents (Frist, 2002). In a speech to religious broadcasters, President George W. Bush grouped together human and viral threat: "Chemical agents, lethal viruses and shadowy terrorist networks are not easily contained" (Dionne, 2003).

The equation was clear, not only can terrorists avail themselves of biological weapons, but terrorists are social pathogens. Such formulations rehearse Michel Foucault's (2008) analysis of the relationship between racism and biopower: the way for a regime that governs, ostensibly, in the name of life to justify killing is to frame it as a means of protection against a biological threat. For this reason, he argues that racism is integral to biopower, because it introduces a distinction between those who can be classed as a biological threat and those who constitute the population to be protected from this threat: "That is the first function of racism [in a biopolitical context]: to fragment, to create caesuras within the biological continuum addressed by biopower" (255). The fact that race played a central role in the war on terror bolsters this point.

It is suggestive that race also had a central role to play in the response to COVID-19, as evidenced by Donald Trump's insistence on calling it the "Chinese virus" and in the associated increase of hate crimes toward Asians in various countries, including the US (NPR, 2021). In contrast to the war on terror, the "war" on the virus (as declared by, among others, the Secretary General of the United Nations (United Nations, 2020)) is not explicitly directed toward a particular human foe. Although the politicized response has resulted in scapegoating, with the poor, immigrants and people of color being demonized for suffering and dying disproportionately), the main targets of those practices that enable viral spread. In a sense, the focus is sociality: the forms of circulation, interaction, and transaction that bring people together in ways that contribute to contagion.

The role played by surveillance in this context is to secure circulation and the forms of sociality with which it is associated. The pandemic provided a stark reminder of the economic impact of stasis. Restrictions on circulation coincided with the threat of an economic downturn: shops closed, airplanes mothballed, venues shuttered. The political fallout generated debates that pitted the health benefits of quarantine against its economic costs. The mobilization of biometric monitoring offered a response to this perceived trade-off: circulation could be reinstated if it was coupled with comprehensive monitoring to track contacts, monitor social distancing, and detect emergent symptoms. The coupling of identification and symptom monitoring at a distance became a strategic tool underwriting the biopolitical imperative of maximizing the productive powers of the population, while placing differential restrictions on that same population relative to disease prevalence, risk and proximity. This imperative relied, as Foucault (2007) notes on, "making possible, guaranteeing, and ensuring circulations: the circulation of people, merchandise, and air…" (51).

Predictably, logistics associated with the war on the virus took on many characteristics from the war on terror. In both cases, everyday forms of circulation and interaction served as vectors of risk and potential threat. Underlying forms of social trust—or lack thereof—represented zones of vulnerability. The invisible character of the virus and the lag in the appearance of symptoms meant that anyone might be a possible carrier (risk or threat). Lack of clarity over the mode of transmission meant that the object world became a threat-laden environment: anything that might have come into contact with some form of contamination was cause for concern. The result was the ongoing cleansing and disinfection of the object world: groceries, doorknobs, lampposts, park benches and entire markets and buildings.

Circulation and its perils provided the background condition for the development of monitoring, tracking, and surveillance "solutions" enabled by networked digital technologies. As soon as physical proximity came to be viewed as a threat, technologies that provided "at-a-distance" services were enrolled to simulate and replace face-to-face activities and thus reduce the potential for viral contagion. For many, as distance learning, telecommuting, and teleworking became a necessity, contactless and touchless interactions were the order of the day. Amazon and other online retailers saw their businesses boom—as did other purveyors of services at a distance, from "telehealth" to video-conferencing platforms. Alongside these conveniences emerged strategies for tracking and governing both individuals and populations "at-a-distance" in the name of productivity, health, and wellbeing. On the one hand, there were remote employee and student monitoring to track how and when work was taking place, and, on the other, remote symptom detection, contact tracing, and social distance monitoring to manage viral spread. Similar technologies were used to secure those forms of circulation that remained and to facilitate the return of those that were curtailed. The social-distancing imperative became a selling point for the emerging biometrics industry, which mobilizes the promise of efficient, mass monitoring of bodies and faces at-a-distance. The pandemic served, in other words, as an alibi for extending online forms of monitoring and tracking into the physical world. The result, we argue, has been the development of infrastructures for environmental governance. We will explore their traits through an examination of pandemic monitoring practices that are likely to outlive the current crisis. The following sections consider some of the technologies that advance the logic of redoubling the social in monitorable, trackable form. The goal is not to provide a comprehensive list of tracking technologies but to consider their various dimensions, including high-resolution distance monitoring, granular mobility monitoring, and passive identity linking.

