International Journal of E-Planning Research
Volume 10 • Issue 2 • April-June 2021

Surveillance in the COVID-19 Normal:
Tracking, Tracing, and Snooping – Trade-Offs in Safety and Autonomy in the E-City

Michael K. McCall, Universidad Nacional Autónoma de México, Mexico
Margaret M. Skutsch, Universidad Nacional Autonoma de Mexico, Mexico
Jordi Honey-Roses, University of British Columbia, Canada
https://orcid.org/0000-0003-0097-1811

ABSTRACT

The COVID-19 pandemic has accelerated the adoption of surveillance technologies in cities around the world. The new surveillance systems are unfolding at unprecedented speed and scale in response to the fears of COVID-19, yet with little discussion about long-term consequences or implications. The authors approach the drivers and procedures for COVID-19 surveillance, addressing a particular focus to close-circuit television (CCTV) and tracking apps. This paper describes the technologies, how they are used, what they are capable of, the reasons why one should be concerned, and how citizens may respond. No commentary should downplay the seriousness of the current pandemic crisis, but one must consider the immediate and longer-term threats of insinuated enhanced surveillance, and look to how surveillance could be managed in a more cooperative social future.

KEYWORDS

Citizen Response, Confidentiality, COVID-19, Phone Apps, Security, Surveillance, Tracing, Tracking, Urban Monitoring

INTRODUCTION

Surveillance technologies are being deployed at an unprecedented pace in cities throughout the world, amid the fears of COVID-19 and with little discussion about the long-term consequences. In the current situation, surveillance is necessary to track infections and the spread of the virus. However, the core issues in any surveillance, beyond specifically for COVID-19, are existential in that surveillance provokes basic human dilemmas and contradictions. Surveillance policies generate tensions between safety and risk at all levels - that of the individual, that of the state, and of all levels of society in-between; and politically to this, the struggles between the individual and society and thus between social / community cooperation and individual self-reliance.

In reviewing these tensions, in no way do we downplay or diminish the seriousness of the current crisis as expressed in the awful numbers of deaths around the world, especially those courageous

DOI: 10.4018/IJEPR.20210401.oa3

health workers who die aiding us, and the millions of frontline workers who are facing the public in the streets and in "essential services", - not comfortably working safely from home. Nor do we underestimate the devastation of people's livelihoods, especially the daily earners, the street and gig workers. All these remind us to take the crisis deadly seriously and not fall into a facile critique (from Left or Right) of how governments and leaders and the public are getting it wrong. The profound question that political leaders are now facing is: 'stay (relatively) safe at home', or, 'go out and work, earn and spend' to keep the economy going. This dilemma faces the leadership of every economic ideology, from the US and the EU to India, South Africa, Mexico, Russia, to China and North Korea. Into this vicious political, economic, ethical, moral question, comes surveillance and questions about its intensity and its extent.

The article addresses structures and mechanisms used for COVID-19 surveillance. It describes what they do, how they are used, what they might do, our reasons to worry, and how citizens may respond. In Section 2 we consider key elements of surveillance in the COVID-19 era, especially referencing its functioning in the Smart City. In Section 3 we outline the salient technologies in this era, which are CCTV, phone apps and wearables. Section 4 considers the obvious and less obvious concerns raised by these, by the public in general and by social critics. The next section 5 suggests commentaries on elements of our "future normal" under enhanced surveillance – risk and its responsibilities, trust and truth. Finally, in Section 6 we re-visit the discourses of surveillance, and how it is resisted and re-imagined.

SURVEILLANCE FOR COVID-19: SETTING AND CONDITIONS

The spread of the Severe Acute Respiratory syndrome coronavirus 2 (SARS-CoV-2, hereafter COVID-19) has particular characteristics which raise new challenges for surveillance (WHO, 2020). Urban structures and urban life are more friendly environments for the COVID-19 virus. Cities concentrate larger human populations (virus hosts), higher densities of people who are highly mobile with multiple opportunities for person-to-person contacts (transmission), and most cities have deep pockets of poverty (vulnerability). COVID-19 needs intense tracking, it is virtually unprecedented in global epidemiology in infection rates and hidden, asymptomatic transmission. Testing is essential and is intrinsically connected to tracing, yet there are continuing critiques of the state of COVID-19 testing in many countries, including the availability and reliability of the kits, the frequency of tests, and delays in getting results, but testing is not the focus of this article and it is not addressed further here.

Tracking means watching people – monitoring movements, locations, interactive behaviour with contacts. Tracking COVID-19 on a Big Data scale in the Smart City needs more than just counting people who present symptoms (WHO, 2005). But, building Big Data pictures from watching people is easily extendable to many other intentions of surveillance and control. The conflict is between strengthening the levels of surveillance for protection, and the fears of where else that could lead. The effort to increase health monitoring sets a precedent for other forms of surveillance.

The scientific literature distinguishes various forms of "surveillance" that are reflected in several sub-concepts (French & Monahan, 2020; Lyon, 2018). "Lateral surveillance" (Andrejevic, 2004) in everyday language means people critically watching each other. This is seen now in the COVID-19 pandemic, in social media trolling, denouncing, and snatched photos of bad behaviour like no masks or no distancing. We used to call this grassing, or snitching and it presents a moral dilemma. There is a common human reluctance to snitch on family, friends, or community. However, such behavior seems easier on anonymous social media platforms, and so it overlaps with what is called "social media surveillance" or 'digital eavesdropping' (Cheng et al., 2020; Zhiyuan Hou et al., 2020). Much of what is termed "participatory surveillance" is not very participatory because it depends on "volunteered geographic information" (VGI) or human sensors (Paolotti et al., 2014). VGI requires a willingness to give up accountability and responsibility and participation in return for gains in speed, efficiency, and reducing innate fears (McCall et al., 2015). The focus in this paper however is

on conventional top-down surveillance of the public citizenry by the state and its agents (Hillebrand, 2020; Lyon, 2018, 2020).

This kind of surveillance is always a ratcheting-up, an insidious creep towards more surveillance. State surveillance is indeed as old as state formation, with significant technology expansions in the two World Wars, but post 9/11 the power of the tools has exploded and governments have leveraged this with enabling and legitimizing legislation. In all polities, the covering justification focuses on the threat of internal and external enemies of social peace and harmony from which the state must protect us (French & Monahan, 2020; Lyon, 2020). Most critical observers assume the expansion in surveillance will be nearly impossible to scale back 'post-pandemic'. As precedent, consider that most of the sweeping investigative powers taken by the US intelligence community in 2001 after the 9/11 terrorist attack remain in place 20 years later. Luhrmann & Rooney (2020) provide sound historical evidence that democratic rights of privacy and data confidentiality surrendered "temporarily" during a crisis are very difficult to crawl back (see also Halpern, 2020; Luhrmann et al., 2020).

The current crisis is normalizing surveillance measures at an unprecedented scope and scale. The public health crisis is making it easier to justify new surveillance and control measures. It is easier for governments to rebrand them as palatable, acceptable, necessary, or even desirable against COVID-19 and whatever surely comes next. Mainstream opinion leaders emphasize the public health risks over the privacy risks in response to our current existential fears of the virus, and the public accepts this. Public acceptance is driven by fear. Hillebrand (2020) notes that fear releases people's consent to voluntary data disclosure and other surveillance. She recognises, also for the COVID-19 case, that fear fosters distrust in others, which is amplified by populist discourse in social media exploiting our primeval fears of pandemics.