High-resolution distance monitoring

Despite recent attention given to the notion that surveillance is a novel add-on to capitalism (Zuboff, 2019), we note that industrial capitalism has, from its inception, relied upon techniques for monitoring and supervision. The move from a piecework system to an hourly wage relied on the ability to subject employees to comprehensive monitoring—as did the development of systems for increasing worker productivity such as Taylorism, Fordism, and, in the interactive mode, Toyotism (Andrejevic, 2007; Steinberg, 2021). This history reveals the ongoing drive for greater worker surveillance—limited by the cost of supervision and by worker pushback (Antaya, 2015). The pandemic, however, facilitated a technological leap in the level of automated monitoring as a support for the widespread practice of responding to lockdowns by promoting telecommuting. If people were working at home, according to some employers, they should be willing to submit to enhanced monitoring regimes that might replicate (or extend) the level of supervision available in their office. In practice, however, the automated monitoring practices went far beyond typical workplace supervision, suggesting that the telecommuting rationale served as an alibi for the implementation of capabilities that supervisors may have long sought (although some workplaces have already implemented many of these technologies). According to the *Washington Post*, by the time the pandemic was only a few months old, "thousands" of companies were using, "monitoring software to record employees' Web browsing and active work hours, dispatching the kinds of tools built for corporate offices into workers' phones, computers, and homes" (Harwell, 2020). One company, for example, provided a monitoring solution that, "can be installed in a hidden way on workers' computers and creates a minute-by-minute timeline of every app and website they view, categorizing each as 'productive' or 'unproductive' and ranking workers by their 'productivity score'" (Harwell, 2020). The system also alerts managers to suspicious activity, which reportedly includes indicators that they might be looking elsewhere for work (as one might expect from people subjected to this kind of surveillance!). Other applications used for remote employee monitoring track keystrokes and take screenshots of workers' computers at random intervals, while engaging in real-time activity tracking (Chyi, 2020; Finnegan, 2020). Employers availed themselves of the fact that Microsoft 365 could be used to give, "managers an overall rating of their team's productivity by measuring things such as how many emails people are sending and who they are communicating with" (Connolly, 2020).

The deployment of such systems highlighted just how useful it is, from a surveillance perspective, to have workers tethered to computers for their jobs. Networked devices serve not just as tools for performing a variety of tasks, but as powerful interactive tracking devices—a lesson that we have been learning for some time in the realms of both consumption and production. Such tools obviate the need for trust. Surveillance promises to lower the risk of shirking or deception by tracking every action and movement of a worker. By contrast, the more managers rely on trust rather than direct supervision, or so the story goes, the more they open themselves up to being taken advantage of. Like the deployment of surveillance more generally, remote monitoring offers double objectives: it promises both a measure of security and the prospect of dramatic efficiency gains. In his classic exploration of management logic, Harry Braverman (1998) describes the alienation of planning from execution achieved by the collection and processing of data about production. Covert and passive tracking devices achieve what the first generation of scientific managers could only dream of—a worker-generated trove of detailed data about every employee's actions throughout the course of the workday, plus the processing power to make sense of it.

An additional set of monitoring technologies are being implemented to secure mobility within workspaces, such as warehouses and factories, which cannot pivot to telecommuting. Remote temperature monitoring and movement tracking has been implemented in some work sites to detect the early onset of symptoms and trace those who might have been in contact with contagious co-workers (Chyi, 2020). These technologies provide detailed information about which workers have been in contact with one another, a capability which doubles as a means of tracking labor organizers in the workplace. What emerges is a portrait of across-the-board forms of management and organization facilitated by generalized surveillance. Component features include efficiency, safety, security, productivity, and control enabled by the deployment of increasingly comprehensive and granular forms of monitoring.

Something similar has been taking place in the educational realm, inspired in part by the promise that detailed data about students can be used not just to tailor instruction but to enable remote learning. Universities have long been pursuing distance learning strategies as a means of expanding enrolments without the attendant costs of physical expansion (Cacault et al., 2021). The pandemic gave a big boost to distance learning as physical campuses closed down, leading educators scrambling for technologies that would enable remote instruction and testing. The result, in many cases, was technology that functioned a lot like the workplace surveillance systems, in some cases even more invasively (Andrejevic and Selwyn, 2020).

The popular meeting application, Zoom, for example, at one point included an attendee attention tracking function that notified hosts when meeting participants clicked away from the meeting window for more than 30 seconds (Amatulli, 2020). Exam proctoring technologies used a variety of sensors and tracking systems to protect against cheating: "One system, Proctorio, uses gaze-detection, face-detection and computer-monitoring software to flag students for any "abnormal" head movement, mouse movement, eye wandering, computer window resizing, tab opening, scrolling, clicking, typing, and copies and pastes. A student can be flagged for finishing the test too quickly, or too slowly, clicking too much, or not enough" (Harwell, 2020).

Such technologies, tellingly, replicated the fantasy of total classroom monitoring that only a few years earlier had been promoted in the name of providing students with a fully customized learning experience. In an article brimming with what now looks like an overwrought techno-optimism, the influential industry publication, *Education Week*, envisioned "classrooms outfitted with cameras that run constantly, capturing each child's every facial expression, fidget, and social interaction, every day, all year long" and supplemented with "infrared cameras, documenting the objects that every student touches throughout the day, and microphones, recording every word that each person utters" (Herold, 2016). These forms of tracking could be used in conjunction with "Fitbit-like devices that track everything from their heart rates to their time between meals" and "Chromebooks and learning software that track their every click and keystroke" (Herold, 2016).