Public health professionals have a specific domain of practice in surveillance of people. The International Health Regulations (IHR) of WHO define surveillance as "the systematic ongoing collection, collation and analysis of data for public health purposes and the timely dissemination of public health information for assessment and public health response" (WHO, 2005: 10). WHO guidelines specifically for surveilling COVID-19 have objectives to: "1) monitor trends in the disease where human-to-human transmission occurs; 2) rapidly detect new cases ….; 3) provide epidemiological information to conduct risk assessments; 4) provide epidemiological information to guide preparedness and response measures" (WHO, 2020). The WHO guidelines also distinguish between "suspected cases," "probable cases," and "laboratory-confirmed cases" which complicates the surveillance mechanisms.

Surveillance of the urban citizen is not new. The past decade has seen many moves towards the *smart city* – the e-city, the digital city, the joined-up, linked, networked city. In critical articles, fears have been raised about the golem of big data and who accesses them and for what ends (Honey-Rosés et al., 2020, Marx & Muschert, 2007; McCall et al., 2015). The smart city is built on real-time (or accelerated) acquisition from multiple data sources that are quantitatively much bigger and from sources previously not interconnected, but now being linked. This is real Big Data, employing multiple analytical methodologies and modelling, and exponentially growing digital technologies including facial recognition, biometrics, and many aspects of AI. As a result, "public" spaces in our cities are being 'big brothered' or 'panopticonned' (Foucault, 2012) at an unprecedented rate. Surveillance technologies identify individuals who may be committing undesirable acts, but tellingly they also create a climate where everyone has the feeling of always being watched.

SURVEILLANCE MECHANISMS – METHODS AND TOOLS

The surveillance systems, tracking technology and restrictions in movement are essential strategies that have allowed some slowing down of the pandemic (WHO, 2020). Traditionally, surveillance was enforced via lateral surveillance (concierges, 'watchmen', police informers, neighbourhood vigilantes) and physical barriers, police checks, and permit systems to travel or leave home.

Physical controls to surveil people during times of epidemics are nothing new. In the 15th century, the Venetians had lazarettos, isolation wards, on the island of San Lazaro, where ships' crews had to wait 40 days to 'dissipate the bad vapours'; enough time to kill infected rats and sailors as Snowden (2019) points out; he termed this an early form of "institutionalized public health". There were many predecessors in the Mediterranean and the Ottoman Empire and for instance, Lhasa centuries ago had a quarantine mechanism. And now we are lauding the efforts of indigenous peoples in Canada, Brazil, or Australia to physically close off entry to their lands.

For the past couple of decades the developments are in the digital technologies which handle Big Data to instantly provide detailed information culled from a plethora of: CCTV security cameras, bodycams, dashcams, multiple sensors on autonomous vehicles, license-plate readers, biometric scans, wearables, robots, drones, GPS devices, phone apps, cell-phone triangulation, internet searches, and commercial transactions. Without diminishing the absolute need for public-health surveillance, COVID-19 is further legitimizing them to facilitate all kinds of spying by governments, businesses, or other malign actors. These snooping mechanisms are being insidiously installed without much public discussion to operate in our global city streets, squares and parks. In China, cameras have even been installed inside apartment buildings to monitor residents, with security notifications when individuals leave their homes or are visited (Gan, 2020; Horwitz & Goh, 2020).

CCTV

The big brother par excellence is CCTV. The reality of this invasion can be gleaned from the business market headline "CCTV Camera Market could reach $16 Billion by 2029 … from Pandemic". This "spike in demand" is estimated by business analysts as primarily from Asian countries, which are better adapted at using digital technologies like thermal imaging, geo-location data and AI-enabled video analysis (Future Market Insights, 2020). Eight of the top ten cities in terms of CCTVs per head of population are in China with Chongqing, Shanghai and Shenzhen having more than 100 cameras per 1,000 people; London and Atlanta are also in the top ten (Bischoff, 2019).

In response to the COVID-19 pandemic, France is trialing CCTV on Paris metros to estimate facemask use. Initially it is secure enough, the data collected by the DakataLab software remain anonymous without facial recognition software and it only uploads aggregated percentages of mask wearers to the metro authorities. So far so good, but it is easy to envisage mission creep, how CCTV can so easily be used for crime detection, or behavioural infractions including the moral criminality of not wearing a mask (Fouquet, 2020; ACLU, 2020). Coastal cities in Spain plan to use cameras to count the number of bodies on beaches and alert authorities when the recommended number of users is surpassed. There are many other cameras about – UAVS and dashcams are common, and robots. A robot 'dog' called Spot already patrols a Singapore park to remind people of safe distancing measures, although supposedly Spot's cameras do not track or recognise individuals, nor collect personal data. (Straits Times, 2020).

Phone APPS

COVID19 tracking and contact tracing with phone apps have been rapidly developing in this crisis time and have garnered considerable acceptance from media influencers and some publics. However, this technology 'solution' bluntly demonstrates the rapidity and complexity of changes in policies, operations and methods which are such a feature of the COVID-19 pandemic. In March and April 2020 (when this article critiquing surveillance began) phone apps were promoted everywhere as the silver bullet solution to tracking and neutralising infected people (Burgess, 2020a; Economist, 2020; Masoodi, 2020; Oliver et al., 2020). By the end of June 2020, so many flaws and weaknesses were appearing, and people's resistance to the apps was clearly growing, (see Sects 5, 6) they were shifting out of favour with governments as well as citizens.

The purpose of contact tracing apps is to alert people if they have been exposed to a person who is later identified as COVID-19-positive or symptomatic. Apps trace contacts through interaction

and proximity analysis, and so they can also function as quarantining enforcement tools, monitoring locations and interactions. In such a context, they are not necessarily anonymous or voluntary tools. They work by using GPS or Bluetooth signals to detect when two people's smartphones are close to each other. If one person later registers themselves as being infected, an alert can be sent to others judged to have been at high risk of contagion. This can be based on the exposure to that other person for a long period of time, or on the number of times the user was in the vicinity of infected people. When a user develops symptoms or tests positive for COVID-19, then that user's history of locations is shared. *Who* it is shared with depends on whether the system is '*centralised*' or '*decentralised*' – (see below). Everyone contacted may voluntarily - or be compelled to - return home, self-isolate and await a test. The exposed persons can then be tested and isolated before they can spread the virus further. The systems may include interactive maps with government data showing the locations where infected people have visited and might have made contacts (Economist, 2020; GDPRHub, 2020; Halpern, 2020; Jinfeng Li & Guo, 2020; Privacy International, 2020; Siddiqui, 2020).

There were more than 50 state-driven tracking app projects being developed in about 40 countries by June 2020. Early adopters were China, Singapore, Iceland, Australia, Germany, Austria, Italy, et al. Significant newer players include India, Brazil, Spain, Switzerland, Israel, UK, Poland, and some states in USA. The PEPP-PT (Pan-European Privacy-Preserving Proximity Tracing) programme unifies many in Europe, and extremely significant globally is the unusual joint Big Tech collaboration of the Apple and Google "Exposure Notification API" (EN-API) project. There are no complete or up-to-date, real-time surveys of these app projects (e.g. GDPRHub, 2020; Oliver et al., 2020; PanDem, 2020; Privacy International, 2020), although Siddiqui (2020) comes close. The technology and applications have moved so fast since March 2020 it is unwise to make hard predictions. There are two deployment systems approaches, centralised and decentralised (see Figure 1), and two main technical locational tools, GPS, Bluetooth LE (Low Energy), and also QR codes (GDPRHub, 2020; Jinfeng Li & Guo, 2020; Siddiqui, 2020).

Centralised Phone APPs

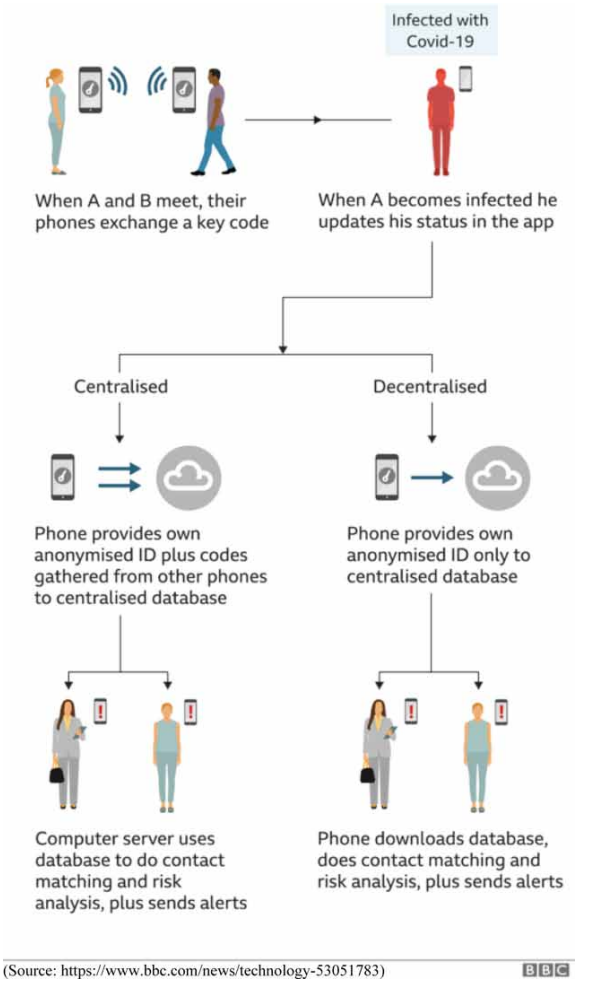
Centralised systems essentially connect the individual user to a centralised government health database where that location and status data can easily be applied to other uses. They geo-track via GPS to identify if the paths of two people have crossed. It captures location data through GPS and uploads this to a central database, tracking the movements of users in real time. Authorities can easily link this sensitive personal information to an individual, as users are required to register with an ID number. So this essentially snoops the locations of users to the central database in real time. Some centralised architectures also use Bluetooth proximity measurements.

The 'centralised' approach was initially adopted by traditionally "autocratizing" countries (Luhrmann et al., 2020) such as China, Singapore, Russia, some Gulf States, Israel, but there were also some unexpected adopters, such as Norway, France, UK, Colombia. However, the trend by late June 2020 had shifted towards 'decentralised' systems, (led by the Apple-Google EN-API), and thus away from overt central surveillance.

China was an early mover on COVID-19 apps. The "Alipay" Health Code is compulsory and this is likely to be continued after the crisis. People are required to install the app, fill in personal details, and then are issued with a colour-coded QR denoting quarantining status. The app shares the status, location, and contact data with various civil and security authorities (Burgess, 2020a; Gan, 2020; Horwitz & Goh, 2020).

In India, over 130 million early downloads made "Aarogya Setu" the fastest growing tracing app, but it is still exclusionary since only about one-third of Indians have access to smartphones, excluding most of the 1.3 billion population. It had some popularity because it includes a self-assessment health check status. The tracing app uses both GPS data and Bluetooth to locate all the people a user has been in contact with and it asks for personal information, name, age, gender, and travel history. Thus

Figure 1. Centralized v. Decentralized systems



it knows the identities of users and it enrolls the contact in the centralised government database of known COVID-19 cases (Christopher, 2020; Reuben, 2020).

The UK experience illustrates the confusion and uncertainty around apps. Initially the UK NHS (National Health Service) opted to roll out "NHSX" as a centralised system that would not follow the privacy guidelines of the decentralised approaches. It argued that in order to notify people most at risk of having been infected, "It's probably easier to do that with a centralised system." (Kelion, 2020). The NHS reportedly were considering adding the ability to warn people who had been outside too long, and the UK Police planned for their own separate app (Burgess, 2020b; Kelion, 2020). Very much money was expended and there were trials in early May at an RAF base and on the Isle of Wight. However, in mid-June the go-it-alone NHSX system was abandoned owing to its technical and cost deficiencies, as well as privacy critiques (Burgess, 2020b, 2020c), and the UK has turned to a decentralised system in collaboration with Apple-Google.

The threats from an unbridled centralized architecture can be seen in many other experiences (Amnesty International, 2020; Luhrmann et al., 2020; PanDem, 2020; Siddiqui, 2020). The French government wanted an app "tied" to the national healthcare system with its comprehensive centralized databases, and called for the Big Tech developers to relax their privacy protections. According to

Amnesty International (2020), "BeAware Bahrain", Kuwait's "Shlonik", China, and Norway's "Smittestopp", are among the most alarming mass surveillance apps because they display live or near-live tracking of users' locations when they upload GPS co-ordinates to central servers. The original Smittestopp stored location data for 30 days on a central server. Following Amnesty's strong critique, Smittestopp will be modified. The Home Quarantining app in Poland required phone numbers, reference photos, and regular check-ins (Poland is switching to an EN-API). Israel tried to enlist the Shin Bet security agency to repurpose its terrorist-tracking protocols for COVID-19 tracking (though as of July 2020 the move is in dispute in court).

Decentralised Phone APPs

The trend even by June 2020 was towards decentralised approaches, driven primarily by concerns of privacy, anonymity, confidentiality, and avoiding overt surveillance. Leading the 'decentralization turn' are two collaborations - the "Exposure Notification API" (EN-API) system of Apple and Google, and the EU-wide PEPP-PT and DP-3T. The two software interfaces are in many ways similar. By mod-2020 there were probably more decentralised than centralised systems, including Germany (13 million downloads), Switzerland, Ireland, Japan, Philippines, Australia, and Saudi Arabia among others.

"Google and Apple jointly created the EN-API system out of a shared sense of responsibility to help governments and our global community fight this pandemic through contact tracing" (Apple website; Google website) with the stated intention of a design to respect user privacy and security. They claim their approach provides more privacy because it limits the ability of the authorities or hackers to use the computer logs to track known individuals and identify their social interactions. They are based on anonymised rather than pseudonymised identifiers of users (Burgess, 2020c; Jinfeng Li & Guo, 2020; Siddiqui, 2020).

The principles behind the decentralised (EN-API and PEPP-PT) apps are: they are voluntary, requiring participants' permission to opt in, they ensure users' anonymity, and no personal identifying data are exchanged or stored. The apps rely solely on peer-to-peer connections via Bluetooth LE (Low Energy), upto c. 9m. range, to cross-identify between two phones. Unlike the centralised systems, there is no use of GPS to actually geo-locate people. It is specifically "proximity-tracing". Once a user downloads an EN-API app, their device starts generating "proximity identifier" IDs that are changed every 15 minutes (on average). These identifiers are periodically shared via Bluetooth with any nearby devices whose users have also opted into contact tracing. If a user is (later) diagnosed with the coronavirus, it is up to them to inform the app. Anyone whose phone has come near a phone owned by an infected person, say in the past two weeks, is alerted. The proximity identifier is processed on-device and does not reveal information about users' locations or personal identity or send it to a central database. It assumes that the phones are being carried by their owners. The apps should be "gracefully dismantled" after (this) pandemic is over.