Such descriptions cast a somewhat sinister light on the observation by media philosopher John Durham Peters that, "Digital devices invite us to think of media as environmental, as part of the habitat, and not just as semiotic inputs into people's heads" (Peters, 2015). This concept of environmental media leads directly to what we describe in the concluding sections of this article as environmental governance. If surveillance in the workplace envisioned the prospect of surveillance displacing trust and human oversight, this comprehensive level of student tracking anticipates the replacement of human instruction. No teacher could make sense of all of this data or provide highly detailed customized instruction to a classroom full of students simultaneously. The goal of such systems, put somewhat differently, is to displace social relations with automated forms of data collection, tracking, and processing, precisely because humans cannot process the sheer volume of information generated by the technology.

Granular mobility monitoring

The historical response to the plague, as Michel Foucault notes, was stasis: the attempt to restrict the forms of human circulation that are coextensive with contagion. As he puts it in his work on panopticism, the plague restrictions result in a "segmented, immobile, frozen space. Each individual is fixed in his place. And, if he moves, he does so at the risk of his contagion or punishment" (1975: 195). This response is certainly familiar to those who found themselves in hard lockdown during the pandemic. The familiar biopolitical-economic response to such measures was to assess the impact of stasis on economic activity and the resulting impact on physical and mental wellbeing. Managing the pandemic alongside the economy became, in many contexts, a question of considering what response might enable the shift to an endemic model, in which some level of secured circulation could be achieved. Quarantine, put somewhat differently, was implicitly framed as an anachronistic response—a technology for a different time. Feudalism may have been able to tolerate stasis and sustain homeostatic conditions, but capitalism depends on relentless growth and circulation, spurring the development of the statistical tools that constructed the population as an object of mathematical observation and intervention. Problems of "territory" (fixing and demarcating it) were supplemented by those of circulation: "allowing circulations to take place, of controlling them, sifting the good and the bad, ensuring things are always in movement, constantly moving around, continually going from one point to another, but in such a way that the inherent dangers of circulation are cancelled out" (Foucault, 2007: 37). Changing economic conditions leveraged the productivity of circulation, which helped fuel consumption and trade, but also exacerbated the risk and severity of contagion. It is a symptom of the neoliberal era that the biopolitical management of circulation devolved onto the commercial tech sector, providing opportunities for companies developing contact tracing applications, remote biometric monitoring systems, and telecommuting tools.

The shock of the COVID-19 moment is that it reintroduced the specter of plague-era quarantine in the context of existing forms of biopolitical governance that had become reliant on endemic strategies (e.g., vaccination and hygiene regimes and antibiotics). Biopolitics is not simply a discrete intervention at times of crisis, but an ongoing process of environmental engineering. The goal is not to improve the quality of life for any particular individual, but rather to treat the maximum of the population as a political and biological problem, against the background of datafication methods that are in turn conditioned by the economic imperative of stable growth.

Foucault situates the emergence of the population as a problem in the second half of the 18th century, but its ongoing salience is revealed by government responses to COVID-19. They highlight the relationship between biopolitical management of the population and economic performance. The significant contemporary development, however, was the introduction of networked digital devices to provide granular mobility tracking. Perhaps the first indication of this was the widespread use of contact tracing apps that could track who had been in proximity to whom. Some versions of the apps collected detailed location information that could be used to reconstruct people's movements throughout the course of a day. Others were used to determine whether people had breached quarantine restrictions by moving beyond the borders within which they had been constrained (Andrejevic and Selwyn, 2020; Kim, 2020). It is worth emphasizing that this level of granular mobility tracking is not novel; as smartphone users have known for some time, their portable devices keep detailed records of their movements. Of particular significance was the direct mobilization of this information for biopolitical governance.

In the case of apps that rely on the active registration of people's movement and their access to enclosed spaces via QR codes, a spate of commercial applications piggybacked on public health imperatives. In restaurants, bars, and cafes, for example, QR check-in codes (for public health purposes) are redoubled by QR menu and ordering apps (to facilitate commerce and lower overhead costs). The threat of contagion provided yet another opening for the alibi of convenience—and the reconfiguration of the workplace. As the *New York Times* put it, "QR codes have allowed some restaurants to build a database of their customers' order histories and contact information. At retail chains, people may soon be confronted by personalized offers and incentives marketed within QR code payment systems" (Woo, 2021). Rather than relying on a member of the wait staff, customers can place their order directly, allowing establishments to reduce the number of workers and to create detailed records of personal preferences. We might describe this as the digital enclosure (Andrejevic, 2007) of multiple retail functions, which has the redoubled result of displacing human interaction and rendering formerly ephemeral interactions trackable, recordable, and storable.

Passive monitoring at-a-distance

Biometrics promise to be the linchpin that brings together different kinds of personal data. Once individuals can be identified at a distance, the trove of data obtained can be linked to stored forms of data from other systems. Growing deployment of biometric technology in response to the pandemic helped pioneer new applications and also normalized the widespread use of passive biometrics. Applications included face identification and detection as well as the collection of surface body temperature and other physiological data (such as heart rate and blood oxygen levels). When used to track and identify individuals, biometrics-at-a-distance turns bodies into metadata:

information about our activities and interactions makes it possible to identify, sort, and respond to them. Biometric forms of identification like facial recognition promise to secure public and shared space by eliminating the forms of anonymity that serve as cover for covert or criminal activity. From the perspective of law enforcement, the technology promises heightened visibility within the realm of the social. This eliminates the frustration of having to rely on potentially unreliable witnesses by crowdsourcing the identities of people caught on CCTV, or by verifying the fact that there may have been no witnesses at all.