Australia created its own 'semi-decentralised system', "COVIDSafe", but is now adapting to EN-API. The app asked users to give age, mobile number, post code and a name/pseudonym. Bluetooth digital handshakes record proximity for a certain length of time to anyone else with the App installed and running. Data are encrypted at all times while held on a user's phone (not accessible even to them) and are periodically automatically deleted. The app has no GPS function, so does not collect geo-location data. If an individual tests positive for COVID-19, they are asked to upload the app's history of digital handshakes to a "secure data storage system". If they consent, the information is assessed by public health officials in order to contact individuals recently in close contact. People thus notified via the app's contact-tracing are only informed they have been close to an infected person, and not who the individual is, nor when and where the contact was. The initial rate of public adoption was very fast, over 2 million downloads by June, but then slowed. The government rapidly recognised people's expressed concerns over confidentiality, and legislation quickly ensured that data were accessible only to health authorities. The Health Minister said "not even a court order" would

allow police to access it, and all data should be wiped after 21 days or when a user deleted the app. (Burgess, 2020a; National Law Review, 2020; Taylor, 2020).

There are also many apps, national, local and commercial for the purpose of self-diagnosis. They are downloadable with a set of questions and observable physical indicators and they offer a probability estimate of whether the person is COVID-19-infected. The user can reach out to medical authorities and potential contacts, and/or choose to self-isolate. Sometimes these apps are installed in conjunction with the tracking apps as an incentive, as well as beneficial in themselves.

Surveilling Bodies - Wearables

Some months into the crisis, 'wearables' have become a new approach for the surveillance of individuals. This is happening now partly as a response to the technical and uptake problems experienced by phone apps which had been hyped as the silver bullet. For instance, in June, Singapore introduced Bluetooth contact tracing devices, 'TraceTogether', as an alternative to the government's smartphone app. It is aimed at people who do not own or prefer not to use a mobile phone, beginning with vulnerable elderly (BBC, 2020).

Most ubiquitous are wearable proximity alarms that beep when wearers are within two metres (or whatever) of each other for a period of time - these may be in pagers, phones, watches, even hard hats. By itself this functionality is confidential and secure, but most devices record the data and can send them to a data center where they are transformable to surveillance. Individuals can be monitored and assessed easily for other activities. This drives the resistance to their uptake when they have been introduced, e.g. in Amazon's "Distance Assistant" in its "Fulfilment Centres" (Simonite, 2020) and by other time-surveilling, snooping employers (Miller, 2020).

More subtle are bio-monitors that track and analyse body data like sleep, heart rate, skin temperature, respiratory function, and render them as transmittable information. These wearables monitor "biomarkers" which may indicate the presence of the virus, even pre-symptom presentation. The range of devices is extensive. A Canadian review (Richardson & Mackinnon, 2018) identified over 420 wearable devices currently in the market, including fitness trackers (e.g. Fitbits), smart watches (e.g. Apple), body sensors, smart glasses, body cameras, 'smart clothing', dosimeters, biometric bracelets, and 'that hot $300 titanium smart ring everyone's talking about, the Oura' (Halpern, 2020; Masoodi, 2020). Liechtenstein, a country which can afford to, will distribute biometric bracelets to all citizens (Pascu, 2020). Indeed, surveillance knows few scale boundaries, from satellites to bracelets.

Old School Detective Work - Tracking by Human Agents

Early adopter countries in East Asia argued for human-led contact tracing (i.e. teams of health officers and detectives) and monitoring multiple media as the better surveillance technique, thus not relying primarily on apps. Apps and phones can certainly provide location and proximity data, but only skilled experienced people can introduce human intelligence into tracking and tracing (Cheng et al., 2020). South Korea and Taiwan achieved dramatically low rates of infection and mortality with their locational data and social network analysis to target individuals. South Korea tracks citizens presenting symptoms and ex-post identifies quarantine breaches which is coupled with a robust testing program. This very effective tracking system does not use a dedicated phone app, but relies on the intensive detective follow-up, individual, in-depth interviews with people about their health status and their movements, and cross-checking with a lot of additional invasive personal data from many sources.

It is clear that such a system cannot be scaled up without expensive labour investment. Most countries in the past, conducted public-health surveillance by contract tracing, but those were small numbers. It is labor-and time-intensive, painstaking, memory-dependent work, and therefore limited in scope and quite easily incomplete or inefficient. For example, at the start of the pandemic in the UK, there were only 2200 contact tracers in the UK, so 25,000 people were hurriedly recruited into a three tier system based on the intensity and sensitivity of contacting. There are reported to be many

deficiencies in the training and protocols in the UK, and elsewhere (e.g. Burgess, 2020c; Cellan-Jones, 2020; Privacy International, 2020; Reuben, 2020; Shabi, 2020).

Track and trace collects a lot of possibly sensitive information that people obviously may want to withhold for personal reasons. The surveillance approach of South Korea, among others, requires lots of supportive cross-referenced data. The government has wide authority to access data from public CCTV footage in streets and private shops, GPS tracking data from phones and cars, credit card transactions, and personal details of people confirmed as infected (Kim, 2020; Privacy International, 2020).

URBAN SURVEILLANCE AND COVID-19 APPS - WHAT ARE PEOPLE CONCERNED ABOUT?

There are continuing concerns about surveillance in general, but at this stage of the pandemic crisis story, many are addressed specifically at the apps. Ultimately these are ethical, moral, political issues, and maybe unsolvable dilemmas.

Confidentiality and Privacy

The salient concern about the apps is confidentiality and privacy. In centralised systems the apps are designed to send data to central government servers, but there are unknowns also for the decentralised apps. What categories of information? Do they include knowledge of sensitive private activities? Who will have access to the information – only health authorities, or community / social health providers? Central government? Police? Commercial users? Will data be stored, for how long?, where? Can the 'user''- who actually is the 'informant and supplier of information' – check and remove information?

For an example, in the South Korean system spatial data on people's movements in public spaces are publicly released to help identify potential contacts, and the family and friends of exposed people can also get tested. This is clearly beneficial for individuals, but it may have sidelined confidentiality. The concern is serious for socially marginalized people like LGBT+, and also sex workers (French & Monahan, 2020; Kim, 2020; PanDem, 2020). Likewise, India's Aarogya Setu knows the identities of users, it locates all the people a user has been in contact with and compares that to the government COVID-19 case database.

There are cases of individual and institutional processes of harassment and stigmatization of (suspected) carriers, such as attacks on scapegoat ethnic groups – Chinese in USA and Canada, Muslims in India, Africans in Shenzhen, South Asian and Filipino workers in Gulf States (UNOHCHR, 2020, and numerous media reports). Individuals or groups may be stereotyped as "super-spreaders" (Ghana, South Korea). Beyond identifying individuals who are committing undesirable acts, surveillance creates in everyone a feeling of always being watched, so that they become self-policing. This may allow the state to command its citizens without having to resort to physical force which is expensive and problematic, and instead constitutes a disempowering form of "self-vigilance" (Foucault, 2012).

There are also conventional data security issues. Apps can leak data to analytics firms and social media platforms; some can generate and lift data from the device without specific permission. There are already cases of data breaches by hackers, as in Australia and Austria, and false positives.

Related to confidentiality is the question of whether the app is voluntary (true in most cases), compulsory (e.g. in China), or trending towards compulsion, as with India's Aarogya Setu app. Initially in April 2020 it was voluntary but was later mandated by many government and non-government agencies as a requisite. It is compulsory for train passengers, and will be for air travel. The app has been used to control behaviour towards returning to 'normal life´, e.g. people who violated a lockdown curfew were forced to download the app before being released from detention. Public officials can be punished for not imposing installation in containment zones, private companies are held responsible for compliance; community welfare associations have forced residents to download it. This massive

acquisition of sensitive personal information is not yet governed by an anchoring law, although protocols supposedly limit its extent (Christopher, 2020, Reuben, 2020).

Commercial Infiltration Into COVID-19 Monitoring

We cannot ignore the ever-growing issues of surveillance and manipulation by commercial interests – continuous unsolicited monitoring, data mining, marketing, and eventually, behaviour manipulation and erosion of democracy. Facebook, Google, Amazon, and analytics companies have been accumulating location data for years, whether in personal detail or aggregated ever since internet platforms discovered how to monetize the "data exhaust" from our online communications: our searches, posts, tweets (Lyon, 2018, 2020; Zuboff, 2019). This must be signaled, but it is not the focus of this review because there is little evidence yet of commercial use of COVID-19 related health data. But such commercial data trawling is just a matter of time, considering that social media and online marketing are already impregnated in 4 billion plus users' smart phones. It is Amazon and Google which are developing many of the world's COVID-19 track-n-trace apps, and ironically, they are seen now as the champions of the decentralised systems which are 'combatting' central governments.

Surveillance as Control of Public Space

Increased surveillance may change how people use public space, how often they venture out in public and what they do there. Will expanded snooping affect individuals' feelings of belonging to a geographical space and a social community? The significance for public spaces lies in the likelihood of heavy and effective control of citizens' physical use of space. China started the strategy (first in post-lockdown Wuhan) of tracking potential infections with health controls in public places. Officials check for the use of face masks, check temperatures, and verify people's individualized QR health codes obtained from the health authorities. The QR code then serves as an electronic voucher for individuals to scan as they try to utilise buildings, subway stations, parks, shopping malls, supermarkets (Honey-Rosés et al., 2020; Horwitz & Goh, 2020).

Structurally, the whole crisis may be used to crackdown on the civil liberties of Freedoms of Peaceful Assembly and Movement (UN and European declarations of human rights (UNOHCHR, 2020) by spying on and controlling large gatherings. Surveilling movements may be an effective strategy against COVID-19, but it is already employed to deny opportunities for mass gatherings and suppress political opposition, e.g. restrictive actions in Catalonia, Hungary, Venezuela, Hong Kong, Russia, or USA. Historically, large public spaces, especially in the political, cultural centres of cities have been the loci of popular political gatherings and protests. Think of: Zocalo in Mexico City; Tiananmen, Beijing; Madan, Kiev; Tahrir, Cairo; Trafalgar, London; Azadi, Tehran; Bastille, Paris; or Gezi Park in Istanbul (Schwartzstein, 2020). There are no specific data on the increased installation of CCTV or drones in these popular places, but social isolation and monitoring Stay at Home are already connected with the suppression of opportunities to protest *en masse* (Brannen, 2020; CELAG, 2020; Selam Gebrekidan, 2020).

The imposed use of tracker apps can add to a paranoia of citizens in public spaces who are already trying to avoid close proximity. The apps, intended 'to save us', can exacerbate our potential misanthropy. It is one thing to be fearful that you may be contaminated, although cognitive dissonance allows that fear to diminish over time. But if you know your phone can always report your proximity (and if this is considered a crime), with the potential for future incarceration in your house, you will be more jumpy. Some people will leave their phones at home rather than carry them in public space (a significant and unlikely behavioural shift for most people). For marginalized urban dwellers, ethnic minorities or vulnerable immigrants, tracker apps and CCTV surveillance create yet more modes of monitoring and restrictions (Honey-Rosés et al., 2020; PanDem, 2020).

TRADE-OFFS IN THE FUTURE NORMAL

Tensions in Surveillance - Whose Responsibility is Risk?

The core issue in surveillance is a deep human dilemma. As argued in the Introduction, we have to confront tensions between the individual and society, and between individual self-reliance and social cooperation, balancing safety and risk at all levels. The related political questions are profound and maybe unanswerable - How much freedom of action must the individual be willing or able to bargain away for more society-based group security? How does anyone know what the trade-offs are between individual responsibility and social protection?

The fundamental discontinuity is between those who believe the responsibility is primarily that of the individual; and those who protest that this deliberately obscures the vast disparities between people - socio-economic classes, ethnicities and histories - as to their capacity to exercise responsibility. The latter argue there is a deliberate evasion of responsibilities, and duties of care by governments and the rich who control them. In the COVID-19 case, this is the diversion of attention from severely underfunded, understaffed public health and social services, brought to their knees by decades of neo-liberal austerity (Shabi, 2020). French & Monahan (2020) call this: "the *responsibilization* move (that) can subtly (and not-so-subtly) redirect blame for the crisis and its (mis)management to individuals and their families". The neo-liberal ideology counter-argues that when the state takes all responsibility, this destroys the initiative of people, that is, the agency of *responsible subjects* who might manage risks on their own and not rely on states or institutions to ensure safety (Adam, 2006; Smart, 1995).

Muddying the issue further are individual differences in attitudes towards risk, and therefore towards what is 'acceptable' surveillance. We can generalise to some extent, younger people tend to be much less risk-averse, and there are personality differences in risk attitudes towards health (Adam, 2006; Luhmann, 2005; Smart, 1995). The complexity of attitudes to risk is seen in the massive turnouts for *Black Lives Matter* in mid-2020 where multitudes of mostly young demonstrators chose to override pandemic fears and the real infection risks and gathered to voice their anger. You cannot social distance in such situations and the likelihood of new outbreaks is real. There are many other examples in this COVID-19 crisis time: large crowds choose to converge inside enclosed spaces for Trump rallies in the US; in Iran, Indonesia, India, South Korea, people worship together without a 1.5 metre rule; political protests flourish in Mali, Serbia, Greece, and everywhere a minority of young people continue partying without concern; they feel no pandemic risk. What is the consequence of this for control and surveillance? In the BLM case, (as elsewhere e.g. in Khabarovsk, Belgrade) many cities chose not to prevent the mass gatherings. This may appear to run counter to the argument that states use the COVID-19 distancing regulations to stop dissent (Luhrmann et al., 2020). Maybe when popular anger is strong enough with sheer numbers, the state has to back down on direct control. However these potential health-endangering public gatherings give some governments more justification, in their eyes, for extending their surveillance machinery.

Away from the profound philosophical and ideological positions, what does this mean in practice? The state can protect "us", if it has sufficient data about our health: our nature, that is, our "underlying health conditions" of diabetes, heart, obesity, cancer, vitamin D levels, and also our nurture, i.e. our exercise patterns, drinking, smoking, doping, partying. As individuals we do not want the state to know all these things, especially if we do not fully trust the state and its apparatus. We have extensive experience of states misusing surveilled information to check not just that we are behaving healthily, but also socially, in line with whatever are the norms of the state or the hegemonic culture. Unaccountable and unlegitimated surveillance tools violate our privacy and the data are easily used for tracking individuals for political control, - as already seen with facial recognition systems in Xinxiang, China (Gan, 2020; Horwitz & Goh, 2020), or potentially in Canada with ClearView AI (Masoodi, 2020).

Trust and Truth

Creating and maintaining trust is slow, it requires 'big' time, accumulated experiences of interactions, and cognitive and behavioral as well as emotional absorption. It is connected with power and accountability and surveillance (Dietz, 2011; Hillebrand, 2020; Luhmann, 2005; McCall et al., 2015). Will (younger) people be more likely to trust known geo-location based socializing (dating) apps, like Grindr, Blendr, Happn, rather than on the new state-sponsored COVID-19 apps? Maintaining public trust over time is crucial. Since any monitoring mechanism needs to be updated as this and new pandemics develop, trust, if any, has to be maintained with open communication and transparency. Among other things, this demands that there is no function creep, or suspicion of it. Moreover, trust is constructed when there is mutually-recognised purpose. "If tracing apps are to be widely adopted, they must make people want to use them. People need to feel like they are contributing to a common good. to feel empowered", - pertinent words spoken by an epidemiologist in Italy, Ciro Cattuto (Economist, 2020).