In response to the pandemic, passive biometrics were deployed in a range of contexts to protect against viral spread and contagion. For example, facial recognition systems offered touchless solutions to reduce the need for physical contact with buttons, doorknobs, and other forms of access control. Shops, workplaces, and apartment buildings could all be provided with touchless access and purchasing solutions, allowing people to "pay with their face." Elevator companies including Otis, Schindler, and Hyundai, all developed systems that incorporated facial recognition technology to enable touchless channeling of individuals through office and residential buildings. Such systems would link a known face with a particular destination and assign elevators accordingly—one need not push buttons to open doors or to select a floor.

Remote biometrics were also deployed to identify individuals in a crowd who were exhibiting symptoms of elevated body temperature by pairing facial recognition cameras with infrared sensors (Freed, 2021). Biometric identification was used not only to identify symptoms, but also to verify vaccination status. A company called TensorMark, for example, created augmented reality glasses equipped with facial recognition technology to, "validate in real-time a person's recent test results for the COVID-19 virus" (Vuzix, 2020). The glasses link people's faces with a database that provides information about test results coupled with an ID photo. The system was marketed to, "employers, retail venues, sports arenas, and concert venues" (Vuzix, 2020). For the time being, the database relies solely on "permission-based consumer information"—though the strengthening push toward vaccine passports suggests that consumers and workers may find themselves under increasing pressure to provide such consent. Jumping on the same bandwagon, the California-based startup FaceFirst promoted the creation and use of a "coronavirus immunity registry" that would be accessible via a mobile phone app. As one media account put it, "The app will also tell employers and border control staff more about a person's experience of Covid-19…It will know what kind of test you received, in case it was a defective one; it will include a record of whether you've been near infected folk or not; and it will note if you've had an antibody test" (Brewster, 2020).

Smart cameras being promoted in response to the pandemic can identify people wearing masks, screen for symptoms, and track individuals from camera to camera (for ensuring adherence to distancing restrictions and quarantines). A Russian company called NtechLab, for example, supplied its "FindFace" system to the city of Moscow for contact tracing and quarantine enforcement. In contrast to privacy protecting apps that shield location information, this system offered the prospect of comprehensive surveillance: if someone tested positive, the people with whom they have been in contact could be identified from CCTV footage, tracked down, and notified.

As previous work on pandemics suggests, the surveillance dimensions of disease containment address, "a deep anxiety about the timeliness of response" (French and Mykhalovskiy, 2013: 175). The ability to collect and process information in real time (or close to it) underwrites "an immense effort to detect, pre-empt or rapidly respond to health events to prevent them from having trans-local effect" (French and Mykhalovskiy, 2013: 175). In the era of high-resolution digital monitoring, what counts as the local diminishes dramatically, potentially down to the individual level. We can discern this logic at work in the development and implementation of "smart" monitoring systems amidst the viral threat. Strategies for pre-emption operate at a range of levels from detecting at-risk communities to detailed monitoring of individuals. A sensor-equipped ring publicized by the US National Basketball Association, for example, was promoted as a means of limiting viral spread among players (and thereby enabling the resumption of the NBA season). The $500 "Oura" ring is a self-tracking device (originally marketed as a sleep tracker) embedded with sensors that capture biometric information including body temperature, respiratory rate, heart rate and sleeping patterns. The ring was repurposed as a COVID-19 alert system after recent research by the Rockefeller Neuroscience Institute indicated it could help detect whether someone is carrying the virus up to three days before symptoms (Abate, 2020).

This combination of sensor systems with automated, customized responses is meant to construct a flexible, ubiquitous form of quarantine—one that bypasses the uncertainty that requires everyone be enclosed. The only people identified are those who, as a consequence of physical positionality, body temperature, or other somatic indicators, pose a threat either now or in the future. The result can be described as a reconfiguration of quarantine borders. Fixed, abstract spatial limits (such as the borders of neighborhoods or whole towns) are displaced by flexible ones, so that we carry our borders around with us. Every entryway or access point, to the extent that it can be fitted with remote sensors, reimposes a new set of electronic borders. We are never fully through the border—on the "inside" versus the "outside"—because the borders multiply and, at the limit, become continuous. When we are always within the radius of a passive data collection system, our "permissions" can be adjusted in real time to reflect our current condition.