At a more profound level, trust needs shared meanings of truth. A sine qua non of the whole discussion is that currently we do not live in a world of shared truths. Instead we live in mini-worlds of informational "filter bubbles". We treasure our confirmations from mutually-reassuring, like-minded, uncritical audiences, and in the pandemic this so easily leads to all kinds of disinformation, skepticism of scientists, conspiracy theories, apocalyptic scenarios. The contemporary exchange of information is "characterized by a form of populist postmodernism where trust in institutions is eroded, leaving no agreed upon mechanisms for adjudicating truth claims" (French & Monahan, 2020, 6-7; also Hillebrand, 2020), and with respect to COVID-19, they say "pandemic anxiety creates dis-ease".

CONCLUSION – DISCOURSES AND RESISTANCE

Positioning Surveillance

There is no singular discourse about surveillance. Citizens and governments all want to know and balance the trade-offs between effective virus management, safety, security, fear, contentment, liberty, invisibility, anonymity, and freedom to dissent. The pandemic is forcing states and societies to revisit their position on these balances. Our new relationship with technologies is also contributing to a re-orientation and re-evaluation of past norms. Because increased surveillance is next to never reversible, we must carefully consider the long-term implications of decisions made today, under pandemic conditions.

The citizen asks 'keep me safe – without snooping from the State (and Big Tech and Big Commerce)' and wants that 'the system takes only the health information that it needs for measurement and prediction'.

Scientists assert that 'more information from tracking means more knowledge, which would provide better modelling and pandemic management'. The data needs are both to predict infection rates and patient load in hospitals, so as to "flatten the curve" by ensuring people "stay at home" and socially distance. Epidemiologists argue that had NYC, and indeed London and elsewhere, closed one week earlier maybe tens of thousands of lives would have been spared.

Some government Health agencies believe: 'we care, but can we trust citizens' good behaviour?' (as in Sweden). But two-way trust is rare, not everyone trusts, and therefore it is essential to identify also the bad behaviours", even if only in a few (Dietz, 2011). Concretely for COVID-19, 'good public behaviour' primarily means home isolation, limited contacts, social distancing, and masks.

Health agencies then tend to add: 'whilst we are about it, let's check for pre-indicators of vulnerable individuals and the asymptomatic carriers' – (In Seoul possibly one person infected 90+, and in Ghana supposedly one infected over 500). That easily leads to 'why not also search for and pre-empt conditions which are life-threatening, socially costly and partially avoidable – heart, liver, diabetes, smoking, obesity, STDs?' And, as mission creep always operates, the limited state surveillance on

individual's health conditions via apps or CCTV will smoothly morph into checking for social bad behaviour, as in e.g. China's Social Credit scoring system (Copyright & Media, 2015), and move on in many countries to suppression of political dissent (Luhrmann et al., 2020).

The profound issue of "how much surveillance" is totally political. But it is (almost) trans-ideological. The left criticizes state snooping, positing that the state has a duty of care towards citizens, but should not spy on them. On the right, libertarians and neo-libs criticize the suffocating hand of Big Government, but demand information on bad actors and dissidents. Nobody wants snooping as such, but each ideological actor wants just the categories of surveilled information that itself considers essential.

Resistance to Surveillance

Resistance to surveillance and snooping in general is a continuing issue beyond the scope here. We do note however, in connection to the viral spread of snooping in COVID-19 times, the civil society warriors like Amnesty, ACLU, the PanDem of Gothenburg University, Privacy International, UNOHCHR, many combative journalists and media, and academics who are creating constructive critiques (e.g. Klingler et al., 2017; Lyon, 2020).

We conclude instead with a contemporary (mid-2020) focus on the COVID-19 tracing apps. There are growing scientific concerns about insufficient adoption rates. Most people are just not using the apps – if they have that option (Jee, 2020; Reuben, 2020). For statistical epidemiological reasons, the apps need high levels of continuing usage to provide useful data. Without sufficient – and sustained - uptake, they have little value epidemiologically, maybe negative if they engender some form of false security.

Despite strong government promotions calling on altruistic social responsibility and pushing the line that downloading the app is essential to 'Get back to Work' whilst ´Flattening the Curve', (e.g. in Australia, Spain, UK, Singapore, France), there appears to be active user-resistance to surveillance by app. Even in Singapore, only 1/6th of a normally compliant population took up the Government's app after a month, and only 40% of Icelanders were using the "Ranking C-19" contact-tracing app, - then the most-adopted worldwide. In Australia after one month, the minimum target of 40% population coverage was unmet, and enthusiasm waned partly because citizens were losing their fear of infection.

There are growing doubts about the various technical flaws that have emerged: problems with Bluetooth range and overload, or with GPS signals, some incompatibility with Apple i-phones, multipath interference, etc. such that the apps may not actually be competent for tracking (Cellan-Jones, 2020; Jinfeng Li & Guo, 2020; Taylor, 2020). In terms of effectiveness, apparently until June, the Australian app had only identified one person additional to standard tracing (National Law Review, 2020; Taylor, 2020); and there is a similar story of minimal actual use from France (Jee, 2020; Reuben, 2020). This could be a short-term technological hitch until the bugs are fixed, but although it is hard to conclude yet, it is plausible these primarily technical deficiencies will turn out to be bigger constraints than any public concerns over privacy and confidentiality. After all, nearly four billion addicted users globally have been using social media (Facebook, WhatsApp, Twitter, Tiktok, Instagram, WeChat, YouTube) and e-commerce platforms (Google, Amazon, Alibaba, Tencent) for decades, and we seem to show slight hesitation over their snooping and data mining, despite that we are regularly alerted about this.

Another e-Space

Any attempt to predict the future of COVID-19 surveillance requires buckets of humility - "That's what bites about the future, there's no way to predict it. You just have to show up and see what happens" (Kirstin Cronn-Mills, 2012).

Despite the uncertain future, we have seen many bold predictions. For now, many people remain optimistic. A surprisingly large part of humanity believes that we may emerge from the pandemic as a world more socially just and environmentally sustainable (RSA, 2020). Is this optimism foolish or

essential in order to keep us going? Ideologically, this COVID-19 moment could be the progressive upside view of Naomi Klein's 'Shock Therapy', a potential counter shock to 'disaster capitalism' (Klein, 2007), a seismic radical realignment from the 'self-above all´ fundamentalism of neoliberalism to a 'self as part of society' vision of a cooperative caring society and economy. "If there was one dogma that defined neoliberalism, it's that most people are selfish. And it's from that cynical view of human nature that all the rest followed – the privatisation, the growing inequality, and the erosion of the public sphere" (Bregman, 2020).

Although we began this article with the golem's threats of the connected panopticon of the e-city, we prefer to end with the alternative offered by Bregman and others of a future space, in part created by the pandemic, of a " ..different, realistic view of human nature: that the evolution of humankind has (always) been to cooperate" (Bregman, 2020). In this cooperative society, the role and positioning of surveillance are such that citizens opt in, knowingly select their level of involvement in apps and their degree of cooperation/individuality, they can monitor what happens to their data, and above all they can monitor the monitors in an 'inverted surveillance'.

REFERENCES

ACLU. (2020). What's wrong with public video surveillance? *American Civil Liberties Union*. Retrieved from https://www.aclu.org/other/whats-wrong-public-video-surveillance

Adam, B. D. (2006). Infectious behaviour: Imputing subjectivity to HIV transmission. *Social Theory & Health*, *4*(2), 168–179. doi:10.1057/palgrave.sth.8700066

Amnesty International. (2020). Bahrain, Kuwait and Norway contact tracing apps among most dangerous for privacy. *Amnesty International Security Lab*. Retrieved from https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/

Andrejevic, M. (2004). The work of watching one another: Lateral surveillance, risk, and governance. *Surveillance & Society, 2*(4). https://www.apple.com/covid19/contacttracing

BBC. (2020). Singapore hands out coronavirus tracing devices. *BBC*. Retrieved from https://www.bbc.com/news/business-53216450

Bischoff, P. (2019). Surveillance camera statistics: which cities have the most CCTV cameras? The 20 most-surveilled cities in the world. *Comparitech*. Retrieved from https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/

Brannen, S. (2020). Will Covid-19 end the age of mass protests? *CSIS (Center for Strategic & International Studies)*. Retrieved from https://www.csis.org/analysis/will-covid-19-end-age-mass-protests

Bregman, R. (2020). The neoliberal era is ending: What comes next? *The Correspondent*. Retrieved from https://thecorrespondent.com/466/the-neoliberal-era-is-ending-what-comes-next/61655148676-a00ee89a

Burgess, M. (2020a). Privacy. Coronavirus contact tracing apps were meant to save us. They won't. *Wired*. Retrieved from https://www.wired.co.uk/article/contact-tracing-apps-coronavirus

Burgess, M. (2020b). Just how anonymous is the NHS Covid-19 contact tracing app? *Wired*. Retrieved from https://www.wired.co.uk/article/nhs-covid-app-data-anonymous

Burgess, M. (2020c). Why the NHS Covid-19 contact tracing app failed. Test, track and trace – just not with the NHS app. *Wired*. Retrieved from https://www.wired.co.uk/article/nhs-tracing-app-scrapped-apple-google-uk

CELAG (Centro Estratégico Latinoamericano de Geopolítica). (2020). *Geografía política del Coronavirus en América Latina.* Análisis político. CELAG. Retrieved from https://www.celag.org/geografia-politica-de-coronavirus-en-america-latina/

Cellan-Jones, R. (2020). Coronavirus: What went wrong with the UK's contact tracing app? *BBC Technology*. Retrieved from https://www.bbc.com/news/technology-53114251

Cheng, H. Y., Li, S. Y., & Yang, C. H. (2020). Initial rapid and proactive response for the COVID-19 outbreak—Taiwan's experience. *Journal of the Formosan Medical Association*, *119*(4), 771–773. doi:10.1016/j.jfma.2020.03.007 PMID:32222336

Christopher, N. (2020). India made its contact tracing app mandatory. Now people are angry. *Wired*. Retrieved from https://www.wired.co.uk/article/india-contact-tracing-app-mandatory-arogya-setu

Copyright and Media. (2015). Planning outline for the construction of a Social Credit System (2014-2020). Author. Copyright and Media (China). (2015). Retrieved from https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/

Cronn-Mills, K. (2012). *Beautiful Music for Ugly Children*. North Star Editions.

Dietz, G. (2011). Going back to the source: Why do people trust each other? *Journal of Trust Research*, *1*(2), 215–222. doi:10.1080/21515581.2011.603514

Economist. (2020, Apr. 15). App-based contact tracing may help end coronavirus lockdowns. But only if countries use it as part of a bigger system. *The Economist*.

Foucault, M. (2012). *Discipline and punish: The birth of the prison*. Vintage.

Fouquet, H. (2020). Paris tests face-mask recognition software on metro riders. *Bloomberg*. Retrieved from https://www.bloomberg.com/news/articles/2020-05-07/paris-tests-face-mask-recognition-software-on-metro-riders

French, M., & Monahan, T. (2020). Dis-ease surveillance: How might surveillance studies address COVID-19? *Surveillance & Society*, *18*(1), 1–11. doi:10.24908/ss.v18i1.13985

Future Market Insights. (2020). CCTV camera market could reach $16 billion by 2029 due to growing need from pandemic. *Future Market Insights*. Retrieved from https://www.sdmmag.com/articles/97983-cctv-camera-market-could-reach-16-billion-by-2029-due-to-growing-need-from-pandemic

Gan, N. (2020). China is installing surveillance cameras outside people's front doors ... and sometimes inside their homes. *CNN News*. Retrieved from https://edition.cnn.com/2020/04/27/asia/cctv-cameras-china-hnk-intl/index.html

GDPRHub. (2020). Projects using personal data to combat SARS-CoV-2. *GDPRHub*. Retrieved from https://gdprhub.eu/index.php?title=Projects_using_personal_data_to_combat_SARS-CoV-2

Gebrekidan, S. (2020). For autocrats, and others, Coronavirus is a chance to grab even more power. *The New York Times*. Retrieved from https://www.nytimes.com/2020/03/30/world/europe/coronavirus-governments-power.html

Google. (n.d.). https://www.google.com/covid19/exposurenotifications/

Halpern, S. (2020). Can we track COVID-19 and protect privacy at the same time? *The New Yorker*. Retrieved from https://www.newyorker.com/tech/annals-of-technology/can-we-track-covid-19-and-protect-privacy-at-the-same-time

Hillebrand, K. (2020, April). State surveillance: Exploiting fear during the pandemic crisis? *SSRN*, *30*. Advance online publication. doi:10.2139/ssrn.3593408

Honey-Rosés, J., Anguelovski, I., Chireh, V., Daher, C., Konijnendijk, C., Litt, J., Mawani, V., McCall, M. K., Orellana, A., Oscilowicz, E., Sánchez, U., Senbel, M., Xueqi, T., Villagomez, E., Zapata, O., & Nieuwenhuijsen, M. (2020). *The impact of COVID-19 on public space: An early review of the emerging questions - design, perceptions and inequities*. Cities and Health. doi:10.1080/23748834.2020.1780074

Horwitz, J., & Goh, B. (2020). As Chinese authorities expand use of health tracking apps, privacy concerns grow. *Reuters Technology News*. Retrieved from https://www.reuters.com/article/us-health-coronavirus-china-tech/as-chinese-authorities-expand-use-of-health-tracking-apps-privacy-concerns-grow-idUSKBN23212V

Hou, Du, Jiang, Zhou, & Lin. (2020). *Assessment of public attention, risk perception, emotional and behavioural responses to the COVID-19 outbreak: social media surveillance in China*. DOI: 10.1101/2020.03.14.20035956

Jee, C. (2020). 8 million people, 14 alerts: why some COVID-19 apps are staying silent. *MIT Technology Review*. Retrieved from https://www.technologyreview.com/2020/07/10/1005027/8-million-people-14-alerts-why-some-covid-19-apps-are-staying-silent/

Kelion, L. (2020). NHS rejects Apple-Google coronavirus app plan. *BBC Technology Desk*. Retrieved from https://www.bbc.com/news/technology-52441428

Kim, M. S. (2020). Seoul's radical experiment in digital contact tracing. *The New Yorker*. Retrieved from https://www.newyorker.com/news/news-desk/seouls-radical-experiment-in-digital-contact-tracing

Klein, N. (2007). *Shock Therapy: The Rise of Disaster Capitalism*. Knopf Canada.

Klingler, C., Silva, D. S., Schuermann, C., Reis, A. A., Saxena, A., & Strech, D. (2017). Ethical issues in public health surveillance: A systematic qualitative review. *BMC Public Health*, *17*(1), 295. doi:10.1186/s12889-017-4200-4 PMID:28376752

Li, J., & Guo, X. (2020). *Review. COVID-19 contact-tracing apps: A survey on the global deployment and challenges*. Retrieved from https://arxiv.org/ftp/arxiv/papers/2005/2005.03599.pdf

Luhmann, N. (2005). *Risk: a sociological theory*. Aldine Transaction.