The dismantling of generalized quarantine, then, is effected by the generalization of surveillance, that is, by the construction of an overarching infrastructure of monitoring enabled by long-range sensors and electromagnetic enclosures. We might describe this, building on Foucault's (2008) work on post-disciplinary forms of control, as a form of environmental governance. In his lectures on biopolitics, Foucault suggests that governance at the environmental level is conceptually distinct from disciplinary control. He describes the signs of, "a massive withdrawal with regard to the normative-disciplinary system" in which "discipline-normalization" is displaced by interventions that modify "the terms of the game, not the players' mentality" (2008: 261-262). Environmental governance is familiar in the online context, whereby information is collected about users to construct their informational environment in ways that guide individual behavior (without requiring them to consciously internalize the imperatives of those who shape the environment). In this respect, environmental governance lends itself to a post-trust situation (especially insofar as it relies upon comprehensive monitoring). By contrast, disciplinary governance depends on some level of trust (backed by the threat of punishment) that individuals will act according to the "rules" and internalize them. In a well-functioning disciplinary system, surveillance becomes superfluous because individuals can be relied upon to behave according to the imperatives that have been imposed upon them. Environmental control, however, seeks to change behavior not by changing minds, but by acting directly upon the context of action—what Foucault calls "the milieu." In practice, environmental governance relies upon environmental monitoring to discern how contexts shape behavior in real time and to intervene in that environment when necessary. In this respect, surveillance, by becoming ubiquitous, displaces social trust. For example, we do not need to rely too heavily on trusting that individuals will not violate quarantine restrictions if their movements can be tracked at a distance, in real time.

It is not clear, however, that any of these biometric forms of data collection contributed in significant ways to manage the pandemic. The most publicized and widespread forms of response worldwide still focused on human contact tracking and lockdown restrictions of various kinds (Ashkan, et al. 2020). The most widely used technologies appeared to be those that allowed authorities to track adherence to pandemic restrictions and to notify those who visited “hot spots” (Gibson and Walker, 2020; Whitelaw et al., 2020). Given the gravity of the crisis, any technology that might help was treated as a welcome addition to managing viral contagion. At the same time, many of these technologies were being developed in advance of the pandemic and are likely to outlive it. Costly infrastructures like touchless forms of access and social sorting are more likely to be repurposed than dismantled, making it likely that the pandemic response will have played a significant role in promoting increasingly comprehensive forms of surveillance in shared and public spaces. Once offices have embedded systems for tracking employee movements, these can be repurposed for spatial allocation studies, productivity monitoring, and other forms of supervision. Biometric scanners are not limited to tracking COVID-19 symptoms and can be used, for example, to minimize the impact of the annual flu season. Perhaps more significantly, such infrastructures are aligned with the imperatives of the surveillance economy, which relies upon data and its automated processing as a means of rationalizing productivity, consolidating control, and managing risk. The development of “smart” spaces equipped with passive monitoring systems has long anticipated granular levels of automated tracking and response. The COVID-19 response, then, should be viewed not as an exceptional moment in terms of the political economy of surveillance, but as continuous with the trajectory of networked digital media technologies.

Conclusion

In the COVID-19 moment, seeing other people, even intimates, as vectors of potential vulnerability and contamination rehearses the defining anxiety of both the classic liberal subject and accelerated globalization. The existence of others undermines (the fantasy of) autonomy as self-sufficiency. The fact that rightwing forms of populism coalesce around this incoherent version of anti-social autonomy is testimony, in part, to its apotheosis—hyper-customization and individuation promoted by the commercial online economy. The surveillance economy participates in a self-stimulating cycle; the detailed collection of personal information—for customizing content, search, goods, and services—privileges consumer sovereignty (Sunstein, 2007) over civic identity. In so doing, this fosters suppression and misrecognition of the underlying forms of sociality and interdependence upon which social life necessarily relies. The processes shaping the information and communication systems that help construct our understanding of the world are irreducibly social. The paradox of *social* media is that they suppress recognition of this fact. Until relatively recently, the social character of this shaping of our information worlds was relatively commonplace. Online, however, automated curation processes render their social character increasingly machinic, opaque, and ostensibly neutral.

This misrecognition manifests itself in a variety of ways but was palpably visible during the US Congressional hearings on social media in which elected representatives repeatedly described human decisions to take down objectionable content as censorship (Browning, 2020). That debate focused on the decisions of social media executives to enforce their stated policies sidelined the fact that there is *no such thing* as a “neutral” social media platform. The sheer volume of content means that these platforms necessarily curate the content viewers see; in accordance with whatever strategy maximizes revenue, some comments are amplified and other suppressed. The terms of the debate (whether humans should intervene by "de-platforming" content or individuals) assumed that the platform was an open public sphere in which content was *not already* being sorted and prioritized. This fantasy repressed recognition of the social choices *already incorporated* into the algorithms. Resistance to this recognition reflects the version of individual autonomy that is threatened by any admission of unchosen interdependence or interconnection. Social media platforms reinforce this version of hyper-individualism through their practices of data-driven targeting and customization: information is framed not as a social or collective good but as a matter of individual consumer choice and personal preference. Against this background, the symbolic threat of the pandemic—in addition to its physiological and biological impact—is that it highlights the reality of irreducible social interdependence and its attendant risks. We might draw a parallel here between the anti-vaxxers/conspiracy theorists on the one hand, and, on the other, those who decry the form of "political correctness" they see manifest in the policies of social media platforms. The latter do not recognize the social decisions that are already present, of necessity, in platform curation. For them, the Internet has ushered in the anti-social prospect of an impossible extreme of free speech—the ability to say anything one wants without *any* social consequences. The anti-vaxxers and conspiracy theorists, by the same token, do not recognize the social character of either public health measures or, more generally, the practices society has developed to adjudicate between rival accounts of reality. They embrace a form of idiotic (in the cognate sense of purely individual) solipsism: the suppression of social interconnectedness and interdependence. If freedom is equated with pure autonomy, then an admission of dependence upon the existence and activities of others is construed as an inherent threat to autonomy. This anxiety is not surprising, given that the pace and scope of contemporary globalization advances interdependence beyond the forms of social capital and social trust necessary to manage it.

The politicization of responses to the pandemic became rapidly framed as follows. On one side, was the recognition of interdependence: that fighting a contagious virus required a collective response whereby individual decisions affected the welfare of others. On the other, is a version of individual liberty that takes each choice—whether to wear a mask and obey social-distancing restrictions—as an individual one, regardless of consequences. Similarly, the libertarian anti-vaccine stance stems from its rejection of the social character of vaccination.

Those who do not recognize social interdependence may offload their refusal onto automated systems. Here, automated monitoring "at-a-distance" comports with the post-trust dimension of the informational-social infrastructure (such that the social is suppressed and misrecognized). If a significant portion of the population sees pro-social behavior in the face of a communal threat as an infringement of personal liberty, comprehensive monitoring offers to compensate with ubiquitous surveillance. Such a system raises a defining question of global interdependence: how to transact and interact in a context beyond the reach of social trust. The libertarian fascination with distributed ledger technology, for example, derives from its ability to displace social trust as a mechanism for accountability and control. As Vigna and Casey (2019) put it, "blockchain is seen as capable of supplanting our outdated, centralized model of trust management, which goes to the heart of how societies and economies function" (22). It should come as no surprise, then, that distributed ledger technology is championed not simply as a surrogate for the "in God we trust" of legal tender, but as a generalized means of bureaucratic control over everything from supply chain logistics to sharing medical data. In this respect, distributed ledgers continue the trajectory of control away from personal trust toward the rationalized bureaucratic systems described by Beniger (2009). They enable forms of international tracking and accountability that rely even less on trust than those institutions and practices that took the place of kinship and personal relations. Taken to (an impossible) limit, a “post-trust” society displaces trust with continuous automated monitoring and control, managed by distributed systems that, in turn, operate globally and automatically, with full accountability. On this matter, distributed ledger technology and total surveillance go hand-in-hand.

The forced nature of splintered and distributed living brought on by the coronavirus pandemic intensifies the deployment of various technologies designed to facilitate, adjudicate, and regulate networked individualism. The attempt to secure circulation by extending detailed monitoring to the most granular and individual level is, in one sense, an attempt to pre-empt the recognition of social interdependence. The notion of shared risk is addressed before it can become an issue. This, for all practical purposes, is an impossible fantasy that gives shape to the cascading logic of automation: if everyone’s behavior and emerging symptoms can be monitored in real time, contagion can be pre-empted.

One lesson of pandemic surveillance that has broader historical resonance, then, is that the potential perils of interdependence can be addressed through the development of increasingly comprehensive and granular forms of surveillance, monitoring, and tracking. Such an analysis does not dispute the important role of contact tracing and symptom tracking in managing viral contagion. Rather, it interrogates the attempt to rely on surveillance as a surrogate for social trust and the recognition of interdependence. The fantasy of dis-aggregated risk—that, for example, portions of the population can, thanks to a range of monitoring and data-mining techniques, be designated as low-risk and thus permitted to circulate while high-risk individuals are detained and quarantined—disavows underlying forms of social interdependence. Perhaps even more relevant to the current moment is the way in which hyper-surveillant technologies of individuation reinforce incoherent versions of autonomy associated with anti-vax and other pandemic conspiracies that disable the capacity for collective response. The alarming sequence goes something like this: social interdependence is framed not simply as an irreducible and inevitable *potential* vulnerability (which it always is) but as an eliminable threat, that is, something that can be dispensed with (which it cannot). The attempt to dispense with the risk of social interdependence, in turn, relies upon the promise to replace social trust (always a potential source of risk) with comprehensive surveillance. However, because social interdependence is irreducible (i.e., we are too deeply entwined with one another, linguistically, economically, biologically), surveillance will never succeed in replacing social trust entirely. Rather, as we have seen, an incoherent version of freedom and autonomy will be dogged by the return of the repressed—most recently in the form of paranoid conspiracy theories that blame a perceived loss of autonomy not on irreducible societal interdependence, but on a shady cabal of collaborators. This is not to suggest that monitoring and tracking can be dispensed with in pandemic contexts. Our point is that such measures can never be anything more than an adjunct to forms of collective action that rely upon a shared sense of interdependence and social trust.

Author bios

Mark Andrejevic is Professor in the School of Media, Film, and Journalism at Monash University, where he leads the Automated Society Working Group. He is a Chief Investigator (CI) in the ARC Centre of Excellence for Automated Decision Making. His work focuses on digital media, popular culture, and surveillance, and he is lead CI for the ARC Discovery Project, "When Your Face is

Your ID." He is the author of numerous academic articles and book chapters as well as four monographs including, most recently, *Automated Media* (Routledge, 2019).