Lührmann, A., Maerz, S. F., Grahn, S., Alizada, N., Gastaldi, L., Hellmeier, S., Hindle, G., & Lindberg, S. I. (2020). *Autocratization surges – Resistance grows. Democracy Report 2020*. Gothenburg: University of Gothenburg, Varieties of Democracy Institute (V-Dem). https://www.v-dem.net/en/

Lührmann, A., & Rooney, B. (2020). *Autocratization by decree: states of emergency and democratic decline.* Gothenburg: University of Gothenburg, Varieties of Democracy Institute (V-Dem), Working Paper Series 2020: 85.

Lyon, D. (2018). *The culture of surveillance: Watching as a way of life*. Polity Press.

Lyon, D. (2020). The coronavirus pandemic highlights the need for a surveillance debate beyond 'privacy'. *The Conversation*. Retrieved from https://theconversation.com/the-coronavirus-pandemic-highlights-the-need-for-a-surveillance-debate-beyond-privacy-137060

Marx, G. T., & Muschert, G. W. (2007). Personal information, borders, and the new surveillance studies. *Annual Review of Law and Social Science*, *3*(1), 375–395. doi:10.1146/annurev.lawsocsci.3.081806.112824

Masoodi, J. (2020). Police & governments may increasingly adopt surveillance technologies in response to coronavirus fears. *The Conversation*. Retrieved from https://www.sscqueens.org/news/categories/new-publication

McCall, M. K., Martinez, J., & Verplanke, J. (2015). Shifting boundaries of volunteered geographic information systems and modalities: Learning from PGIS. *ACME: An International E-Journal for Critical Geographies*, *14*(3), 791–826.

Miller, L. (2020). Companies are enforcing their own contact tracing to track employees. *Wired.* Retrieved from. uk/article/contact-tracing-offices-coronavirus

National Law Review. (2020). How safe is "COVIDSafe" – Australia's COVID-19 contact-tracing app? *National Law Review*. https://www.natlawreview.com/article/how-safe-covidsafe-australia-s-covid-19-contact-tracing-app

Oliver, N., Lepri, B., Sterly, H., Lambiotte, R., Deletaille, S., De Nadai, M., & Colizza, V. et al. (2020). Mobile phone data for informing public health actions across the COVID-19 pandemic life cycle. *Science Advances*, *6*(23), eabc0764. Advance online publication. doi:10.1126/sciadv.abc0764 PMID:32548274

PanDem (Pandemic Backsliding Project). (2020). *Pandemic backsliding: Democracy during COVID-19*. Gothenburg: University of Gothenburg: Varieties of Democracy Institute (V-Dem). https://www.v-dem.net/en/analysis/PanDem/

Paolotti, D., Carnahan, A., Colizza, V., Eames, K., Edmunds, J., Gomes, G., & Van Noort, S. et al. (2014). Web-based participatory surveillance of infectious diseases: The Influenzanet participatory surveillance experience. *Clinical Microbiology and Infection*, *20*(1), 17–21. doi:10.1111/1469-0691.12477 PMID:24350723

Pascu, L. (2020) Liechtenstein to provide citizens with biometric bracelets to contain coronavirus. *BiometricUpdate.com*. Retrieved from https://www.biometricupdate.com/202004/liechtenstein-to-provide-citizens-with-biometric-bracelets-to-contain-coronavirus

Privacy International. (2020). COVID Contact tracing apps are a complicated mess: what you need to know. *Privacy International*. Retrieved from https://privacyinternational.org/long-read/3792/covid-contact-tracing-apps-are-complicated-mess-what-you-need-know

Reuben, A. (2020). Coronavirus: Does anyone have a working contact-tracing app? *BBC Reality Check*. Retrieved from https://www.bbc.com/news/53168438

Richardson, S., & Mackinnon, D. (2018). Left to their own devices? Privacy implications of wearable technology in Canadian workplaces. Report to the Office of the Privacy Commissioner of Canada, under the 2016-2017 Contributions Program. Queens University, Surveillance Studies Centre.

RSA (Royal Society). (2020). *Time for change. Brits see cleaner air, stronger social bonds and changing food habits amid lockdown*. London: RSA (Royal Society for the Encouragement of Arts, Manufactures and Commerce). Retrieved from https://www.thersa.org/about-us/media/2019/brits-see-cleaner-air-stronger-social-bonds-and-changing-food-habits-amid-lockdown

Schwartzstein, P. (2020). How urban design can make or break protests: Cities' geography can aid, underscore or discourage a protest movement's success. *Smithsonian Magazine*. Retrieved from https://www.smithsonianmag.com/history/geography-protest-how-urban-design-can-make-or-break-people-power-180975189/

Shabi, R. (2020, July). The pro-privatization shock therapy of the UK's COVID response. *The New York Review of Books*, *8*. https://www.nybooks.com/daily/2020/07/08/the-pro-privatization-shock-therapy-of-the-uks-covid-response/

Siddiqui, A. (2020). Here are the countries using Google and Apple's COVID-19 contact tracing API. *XDAdevelopers*. Retrieved from https://www.xda-developers.com/google-apple-covid-19-contact-tracing-exposure-notifications-api-app-list-countries/

Simonite, T. (2020). Amazon touts AI for social distancing amid worker complaints. *Wired*. Retrieved from https://www.wired.com/story/amazon-touts-ai-social-distancing-worker-complaints/

Smart, B. (1995). The subject of responsibility. *Philosophy and Social Criticism*, *21*(4), 93–109. doi:10.1177/019145379502100405

Snowden, F. M. (2019). *Epidemics and society: from the black death to the present*. Yale University Press. doi:10.2307/j.ctvqc6gg5

Straits Times. (2020). Singapore robot reminds visitors about safe distancing measures in Bishan-Ang Mo Kio Park. *Straits Times*. Retrieved from https://www.straitstimes.com/singapore/robot-reminds-visitors-about-safe-distancing-measures-in-bishan-ang-mo-kio-park

Taylor, J. (2020). The PM told Australians in April the contact tracing app was key to getting back to normal but just one person has been identified using its data. *The Guardian*. Retrieved from https://www.theguardian.com/world/2020/may/24/how-did-the-covidsafe-app-go-from-being-vital-to-almost-irrelevant

UNOHCHR. (2020). *COVID-19: States should not abuse emergency measures to suppress human rights – UN experts*. Geneva: Office of the United Nations High Commissioner for Human Rights. https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25722%26LangID=E

World Health Organization. (2005). *International health regulations*. World Health Organization.

World Health Organization. (2020). Critical preparedness, readiness and response actions for COVID-19: interim guidance, 22 March 2020 (No. WHO/2019-nCoV/Community_Actions/2020.3). Geneva: World Health Organization.

Zuboff, S. (2019). *The age of surveillance capitalism*. Profile.

Michael McCall (studied at Bristol and Northwestern) is currently Senior Researcher in CIGA research centre of UNAM in Morelia, Mexico. Previously he worked in ITC, Netherlands and in Sri Lanka and the University of Dar es Salaam. He is a social geographer involved mainly in Eastern & Southern Africa, South Asia, Mexico and Latin America. Primary research and teaching experience are in community mapping, Participatory GIS and VGI of rural and urban local spatial knowledge, with emphases on participatory spatial planning, community initiatives, risks and vulnerability, and environmental management.

Margaret M. Skutsch is a human geographer working on a range of local level natural resource management issues and climate change policy in developing countries. She is a senior researcher at CIGA-UNAM from 2008-2019, now retired.

Jordi Honey-Rosés is Associate Professor at the School of Community and Regional Planning at the University of British Columbia in Vancouver, Canada. He is an environmental planner with interests in experimental methods and public space.