Zala Volcic is Senior Lecturer in the School of Media, Film, and Journalism at Monash University where she directs the Bachelor of Media Communication Degree Program. Her work focuses on media, nationalism, and identity. She is the author of numerous academic articles and book chapters as well as a monograph on national identity in the Balkans. She is the co-editor of a collection of articles on commercial nationalism and the media.

References

Abate E (2020) Here's how the NBA's coronavirus-fighting ring might help. *GQ*, 17 June. Available at: https://www.gq.com/story/oura-ring-nba (accessed 14 August 2021).

ABC News (2005) Former spy claims 60 terrorists in Aust cells. Available at: https://www.abc.net.au/news/2005-08-03/former-spy-claims-60-terrorists-in-aust-cells/2072344 (accessed 20 August 2021).

Amatulli J (2020) Zoom can track who's not paying attention in your video calls. Here's how. *Huffpost,* 25 March. Available at: https://www.huffpost.com/entry/zoom-tracks-not-paying-attention-video-call_l_5e7b96b5c5b6b7d80959ea96 (accessed 10 July 2021).

Amoore L and De Goede M (2005) Governance, risk and dataveillance in the war on terror. *Crime, Law and Social Change* 43(2-3): 149-173.

Andrejevic M (2007) *ISpy*. Kansas: University of Kansas Press.

Andrejevic M and Selwyn N (2020) Facial recognition technology in schools: critical questions and concerns. *Learning, Media and Technology* 45(2): 115-128.

Antaya S (2015) At war with the machine: Canadian workers' resistance to Taylorism in the early 20th century. *The Great Lakes Journal of Undergraduate History* 3(1):7-19.

Ashkan S, Calo R and Bergstrom C (2020) Contact tracing apps are not a solution to the COVID-19 crisis. *TechStream*, 27 April. https://www.brookings.edu/techstream/inaccurate-and-insecure-why-contact-tracing-apps-could-be-a-disaster/

Bauman Z and Lyon D (2013) *Liquid Surveillance: A Conversation*. John Wiley & Sons.

Beniger J (2009) *The Control Revolution: Technological and Economic Origins of the Information Society*. Harvard University Press.

Berinato S (2003) US HomeGuard: Someone to watch over you. CSO Online, 2 September. Available at: https://www.csoonline.com/article/2116759/us-homeguard--someone-to-watch-over-you.html (accessed 14 August 2021).

Braverman H (1998) *Labor and Monopoly Capital*. NY: Monthly Review Press.

Brewster T (2020) Facial recognition firms pitch Covid-19 'immunity passports' for America and Britain. *Forbes*, 20 May. Available at: https://www.forbes.com/sites/thomasbrewster/2020/05/20/facial-recognition-firms-pitch-covid-19-immunity-passports-for-america-and-britain/#6f0f60d15914 (accessed 14 August 2021).

Browning K (2020) Zuckerberg and Dorsey face harsh questioning from Lawmakers. *New York Times*, 17 November. Available at: https://www.nytimes.com/live/2020/11/17/technology/twitter-facebook-hearings (accessed 15 August 2021).

Cacault MP, Hildebrand C, Laurent-Lucchetti J and Pellizzari M (2021) Distance learning in higher education: evidence from a randomized experiment. *Journal of the European Economic Association* 19(4): 2322–2372.

Chyi N (2020) The workplace-surveillance technology boom. *Slate*, 12 May. Available at: https://slate.com/technology/2020/05/workplace-surveillance-apps-coronavirus.html?utm_source=pocket_mylist (accessed 14 August 2021).

Connolly R (2020) The pandemic has taken surveillance of workers to the next level. *The Guardian*, 14 December. Available at: https://www.theguardian.com/commentisfree/2020/dec/14/pandemic-workers-surveillance-monitor-jobs (accessed 20 August 2021).

Defence Advanced Research Projects Agency (2002) Information Awareness Proposer Information Pamphlet BAA 02-08. Available at https://www.petervronsky.org/HST540/HST540/DARPA-InfoAwareness.pdf (accessed 20 August 2021).

Dionne E.J (2003) Inevitability, the politics of terror: fear has become part of Washington's power struggle. *Brookings,* 25 May. Available at: https://www.brookings.edu/opinions/inevitably-the-politics-of-terror-fear-has-become-part-of-washingtons-power-struggle/ (accessed 20 August 2021).

FindFace (2020) Biometric solution against Covid-19. Available at: https://ntechlab.com/en_au/solution/biometric-solution-against-covid-19/ (accessed 20 August 2021).

Finnegan M (2020) The new normal: when work-from-home means the boss is watching. *Computer World*, 29 October. Available at: https://www.computerworld.com/article/3586616/the-new-normal-when-work-from-home-means-the-boss-is-watching.html (accessed 20 August 2021).

Foucault M (1975) *Discipline and Punish: The Birth of the Prison*. NY: Penguin Classics.

Foucault M (2007) *Security*, *Territory, Population: Lectures at the College de France, 1997-78.* Burchell G (trans). London: Palgrave Macmillan.

Foucault M (2008) *The Birth of Biopolitics: Lectures at the Collège de France 1978-1979*. Sennelart M (ed), Ewald, F. and Fontana, A. (general eds), Burchell G. (trans). Basingstoke: Palgrave.

Freed B (2021) Hawaii adds facial recognition to COVID-19 airport screening. *Statescoop*, 18 May. Available at https://statescoop.com/hawaii-airports-covid-19-facial-recognition/ (accessed 20 August 2021).

French M and Mykhalovskiy E (2013) Public health intelligence and the detection of potential pandemics. *Sociology of Health & Illness* 35(2): 174-187.

Frist W (2002) *When Every Moment Counts: What You Need to Know about Bioterrorism from the Senate's Only Doctor*. Lanham: Rowman & Littlefield Publishers.

Gibson B and Walker A (2020) QR codes skyrocket in popularity due to COVID-19. Here's the history behind the 2020 technology of choice. *ABC News*, 2 December. Available at: https://www.abc.net.au/news/2020-12-02/history-of-qr-codes-as-popularity-skyrockets-due-to-covid-19/12942318 (accessed 14 August 2021).

Greenwald G (2014) *No place to hide: Edward Snowden, the NSA, and the US surveillance state*. United States: Macmillan.

Harwell D (2020) Cheating-detection companies made millions during the pandemic. Now students are fighting back. *Washington Post*, 12 November. Available at: https://www.washingtonpost.com/technology/2020/11/12/test-monitoring-student-revolt/ (accessed 15 August 2021).

Herold B (2016) The future of big data and analytics in K-12 education. *Education Week*, 11 January. Available at: https://www.edweek.org/policy-politics/the-future-of-big-data-and-analytics-in-k-12-education/2016/01 (accessed 14 August 2021).

Kim N (2020) 'More scary than coronavirus': South Korea's health alerts expose private lives. *The Guardian*, 6 March. Available at: https://www.theguardian.com/world/2020/mar/06/more-scary-than-coronavirus-south-koreas-health-alerts-expose-private-lives (accessed 14 August 2021).

Linn A (2011) Post 9/11, surveillance cameras everywhere. *NBC News*, 23 August. Available at: https://www.nbcnews.com/id/wbna44163852 (accessed 14 August 2021).

NEC (2021) NEC Delight: Personalized adventures unified by trust. Available at: https://www.nec.com/en/global/delight/ (accessed 15 August 2021).

NPR (2021) More than 9,000 anti-Asian incidents have been reported since the pandemic began. *NPR,* 12 August. Available at: https://www.npr.org/2021/08/12/1027236499/anti-asian-hate-crimes-assaults-pandemic-incidents-aapi (accessed 15 August 2021).

Peters J D (2015) *The Marvelous Clouds*. University of Chicago Press.

Phillips J (2002) Human ID at a distance (HumanID). Available at: https://web.archive.org/web/20020817002159/http:/www.darpa.mil/IAO/HID.htm (accessed 15 August 2021).

Rotenberg M (2006) The sui generis privacy agency: how the United States institutionalized privacy oversight after 9-11. *SSRN* 28 September. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=933690

Rushkoff D (2009) Terrorism as Virus. Available at: https://rushkoff.com/terrorism-as-virus/ (accessed 15 August 2021).

Sledge M (2013) CIA's Gus Hunt on big data: we 'try to collect everything and hang on to it forever'. *Huffpost*, 20 March. Available at: https://www.huffpost.com/entry/cia-gus-hunt-big-data_n_2917842

Steinberg M (2021). From automobile capitalism to platform capitalism: Toyotism as a prehistory of digital platforms. *Organization Studies* (Special issue on technology and organisation): 1-22. DOI:10.1177/01708406211030681

Stevens GM (2003) Privacy: total information awareness programs and related information access, collection, and protection laws. Federation of American Scientists, Washington, D.C., Report for Congress. https://fas.org/irp/crs/RL31730.pdf (accessed 14 August 2021).

Sunstein C (2007) *Republic 2.0*. Princeton: PUP.

United Nations (2021) COVID-19. Available at: https://www.youtube.com/watch?v=ubJaJPRdoMk (accessed 14 August 2021).

Vigna P and Casey M (2019) *The Truth Machine: The Blockchain and the Future of Everything*. New York: Picador.

Vuzix (2020) *Vuzix Expands Partnership with TensorMark for Facial Recognition Related to COVID-19 Hospital Testing Initiative.* Press Release, 28 March. Available at: https://ir.vuzix.com/press-releases/detail/1786/vuzix-expands-partnership-with-tensormark-for-facial (accessed 14 August 2021).

Whitelaw S, Mamas A, Topol E, Van Spall HGC (2020) Applications of digital technology in COVID-19 pandemic planning and response. *The Lancet Digital Health* 2(8): e435-e440.

Woo E (2021) QR Codes Are Here to Stay. So Is the Tracking They Allow. *New York Times*, 26 July. Available at: https://www.nytimes.com/2021/07/26/technology/qr-codes-tracking.html (accessed 14 August 2021).

Yeo SJ (2021) Tech companies and public health care in the ruins of COVID. *International Journal of Communication* 15 (1617-1636).

Zuboff S (2019) *The Age of Surveillance Capitalism*. NY: Profile Books.